**НОРМАТИВНИЙ ДОКУМЕНТ**
**СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ**

# Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем

**НД ТЗІ 3.6-006-24**

Адміністрація Державної служби спеціального зв’язку та захисту інформації України

Київ 2024

**НОРМАТИВНИЙ ДОКУМЕНТ**
**СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ**

Затверджено
Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України
від "  "  20  р. №

# Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем

**НД ТЗІ 3.6-006-24**

Адміністрація Держспецзв'язку

Київ 2024

## ПЕРЕДМОВА

1 РОЗРОБЛЕНО: Державною службою спеціального зв’язку та захисту інформації України.

УВЕДЕНО ВПЕРШЕ.

**ЗМІСТ**

# НД ТЗІ 3.6 -006-23

**Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем**

Чинний від _____

## 1 Галузь використання

Цей нормативний документ (НД) описує систему дій щодо вибору заходів захисту як окремий етап Порядку впровадження систем безпеки інформації в державних органах, на підприємствах, в організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці.

Нормативний документ деталізує заходи захисту інформації, що впроваджуються в інформаційних системах, які обробляють критичну інформацію.

Цей нормативний документ також має на меті надати методичну допомогу організаціям щодо впровадження системи управління ризиками інформаційної безпеки та задоволення вимог безпеки інформації та приватності:

- надання всеосяжного та гнучкого каталогу заходів захисту для задоволення поточних потреб організації в захисті інформації, а також для задоволення майбутніх потреб, які можуть виникати на основі постійно мінливих загроз безпеки, посилення вимог безпеки та приватності, удосконалення технологій обробки інформації, а також підвищення обізнаності потенційних порушників;
- створення основ для розроблення методів і процедур оцінювання ефективності заходів захисту;
- поліпшення взаємодії між організаціями шляхом надання загального лексикону безпеки, який підтримує обговорення концепцій безпеки, приватності та управління ризиками безпеки.

Заходи захисту, що містяться в цьому нормативному документі, за своїм змістом не залежать від процесу обґрунтування та вибору заходів захисту, що впроваджені в конкретній організації. Процес вибору заходів захисту може бути частиною загальноорганізаційного процесу управління ризиками, процесу проєктування інформаційної системи на основі життєвого циклу тощо.

Правила вибору заходів захисту можуть спиратися на багато факторів, наприклад:

- потреби та завдання захисту інтересів основних зацікавлених сторін (стейкхолдерів);
- мету (місію, призначення), цілі, завдання організації;
- стандарти та найкращі практики захисту інформації, вимоги щодо дотримання чинного законодавства у сфері захисту інформації та кібербезпеки, нормативних документів, політик і правил безпеки тощо.

Комплексний характер заходів захисту у поєднанні з гнучким процесом вибору заходів захисту дозволить організаціям дотримуватися чинних вимог безпеки та приватності й досягнути адекватного рівня безпеки для своїх інформаційних систем.

Каталог заходів захисту може бути ефективно використаний для захисту організацій, осіб та інформаційних систем від відомих і нових загроз, що реалізуються в різних операційних, експлуатаційних і технічних середовищах. Організації, в особі визначених посадовців, безпосередньо несуть відповідальність за вибір і обґрунтування відповідного заходу захисту, який є елементом профілю безпеки інформаційної системи (організації).

Заходи захисту, що надані в цьому нормативному документі, являють собою сучасні й актуальні на цей час заходи захисту, впровадження яких гарантує безпеку інформаційних систем і організацій, а також приватність осіб.

Заходи захисту мають періодично переглядатися з метою:

- урахування практичного досвіду, отриманого від реалізації заходів захисту та використання засобів захисту;
- задоволення нових або переглянутих вимог безпеки та приватності, що містяться в

законодавстві у сфері захисту інформації, захисту персональних даних, кібербезпеки тощо;

- урахування нових загроз безпеці, вразливостей, технологій порушення безпеки та конкретних атак;
- урахування розвитку технологій обробки інформації тощо.

Запропоновані зміни до заходів захисту мають проходити через прозорий процес публічного перегляду для отримання зворотного зв'язку від державного та приватного секторів, а також досягнення консенсусу щодо таких змін. Це забезпечує стабільний, гнучкий, технічно обґрунтований набір (систему) заходів захисту для організацій, які використовують цей нормативний документ.

## 2 Нормативні посилання

У цьому НД ТЗІ наведено посилання на такі закони, стандарти, політики, регламенти, директиви, інструкції та нормативні документи:

ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення;

ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення;

НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу;

ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT);

НД ТЗІ 3.6-004-21 «Порядок впровадження систем безпеки інформації в державних органах, на підприємствах, в організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці»;

НД ТЗІ 3.6-005-21 «Порядок категоріювання безпеки інформаційної системи та інформації»;

НД ТЗІ 3.6-007-21 «Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем».

## 3 Визначення

У цьому НД ТЗІ подано терміни та визначення згідно із ДСТУ 3396.2, ДСТУ 2226, НД ТЗІ 1.1-003, а також НД ТЗІ, який описує Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, в організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці.

## 4 Позначення та скорочення

У цьому НД використано такі позначення та скорочення:

БІ – Безпека інформації;
ІС – Інформаційна система;
ІТ – Інформаційна технологія;
НД – Нормативний документ;
ОС – Операційна система;
ПД – Персональні дані;
ПЕМВН – Побічні електромагнітні випромінювання і наведення;
СБІ – Система безпеки інформації;
VPN – Virtual Private Network.

## 5 Передумови вибору заходів захисту

### 5.1. Мета та завдання вибору заходів захисту

Вибір заходів захисту для інформаційних систем є одним з етапів розгортання системи безпеки інформації (СБІ) в Організації, що ґрунтується на моделі ПВПД (плануй – виконуй – перевіряй – дій), яка визначена в ISO/IEC 27001:2015 (рис. 5.1).

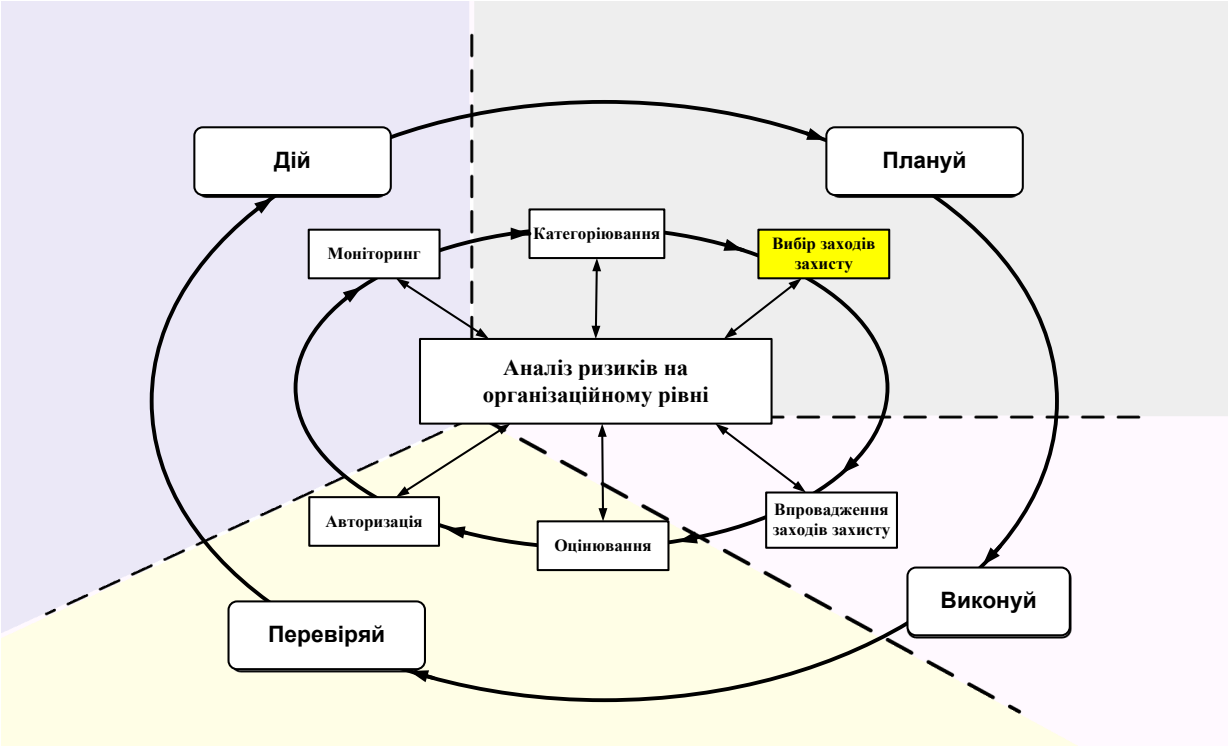


Рисунок 5.1 – Відповідність етапу вибору заходів захисту СБІ моделі ISO/IEC 27001

**Метою етапу** є формулювання вимог безпеки та приватності для ІС, а також вибір рівня базового (галузевого) профілю безпеки заходів захисту.

У таблиці 5.1 наведено короткий опис **завдань та очікуваних результатів етапу** вибору заходів захисту.

Таблиця 5.1 – Завдання та результати етапу впровадження (реалізації) заходів захисту

| Завдання | Результати |
|---|---|
| **Завдання В-1**<br>Формулювання Програми БІ та приватності | Програми БІ та приватності ***розроблена*** та ***задокументована*** |
| **Завдання В-2**<br>Вибір базового профілю безпеки або галузевого профілю безпеки | ***Обрано*** та ***задокументовано*** рівень базового профілю безпеки або галузевого профілю безпеки |

Відповідальність за вибір ЗЗІ та ПД покладається на Власника (Розпорядника) ІС. Безпосереднє виконання покладається на адміністратора безпеки або інших відповідальних осіб за безпеку інформації.

### 5.2. Вимоги безпеки й приватності та заходи захисту

Вимога безпеки — це твердження, яке виражає конкретну потребу в безпеці інформації (активу), включно із супутніми обмеженнями та умовами. Вимога безпеки, що висувається до інформації, інформаційної системи чи організації, може походити з різних джерел, серед яких,

наприклад, закони, розпорядчі документи уряду, нормативні документи, міжнародні, національні та галузеві стандарти, накази, директиви, правила (політики), положення, а також потреби конкретної організації. Вимоги безпеки можуть стосуватися можливостей розроблених інформаційних систем, які впроваджені для підтримки функцій або процесів організації в різних сферах її діяльності.

Вимоги безпеки та приватності — це підмножина вимог, які висуваються до інформаційної системи чи організації для забезпечення конфіденційності, цілісності та доступності інформації, що обробляється, зберігається або передається інформаційною системою.

Вимоги щодо приватності спрямовані на захист особистого життя приватних осіб, що пов'язано зі створенням, збиранням, використанням, обробкою, зберіганням, поширенням, розкриттям чи видаленням персональних даних.

Заходи захисту — це заходи, які спрямовані на задоволення вимог безпеки та приватності. Заходи захисту можуть реалізовуватися в різних контекстах для досягнення цілей безпеки. Заходи захисту, що застосовуються в контексті безпеки та приватності, впроваджуються для задоволення потреб захисту організацій, інформаційних систем і осіб. Своєю чергою, такі потреби визначаються набором вимог безпеки та приватності. Заходи захисту також визначають політику (правила) безпеки та приватності. Важливо зрозуміти взаємодоповнювальний характер вимог безпеки та заходів захисту.

Інформаційні системи являють собою складну організаційно-технічну систему (середовище). Відповідно, механізми, що реалізують заходи захисту в інформаційних системах, можуть містити як технічні, так і організаційні й адміністративні заходи.

Заходи захисту в цьому документі систематизовані та представлені у вигляді каталогу — набору класів заходів захисту. Заходи захисту вибираються та впроваджуються залежно від результатів категоріювання безпеки інформаційної системи й аналізу ризиків на організаційному та системному рівнях. Наприклад, процес вибору заходів захисту може бути елементом процесів управління ризиками, проєктування інформаційних систем на основі життєвого циклу, експлуатації наявних інформаційних систем тощо. Незалежно від того, яким чином визначені вимоги безпеки та вибрані заходи захисту в певній організації, важливо чітко встановити: взаємозв'язок між ними для досягнення результатів щодо безпеки та приватності, враховуючи потреби захисту зацікавлених сторін та приватних осіб; припущення щодо безпеки; обмеження, які визначені для організації; обмеження щодо вартості, часу та продуктивності реалізації (впровадження) заходів захисту; рішення щодо управління ризиками.

## 6 Організація каталогу та структура заходів захисту

### 6.1 Каталог заходів захисту

Заходи захисту, що визначені в цьому нормативному документі, мають чітко визначену організацію та структуру.

На рисунку 6.1 проілюстроване впорядкування заходів захисту (структура каталогу).

Всього визначено 20 класів заходів захисту. Кожний клас містить декілька груп заходів захисту (всього 294 групи). Своєю чергою захід захисту може мати декілька посилень (всього 1039 посилених заходів захисту).

Клас заходів захисту — це сукупність заходів захисту, які стосуються конкретного аспекту забезпечення безпеки інформації. Для позначення класу використовується ідентифікатор з двох літер, наприклад УПРАВЛІННЯ ДОСТУПОМ (AC). (Латиниця збережена для забезпечення гармонізації профілів безпеки з профілями безпеки інших країн.)

У таблиці 6.1 наведено перелік класів заходів захисту.

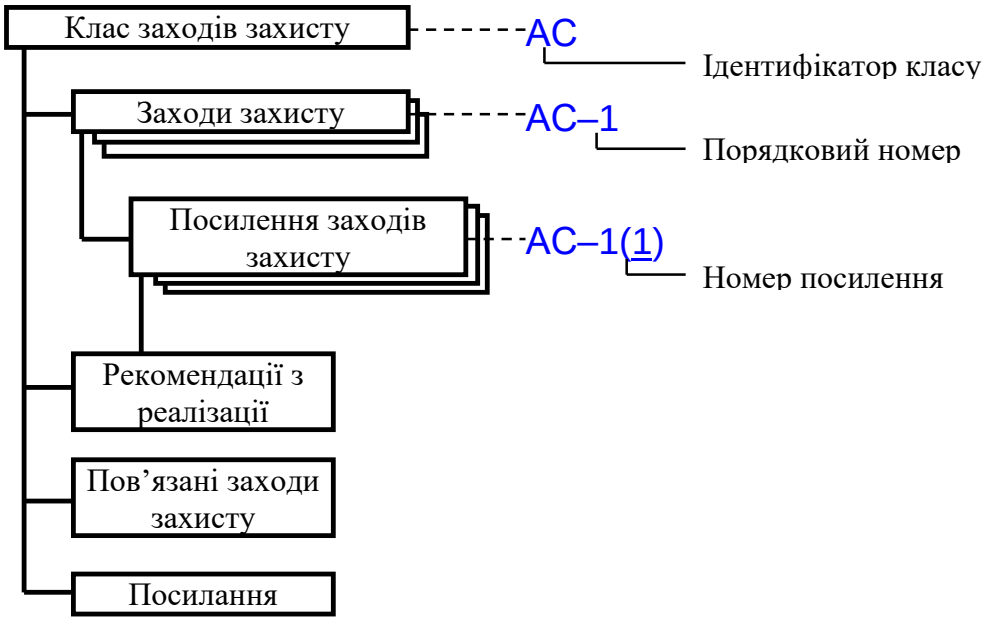


Рисунок 6.1 — Упорядкування заходів захисту (структура каталогу)

Таблиця 6.1 — Перелік класів заходів захисту

| № з/п | ID класу | Назва класу |
|---|---|---|
| 1. | AC | Управління доступом |
| 2. | AT | Обізнаність і навчання |
| 3. | AU | Аудит і підзвітність |
| 4. | CA | Оцінювання, акредитація та моніторинг безпеки |
| 5. | CM | Управління конфігурацією |
| 6. | CP | Планування безперервної роботи |
| 7. | IA | Ідентифікація та автентифікація |
| 8. | IR | Реагування на інциденти |
| 9. | MA | Технічне обслуговування |
| 10. | MP | Захист носіїв інформації |
| 11. | PE | Фізичний захист і захист робочого середовища |
| 12. | PL | Планування безпеки |
| 13. | PM | Менеджмент інформаційної безпеки |
| 14. | PS | Кадрова безпека |
| 15. | PT | Повноваження на обробку персональних даних |
| 16. | RA | Оцінка ризику |
| 17. | SA | Придбання системи та послуг |
| 18. | SC | Системний і комунікаційний захист |
| 19. | SI | Цілісність системи та інформації |
| 20. | SR | Управління ризиками ланцюга поставок |

Захід захисту представляється у вигляді описового формулювання, що може мати в собі аспекти політики, нагляду, впровадження процесів і використання технічних (програмних, програмно-апаратних, апаратних) засобів захисту. Заходи захисту реалізуються діями окремих

осіб або механізмами захисту в інформаційних системах. Заходи захисту позначаються групою з двох літер (за позначенням класу) та цифри — порядкового номера групи заходів захисту в класі. Наприклад, AC-1 — Політика та процедури управління доступом. Якщо захід захисту вилучений з каталогу, за ним зберігається умовне позначення для забезпечення спадковості профілів безпеки, що були розроблені раніше.

### 6.2 Структура заходів захисту

Кожний захід захисту має таку структуру (шаблон) (рисунок 6.2):

- основний розділ;
- розділ рекомендацій з реалізації;
- розділ посилення заходу;
- розділ, який містить інформацію про пов'язані заходи захисту;
- довідковий розділ (посилання).

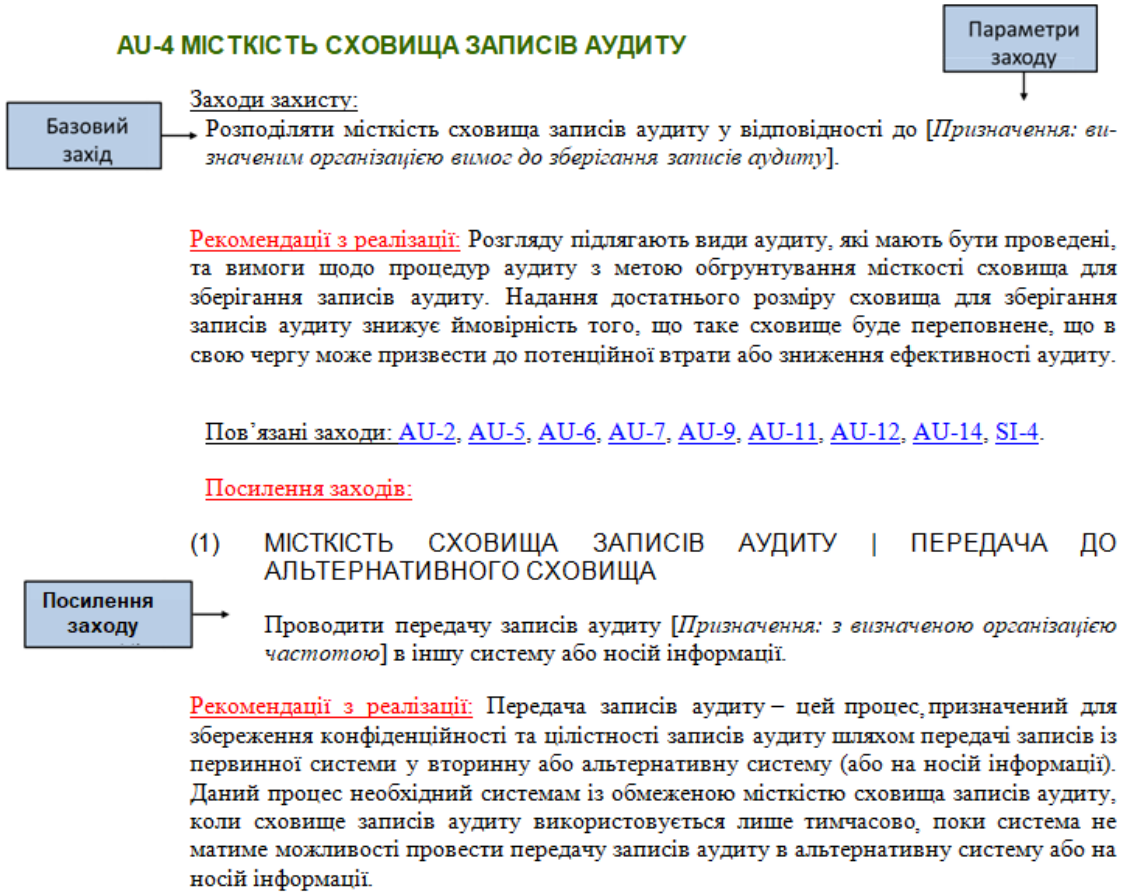


Рисунок 6.2 — Структура групи заходів захисту

*Основний розділ* описує базові заходи захисту, які потрібно реалізувати (впровадити) в інформаційній системі та організації. У розділі описуються заходи захисту, які можуть бути реалізовані в інформаційній системі із застосуванням технічних (програмних, апаратних, програмно-апаратних) засобів захисту або впроваджені шляхом виконання певних дій і діяльності, що здійснюються окремими особами (персоналом) або організаціями. Організація призначає відповідальних осіб за розробку, впровадження, управління та моніторинг заходу захисту. Організації мають можливість реалізувати або впровадити вибраний захід захисту будь-яким способом (механізмом), який забезпечить виконання вимоги безпеки та відповідає призначенню (місії, завданням) і потребам організації, відповідно до законодавства та політик безпеки.

Заходи захисту мають змінні параметри, які треба визначити чи вибрати зі списку запропонованих під час налаштування профілю безпеки з урахуванням конкретних умов діяльності організації та застосування інформаційної системи, структурно-функціональних характеристик інформаційної системи, результатів аналізу ризиків безпеки. Цей механізм надає організаціям можливість налаштувати заходи захисту з урахуванням вимог політики безпеки та приватності конкретних зацікавлених сторін. Результати оцінювання ризиків безпеки також є важливим фактором при визначенні конкретних значень параметрів заходів захисту. Організації, в особі визначених посадових осіб, безпосередньо несуть відповідальність за вибір, обґрунтування та призначення параметрів для кожного заходу захисту.

Розділ *рекомендацій з реалізації* містить додаткову інформацію про захід захисту. Розділ має рекомендаційний характер, та організація може використовувати ці рекомендації за потреби. Рекомендації з реалізації містять інформацію щодо впровадження заходу в контексті реалізації та робочого середовища засобів захисту, оцінок ризиків безпеки, особливостей технологій і механізмів безпеки, вимог галузевих стандартів та нормативних документів, практики захисту інформації тощо. Рекомендації з реалізації також можуть пояснювати результати впровадження заходів захисту, їх значущість щодо забезпечення вимог безпеки та наводити приклади застосування заходів захисту. Також рекомендації з реалізації можуть міститься в розділі посилення заходу захисту.

Розділ *посилення заходів захисту* містить положення про можливості посилення та розширення функціональності базового заходу захисту. В обох випадках посилення заходу захисту реалізуються (впроваджуються) в інформаційних системах та середовищах, які потребують більшого захисту, ніж забезпечується базовим заходом захисту, або коли організації вимагають доповнення функціональних можливостей базового заходу захисту чи гарантій безпеки за результатами оцінювання ризику та моніторингу безпеки. Посилення заходів захисту послідовно нумеруються в межах кожного базового заходу захисту. Кожне посилення заходу захисту має коротку назву, яка вказує на передбачувану функцію або можливість, що надається удосконаленням. Наприклад, якщо для заходу захисту AU-4 «Місткість сховища записів аудиту» вибрано посилення заходу, то ідентифікатор заходу захисту стає AU-4 (1). Числове позначення посилення заходу захисту використовується для ідентифікації цього розширення в межах базового заходу захисту. Позначення не вказує на значущість посилення заходу захисту, рівень або ступінь захисту чи будь-яку ієрархічну залежність між посиленими заходами захисту. Посилення заходу захисту не може бути вибрано окремо. Тобто, якщо вибрано посилення заходу захисту, то відповідний базовий захід захисту все одно має бути впроваджений (реалізований).

У розділі *пов'язані заходи захисту* надано перелік заходів захисту, які безпосередньо впливають або підтримують впровадження (реалізацію) цього заходу чи посилення заходу захисту. Якщо посилення заходу захисту безпосередньо пов'язані з їх базовим заходом захисту, то пов'язані заходи захисту, на які посилається базовий захід захисту, не повторюються в посиленнях заходу захисту. Однак можуть бути пов'язані заходи захисту, що визначені для посилень заходів захисту, на які не посилається базовий захід захисту (тобто, пов'язаний захід захисту пов'язаний лише з цим конкретним посиленням заходу захисту).

Розділ *посилання* містить перелік релевантних стандартів, нормативних документів та інших корисних посилань, які стосуються впровадження (реалізації) заходу захисту.

## 7 Вибір заходів захисту для впровадження (реалізації) в інформаційній системі

Вибір заходів захисту для їх впровадження (реалізації) в інформаційній системи здійснюється під час проєктування системи захисту інформації інформаційної системи.

Вибір заходів захисту здійснюється на основі категорії критичності інформаційної системи, який визначається за рівнем критичності інформації, що обробляється інформаційною системою, а також з урахуванням призначення та структурно-функціональних характеристик інформаційної системи та результатів аналізу ризиків безпеки. Положення щодо визначення категорії критичності ІС містяться в НД ТЗІ «Порядок категоріювання

безпеки інформаційної системи та інформації». До структурно-функціональних характеристик інформаційної системи належать: структура та склад інформаційної системи; фізичні, логічні, функціональні та технологічні взаємозв'язки між компонентами системи; взаємозв'язки з іншими інформаційними системами та інформаційно-комунікаційними мережами; режими обробки інформації та інші характеристики інформаційної системи, використані інформаційній технології, а також особливості функціонування інформаційної системи.

**7.1 Види профілів безпеки та їх взаємозв'язок**

Заходи захисту інформації реалізуються (впроваджуються) в інформаційній системі в рамках системи захисту інформації залежно від категорії критичності інформаційної системи, структурно-функціональних характеристик інформаційної системи, результатів аналізу ризиків, застосовуваних інформаційних технологій і особливостей функціонування інформаційної системи.

Вибір набору заходів захисту є важливим завданням для організацій. Цей процес має бути ефективним, адекватно відповідати призначенню (місії), цілям і завданням організації, задовольняти тим вимогам безпеки, що висуваються чинним законодавством, нормативними документами, стандартами, положеннями, політиками безпеки та приватності. Немає єдиного набору заходів захисту, який би розв'язував усі проблеми безпеки та приватності в будь-якій ситуації. Вибір найбільш прийнятного заходу захисту для конкретної ситуації або інформаційної системи з метою адекватного реагування на ризики безпеки вимагає розуміння цілей і завдань організації, призначення інформаційної системи, її структурно-функціональних характеристик, а також робочого середовища інформаційної системи. Визначення заходів захисту також вимагає тісної співпраці з ключовими зацікавленими сторонами. З огляду на таке розуміння вибору заходів захисту, організації мають продемонструвати, як ефективно й економічно забезпечити конфіденційність, цілісність і доступність інформації та систем, а також безпеку приватного життя приватних осіб у контексті підтримки цілей і завдань організації.

Щоб допомогти організаціям у виборі набору засобів захисту вводиться концепція профілю безпеки.

Профіль безпеки — це реалізаційно незалежний набір заходів захисту, який відображає потреби в безпеці інформації та приватності особистого життя, що обумовлені цілями та завданнями організації, призначенням інформаційної системи, критичністю інформації та ризиками безпеки.

Виділять наступні види профілів безпеки (рисунок 7.1)

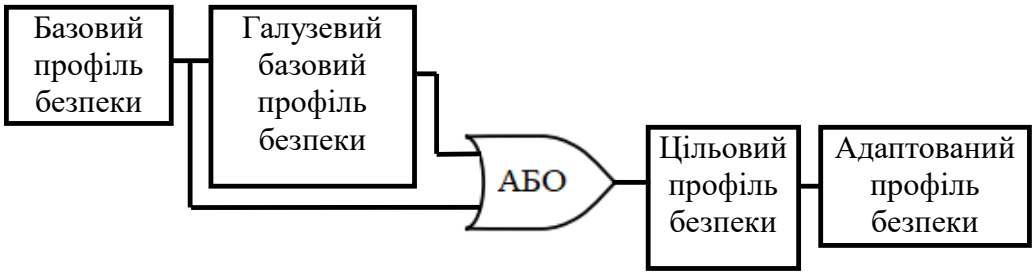


Рисунок 7.1 — Види профілів безпеки та їх взаємозв'язок

Базовий профіль безпеки — це мінімальний набір заходів захисту, встановлених для відповідної категорії безпеки інформаційної системи. Він є відправною точкою для наступних налаштувань, які можуть бути застосовані до базового профілю безпеки для створення галузевого, цільового та адаптованого профілів безпеки інформаційної системи.

Вибір заходів захисту для базового профілю безпеки ґрунтується на багатьох чинниках, включно з усталеною практикою захисту, технології захисту інформації, вимог міжнародних і національних стандартів у сфері захисту інформації. Цей нормативний документ містить три базових профілі безпеки для інформаційних систем низького, середнього та високого рівня (Додаток А).

Базовий профіль безпеки є відправною точкою для розробки галузевого профілю безпеки або цільового профілю безпеки.

Порядок вибору заходів захисту наведений на рисунку 7.2.

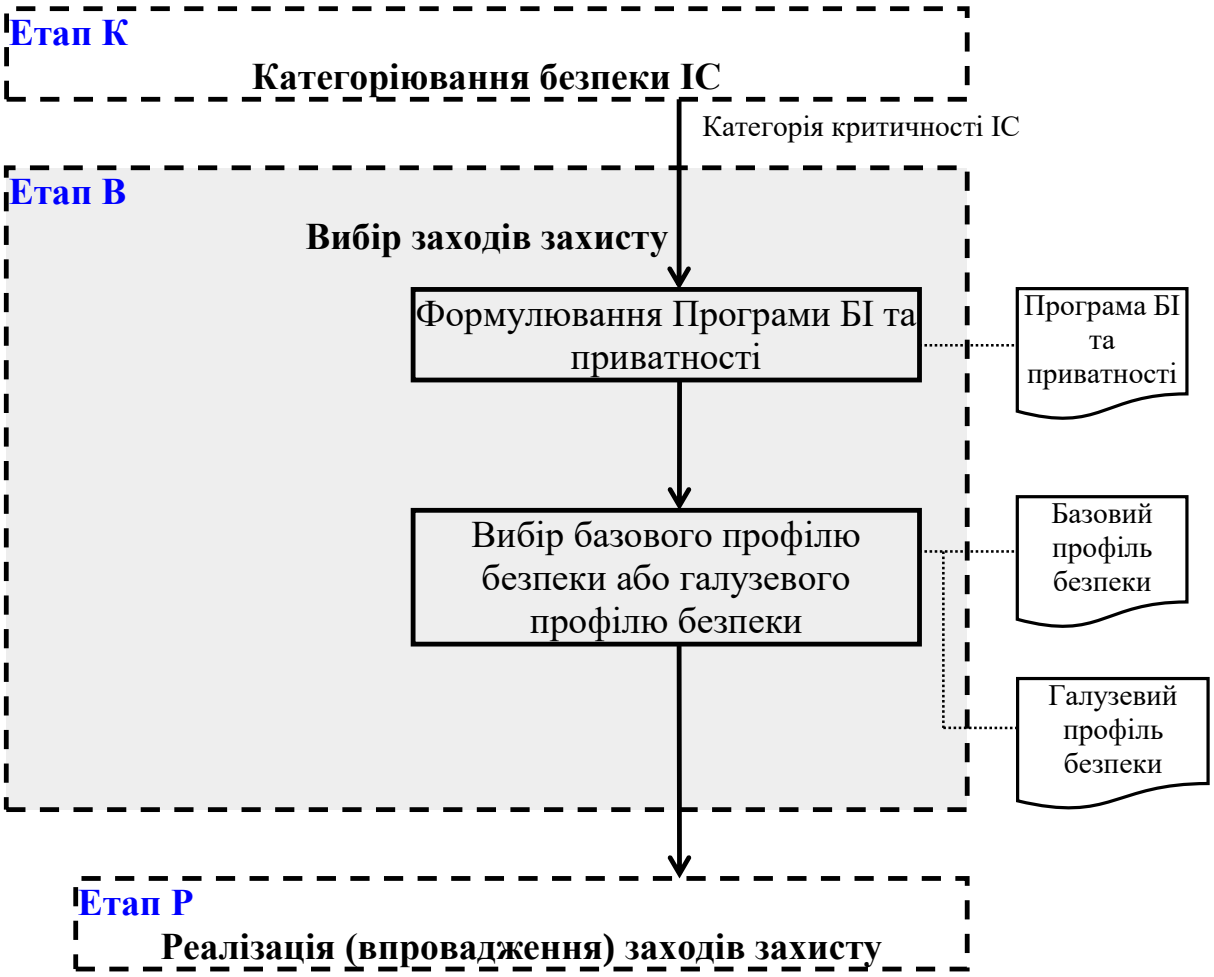


Рисунок 7.2 — Порядок вибору (обґрунтування) профілю безпеки

Категоріювання безпеки відбувається у порядку, встановленому в НД ТЗІ «Порядок категоріювання безпеки інформаційної системи та інформації».

Реалізація (впровадження) заходів захисту відбувається у порядку, встановленому в НД ТЗІ «Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем».

Розробка галузевого профілю безпеки здійснюється з метою пристосування базового профілю безпеки до вимог безпеки та застосування інформаційних систем у конкретній галузі.

У певних ситуаціях організаціям необхідно обґрунтовувати вибір заходів захисту, що враховують специфічні вимоги, технології або унікальні функції/завдання робочого середовища. Організація може вирішити встановити набір заходів захисту для особливих випадків використання інформаційних систем, наприклад, системи хмарних обчислень, промислові системи управління, системи управління транспортними засобами тощо. Тобто можна розробити профілі безпеки для конкретної галузі, технології або специфічних умов функціонування інформаційної системи. Таким чином досягається стандартизовані та раціональні, з точку зору витрат, рішення щодо забезпечення вимог конфіденційності, цілісності та доступності в інформаційних системах конкретної галузі або технології. Саме для розв’язання таких потреб призначена концепція галузевого профілю безпеки.

Галузевий профіль безпеки — це визначений набір заходів захисту, посилень заходів захисту та додаткових рекомендацій, отриманих на основі налаштування й уточнення базового профілю безпеки з урахуванням особливостей галузі. Галузевий профіль безпеки містить

налаштування та уточнення заходів захисту базового профілю безпеки, додаткові заходи захисту (або обґрунтоване вилучення заходів захисту), які обґрунтовані для конкретних технологій, робочих середовищ, типів інформаційних систем, типів функцій/завдань/операцій, режимів роботи, які є специфічними для галузі, та встановлених галузевими стандартами або нормативними документами вимог. Також галузевий профіль безпеки містить заходи захисту зі встановленими значеннями параметрів і вибраними посиленнями, які придатні для зацікавлених сторін галузі.

Галузевий профіль безпеки надає можливість досягти консенсусу серед зацікавлених сторін та розробити заходи захисту для організацій і систем, що підтримують дуже специфічні функції, функціонують у конкретних робочих середовищах, ситуаціях, умовах.

Галузевий профіль безпеки розробляється для:

- конкретної галузі, наприклад охорона здоров'я, фінанси, енергетика, транспорт тощо;
- конкретної інформаційної технології, наприклад хмарні обчислення, мобільні технології, smart-grid системи тощо;
- специфічних робочих середовищ, наприклад космічні, морські, польові тощо;
- конкретних типів систем і режимів роботи, наприклад промислове/технологічне управління, системи озброєння, автономні системи, системи IT тощо;
- конкретних призначень, функцій або завдань, наприклад дослідження, розробка, тестування та оцінювання систем тощо;
- задоволення конкретних законодавчих або нормативних вимог, наприклад захист персональних даних, страхування тощо.

Галузевий профіль безпеки може бути використаний організацією для впровадження дисциплінованого та структурованого підходу до розробки цільових профілів безпеки інформаційних систем. Таким чином, галузевий профіль безпеки є відправною точкою для налаштування та створення цільового профілю безпеки інформаційних систем, що є специфічними для цієї галузі. Галузеві профілі безпеки розробляються уповноваженими органами галузі та погоджуються з уповноваженим органом у сфері захисту інформації.

Порядок розробки цільового та адаптованого профілів безпеки визначається окремомим НД ТЗІ.

### 7.2 Застосування механізму компенсації

Профіль безпеки може містити заходи захисту, які не можуть бути реалізовані (впроваджені) в інформаційній системі. Наприклад, висока вартість, великі терміни реалізації, відсутність компетенцій для експлуатації, відсутність апробованих рішень тощо. У таких випадках дозволяється замінити відповідні заходи захисту на інші заходи — компенсуючи заходи захисту. Для розробки компенсуючих заходів захисту необхідно розглянути:

- вимоги нормативної бази у сфері захисту інформації;
- міжнародні, національні та галузеві стандарти у сфері безпеки інформації;
- результати власних розробок (науково-дослідні, дослідно-конструкторські роботи).

Використання компенсуючих заходів захисту має бути обґрунтовано. При цьому:

- викладаються причини неможливості впровадження (реалізації) заходу захисту з профілю безпеки;
- здійснюється порівняння можливостей заходу захисту, що виключено, з компенсуючим заходом захисту;
- надається опис компенсуючого заходу захисту у форматі (шаблоні) опису заходів захисту, що встановлений у цьому документі;
- надається аргументація достатності компенсуючого заходу захисту в рамках визначеної моделі загроз.

Оцінювання достатності й адекватності компенсуючого заходу захисту здійснюється на етапі оцінювання впровадження заходів захисту.

## 8 Гарантії безпеки та довірчість

Довірчість — це гідний довіри ступінь реалізації (впровадження) заходів захисту, необхідних для задоволення вимог безпеки для певної системи, підсистеми, компоненту, мережі, функції, процесу або організації в цілому.

Довірчість ґрунтується на двох фундаментальних компонентах — функціональність і гарантії.

Функціональність визначається в термінах властивостей безпеки та приватності, функцій, механізмів, послуг, процедур і архітектури, що реалізовані в складі інформаційних систем, які використовують організації, а також у середовищах, у яких ці інформаційні системи функціонують.

Гарантії безпеки — це міра впевненості в тому, що функції безпеки (заходи захисту) інформаційної системи реалізовані правильно, працюють за призначенням і досягають бажаного результату стосовно додержання вимог безпеки та приватності.

Заходи захисту, що визначені в цьому документі, стосуються як функціональності, так і гарантій безпеки. Деякі заходи захисту насамперед орієнтовані на забезпечення функціональності. Інші заходи захисту в основному зосереджені на досягнення гарантій безпеки. Певні заходи захисту можуть бути спрямовані як на забезпечення функціональності, так і гарантій. Організації можуть визначати заходи, які пов’язані з гарантіями, для створення відповідних і достовірних доказів (свідчень) про функціональність своїх інформаційних систем. Ці докази необхідні для отримання певної міри впевненості, що інформаційні системи ефективно задовольняють заявленим вимогам щодо безпеки та приватності.

Інформація щодо спрямованості конкретного заходу захисту надана в Додатку Б.

## 9 Перелік заходів захисту

У цьому розділі наведений повний перелік заходів захисту (без посилень), представлених у нормативному документі.

Для зручності використання нормативного документа (зокрема в електронній формі) у таблиці 9.1 надається перелік заходів захисту з указанням номерів сторінок основних класів заходів захисту.

Таблиця 9.1 — Перелік заходів захисту

| Шифр | Назва | Стор. |
|---|---|---|
| УПРАВЛІННЯ ДОСТУПОМ (AC) | | 20 |
| AC-1 | Політика та процедури управління доступом | |
| AC-2 | Управління обліковими записами | |
| AC-3 | Забезпечення доступу | |
| AC-4 | Управління інформаційними потоками | |
| AC-5 | Розмежування обов’язків | |
| AC-6 | Мінімізація повноважень | |
| AC-7 | Невдалі спроби входу в систему | |
| AC-8 | Попередження про використання системи | |
| AC-9 | Сповіщення про попередній вхід (доступ) | |
| AC-10 | Управління паралельною сесією | |
| AC-11 | Блокування пристрою | |
| AC-12 | Припинення сеансу | |
| AC-13 | Нагляд та огляд — управління доступом | |
| AC-14 | Дозволені дії без ідентифікації або автентифікації | |
| AC-15 | Автоматизоване маркування | |

## 10 Каталог заходів захисту

## 10.1 Клас заходів захисту AC — УПРАВЛІННЯ ДОСТУПОМ

### AC-1 ПОЛІТИКА ТА ПРОЦЕДУРИ УПРАВЛІННЯ ДОСТУПОМ

Заходи захисту:

a. Розробити, задокументувати та поширити [*Призначення: серед визначеного організацією персоналу або ролей*]:

1. [*Вибір (один або декілька): Рівень організації; Рівень місії/бізнес-процесу; рівень системи*] політики контролю доступу, яка:

(a) містить мету, сферу застосування, ролі, відповідальність, зобов’язання керівництва, координацію між організаційними підрозділами та систему контролю відповідності (compliances);

(b) відповідає чинному законодавству, нормативним документам, директивам, нормам, політикам, стандартам і керівним документам.

2. Процедури, що сприяють реалізації політики управління доступом і відповідних заходів управління доступом.

b. Призначити на посаду [*Призначення: визначену організацією посадову особу*] для управління, документування і розповсюдження політики та процедур контролю доступом.

c. Переглянути та оновити:

1. поточну політику управління доступом [*Призначення: з визначеною організацією частотою*] та [*Призначення: події, визначені організацією*];

2. поточні процедури управління доступом [*Призначення: з визначеною організацією частотою*] та [*Завдання: події, визначені організацією*].

Рекомендації з реалізації: Цей захід захисту впроваджує політику та процедури з ефективної реалізації заходів захисту та посилення заходів захисту, пов'язаних з управлінням доступом. Важливим фактором формування політики та процедур управління доступом є стратегія управління ризиками. Комплексні політики та процедури дозволяють забезпечити виконання вимог безпеки та приватності. Політики та процедури безпеки, які сформовані на організаційному рівні, можуть вимагати розроблення окремих політик і процедур для компонентів складної системи. Політика конкретного компонента системи може бути включена до загальної політики безпеки або бути окремим документом (залежно від рівня складності організаційної структури). Аналогічно, процедури безпеки можуть бути запроваджені на організаційному рівні та поширюватися на всі компоненти (підсистеми) інформаційної системи, або, за необхідності, бути розробленими для специфічних компонентів. Процедури мають описувати спосіб реалізації політик, а також засоби контролю за їх виконанням. Процедури можуть бути задокументовані в планах захисту інформації та персональних даних або в окремих документах. Події, які можуть спричинити оновлення політики та процедур контролю доступу, включають висновки оцінки або аудиту, інциденти чи порушення безпеки або зміни в законах, розпорядженнях, директивах, постановах, політиках, стандартах і вказівках. Просте повторне встановлення засобів контролю не є заходом чи процедурою організаційної політики.

Пов'язані заходи: IA-1, PM-9, PM-24, PS-8, SI-12.

Посилення заходів: Немає.

Посилання: [OMB A-130], [SP 800-12], [SP 800-30], [SP 800-39], [SP 800-100], [IR 7874].

## AC-2 УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ

Заходи захисту:

a. Визначити та задокументувати типи облікових записів системи, дозволених для використання в ІС для підтримки цілей, завдань, функцій і процесів організації.

b. Призначити менеджерів облікових записів для управління системними обліковими записами.

c. Створити умови для групового та рольового членства.

d. Визначити авторизованих користувачів інформаційної системи, членство в групі та ролі, а також дозволи доступу (наприклад, привілеї) та інші атрибути (за потреби) для кожного облікового запису.

e. Вимагати схвалення [*Призначення: визначеною організацією відповідальною особою або роллю*] запитів на створення облікових записів системи.

f. Створювати, активувати, змінювати, деактивувати та видаляти системні облікові записи відповідно до [*Призначення: визначених організацією політики, процедур та умов*].

g. Впровадити моніторинг використання облікових записів системи.

h. Повідомляти адміністраторів облікових записів у межах [*Призначення: визначеного організацією часового періоду для кожної ситуації*]:

1. коли облікові записи більше не потрібні;

2. коли користувачі звільнені чи переведені;

3. коли використовуються індивідуальні системи або наявні зміни, які потребують нових знань.

i. Авторизувати доступ до системи на основі:

1. Дійсної авторизації доступу.

2. Передбачуваного використання системи.

3. Інших атрибутів, що вимагаються організацією.

j. Проводити перегляд облікових записів на відповідність вимогам управління обліковими записами з [*Призначення: визначеною організацією частотою*].

k. Впровадити процес повторного випуску облікових даних спільного/групового облікового запису (якщо він буде розгорнутий), коли особи виходять з групи.

l. Узгодити процеси управління обліковими записами з процесами звільнення та переводу (передачі повноважень) персоналу.

Рекомендації з реалізації: Типи облікових записів системи містять, наприклад, індивідуальний, спільний, груповий, системний, гостьовий, анонімний, запис розробника/виробника/постачальника, екстрений, тимчасовий. Ідентифікація авторизованих користувачів системи та специфікація привілеїв доступу мають відображати вимоги, що містяться в інших елементах управління. Користувачі, які потребують адміністративних привілеїв на облікових записах системи, повинні проходити додаткову перевірку відповідальною за затвердження таких облікових записів особою (власник системи або адміністратор безпеки). Організації можуть визначати привілеї доступу чи інші атрибути безпосередньо за обліковим записом, типом облікового запису або комбінацією обох. Інші атрибути, необхідні для авторизації доступу, містять, наприклад, обмеження часу чи дня тижня. Для визначення інших атрибутів облікових записів організаціям необхідно враховувати системні вимоги та вимоги організації. Неврахування цих факторів може вплинути на доступність системи.

Тимчасові та екстрені облікові записи призначені для короткострокового використання. Тимчасові облікові записи виступають частиною стандартних процедур активації облікових записів, коли виникає потреба в короткострокових облікових

записах, без вимоги негайності активації запису. Екстрені облікові записи можуть бути створені у відповідь на кризові ситуації та потребують швидкої активації. Тому активація екстреного облікового запису може обійти звичайні процеси авторизації облікового запису. Треба зауважити, що екстрені й тимчасові облікові записи не слід плутати з обліковими записами, які рідко використовуються (наприклад, локальні облікові записи для доступу до спеціальних завдань). Такі облікові записи залишаються доступними й не потребують автоматичного відключення чи видалення. Умови деактивації облікових записів містять, наприклад, ситуації, коли спільні/групові, резервні або тимчасові облікові записи більше не потрібні; чи коли персонал переводиться або звільняється (складає повноваження).

Пов'язані заходи: AC-3, AC-5, AC-6, AC-17, AC-18, AC-20, AC-24, AU-9, CM-5, IA-2, IA-8, MA-3, MA-5, PE-2, PL-4, PS-2, PS-4, PS-5, PS-7, SC-7, SC-13, SC-37.

Посилення заходів:

(1) УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ - АВТОМАТИЗОВАНЕ УПРАВЛІННЯ СИСТЕМНИМИ ОБЛІКОВИМИ ЗАПИСАМИ

Використовувати автоматизовані механізми для підтримки управління системними обліковими записами.

Рекомендації з реалізації: Використання автоматизованих механізмів може охоплювати, наприклад, використання електронної пошти чи текстових повідомлень для автоматичного сповіщення менеджерів облікових записів про припинення роботи користувачів; використання системи моніторингу активності облікових записів і використання телефонного сповіщення для повідомлення про нетипове використання облікового запису.

Пов'язані заходи: Немає.

(2) УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ - ВИДАЛЕННЯ ТИМЧАСОВИХ ТА ЕКСТРЕНИХ ОБЛІКОВИХ ЗАПИСІВ

Автоматично [*Вибір: видаляти, деактивувати*] тимчасові та екстрені облікові записи після [*Призначення: визначеного організацією часового періоду для кожного типу облікових записів*].

Рекомендації з реалізації: Це посилення вимагає автоматичного видалення або деактивацію тимчасових і екстрених облікових записів після того, як минув попередньо визначений період часу, без участі системного адміністратора. Автоматичне видалення або деактивація облікових записів забезпечує послідовну реалізацію політики управління обліковими записами.

Пов'язані заходи: Немає.

(3) УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ - ДЕАКТИВАЦІЯ ОБЛІКОВИХ ЗАПИСІВ

Автоматично деактивувати облікові записи коли:

a) їх строк дії минув;

b) вони більше не пов'язані з користувачем;

c) вони порушують організаційну політику;

d) вони були неактивними впродовж [*Призначення: визначеного організацією періоду часу*].

Рекомендації з реалізації: Вимкнення прострочених, неактивних або іншим чином аномальних облікових записів підтримує концепцію найменших привілеїв і найменших функціональних можливостей, які зменшують поверхню атаки системи.

Пов'язані заходи: Немає.

(4) УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ - ДІЇ ПРИ АВТОМАТИЗОВАНОМУ АУДИТІ

Проводити автоматизований аудит створення, модифікації, активації, деактивації та видалення облікових записів і сповіщення про дії.

Рекомендації з реалізації: Записи аудиту управління обліковими записами визначаються відповідно до AU-2 та переглядаються, аналізуються і звітуються відповідно до AU-6.

Пов'язані заходи: AU-2, AU-6.

(5) УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ - ВИХІД ІЗ СИСТЕМИ ЗА ВІДСУТНОСТІ АКТИВНОСТІ

Вимагати від користувачів виходити із системи, коли [*Призначення: вичерпано визначений організацією період часу очікування або опис того, коли необхідно вийти із системи*].

Рекомендації з реалізації: Це посилення вимагає від користувачів виходити із системи в разі перевищення визначеного періоду бездіяльності. Автоматичний примусовий вихід із системи бездіяльності регулюється AC-11.

Пов'язані заходи: AC-11.

(6) УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ - ДИНАМІЧНЕ УПРАВЛІННЯ ПРИВІЛЕЯМИ

Реалізувати такі можливості динамічного управління привілеями: [*Призначення: визначений організацією перелік можливостей динамічного управління привілеями*].

Рекомендації з реалізації: На відміну від звичайних підходів до управління доступом, які використовують статичні облікові записи системи та попередньо визначені привілеї користувачів, підходи до динамічного управління доступу залежать від часових обмежень (наприклад управління доступом на основі атрибутів — ABAC). Хоча ідентичність користувачів залишається постійною протягом часу, їхні привілеї змінюються залежно від поточних вимог та операційних потреб організацій. Динамічне управління привілеями може містити, наприклад, негайне скасування привілеїв користувачів, без необхідності завершення та перезапуску сеансів. Динамічне управління привілеями також може містити ті механізми, які змінюють привілеї користувача на основі динамічних правил і не вимагають редагування конкретних профілів користувачів. До прикладів належать автоматичні коригування привілеїв користувачів, якщо вони працюють поза звичайним

робочим часом, змінюються їхні робочі функції або якщо системи перебувають у позаштатних умовах функціонування. Це посилення заходу також охоплює випадки зміни ключів шифрування.

Пов'язані заходи: AC-16.

(7) УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ - СХЕМИ, ЗАСНОВАНІ НА РОЛЯХ

a) Створювати й адмініструвати привілейовані облікові записи користувачів відповідно до схеми доступу на основі ролей (role-based), яка реалізує дозволений доступ до системи та призначення привілеїв для ролей.

b) Проводити моніторинг призначення привілейованих ролей.

c) Відстежувати зміни ролей або атрибутів.

d) Скасовувати доступ, коли призначені привілейовані ролі більше не потрібні.

Рекомендації з реалізації: Привілейовані ролі — це визначені організацією ролі, що призначені особам і дозволяють цим особам виконувати певні функції безпеки, які звичайні користувачі не мають права виконувати. Ці привілейовані ролі містять, наприклад, управління ключами, управління обліковими записами, мережеве та системне управління, адміністрування баз даних і вебадміністрування. Схема доступу на основі ролей організовує дозволений доступ до системи та привілеїв в ролі. Навпаки, схема доступу на основі атрибутів визначає дозволений доступ до системи та привілеїв на основі атрибутів.

Пов'язані заходи: Немає.

(8) УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ - ДИНАМІЧНЕ УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ

Створювати, активувати, управляти та деактивувати [*Призначення: системні облікові записи, визначені організацією*] динамічно.

Рекомендації з реалізації: Підходи до динамічного створення, активації, управління та деактивації облікових записів системи чи служб/застосунків покладаються на автоматичне обслуговування облікових записів суб'єктів, які раніше не були відомі безпосередньо під час функціонування. Динамічне управління цих облікових записів планується шляхом встановлення довірчих відносин, ділових правил і механізмів з відповідними органами для підтвердження відповідних дозволів і привілеїв.

Пов'язані заходи: AC-16.

(9) УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ - ОБМЕЖЕННЯ НА ВИКОРИСТАННЯ СПІЛЬНИХ ТА ГРУПОВИХ ОБЛІКОВИХ ЗАПИСІВ

Використовувати лише ті спільні та групові облікові записи, які відповідають [*Призначення: визначеним організацією умовам для створення спільних та групових облікових записів*].

Рекомендації з реалізації: Перш ніж дозволити використання спільних або групових облікових записів, необхідно проаналізувати ризики, які пов'язані з відсутністю підзвітності таких облікових записів.

Пов'язані заходи: Немає.

(10) УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ - ЗМІНА ДАНИХ СПІЛЬНИХ ТА ГРУПОВИХ ОБЛІКОВИХ ЗАПИСІВ

[Вилучено до AC-2k.].

(11) УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ - УМОВИ ВИКОРИСТАННЯ

Забезпечити дотримання [*Призначення: обставин та/або умов використання, визначених організацією*] для [*Призначення: визначених організацією облікових записів системи*].

Рекомендації з реалізації: Це посилення допомагає застосувати принцип мінімізації привілеїв, підвищити підзвітність користувачів та забезпечити більш ефективний моніторинг облікових записів. Такий моніторинг містить, наприклад, сповіщення про використання облікового запису поза визначеними параметрами. При цьому можуть бути описані конкретні умови або обставини, за яких системні облікові записи можуть використовуватися (наприклад, лише в певні дні тижня, протягом певного часу, тощо).

Пов'язані заходи: Немає.

(12) УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ - МОНІТОРИНГ НЕТИПОВОГО ВИКОРИСТАННЯ ОБЛІКОВИХ ЗАПИСІВ

a) Проводити моніторинг облікових записів системи на [*Призначення: визначене організацією нетипове використання*].

b) Повідомляти про нетипове використання облікових записів системи [*Призначення: визначеного організацією персоналу або ролей*].

Рекомендації з реалізації: До нетипового використання належить, наприклад, доступ до систем у певний час доби та день місяця чи з локацій, які не відповідають робочим функціям персоналу. Моніторинг облікових записів може ненавмисно створити ризики приватності. Дані, зібрані для виявлення нетипового використання, можуть виявити раніше невідому інформацію про поведінку людей. Ці ризики мають бути оціненими та задокументованими. На основі таких оцінок мають бути ухвалені рішення відповідно до чинної програми (концепції) приватності.

Пов'язані заходи: AU-6, AU-7, CA-7, IR-8, SI-4.

(13) УПРАВЛІННЯ ОБЛІКОВИМИ ЗАПИСАМИ - ДЕАКТИВАЦІЯ ОБЛІКОВИХ ЗАПИСІВ ОСІБ З ВИСОКИМ РІВНЕМ РИЗИКУ

Деактивувати облікові записи користувачів, які становлять значний ризик, у межах [*Призначення: визначеного організацією періоду часу*] після виявлення ризику.

Рекомендації з реалізації: Користувачами, які становлять значний ризик для

організацій, є особи, щодо яких наявні достовірні докази, що вказують на їхній намір використовувати або свій санкціонований доступ до систем для заподіяння шкоди напряму, або через посередників. Такий ризик містить можливі несприятливі наслідки для організаційних операцій і активів, окремих людей, інших організацій чи держави. Для своєчасного здійснення цього посилення необхідна тісна координація та співпраця між посадовими особами, адміністраторами системи та менеджерами з управління персоналом.

Пов'язані заходи: AU-6, SI-4.

Посилання: [SP 800-162], [SP 800-178], [SP 800-192].

## AC-3 ЗАБЕЗПЕЧЕННЯ ДОСТУПУ

Заходи захисту:
Застосовувати затверджені повноваження для логічного доступу до інформації та ресурсів системи відповідно до чинної політики (правил) управління доступом.

Рекомендації з реалізації: Політика управління доступом контролює доступ між активними об'єктами чи суб'єктами (тобто користувачами або процесами, що діють від імені користувачів) та пасивними об'єктами чи об'єктами (тобто пристроями, файлами, записами, доменами) в системах організації. Окрім забезпечення авторизованого доступу на системному рівні та визнання того, що системи можуть розміщувати багато застосунків і служб для підтримки операцій, механізми забезпечення доступу також можуть бути використані на рівні застосунків і послуг для забезпечення підвищеної інформаційної безпеки.

Пов'язані заходи: AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AC-24, AC-25, AT-3, AU-9, CA-9, CM-5, CM-11, IA-2, IA-5, IA-6, IA-7, IA-11, MA-3, MA-4, MA-5, MP-4, PM-2, PS-3, PT-2, PT-3, SA-17, SC-2, SC-3, SC-4, SC-12, SC-13, SC-28, SC-31, SC-34, SI-4, SI-8.

Посилення заходів:

(1) ЗАБЕЗПЕЧЕННЯ ДОСТУПУ - ОБМЕЖЕНИЙ ДОСТУП ДО ПРИВІЛЕЙОВАНИХ ФУНКЦІЙ

[Вилучено: включено до AC-6].

(2) ЗАБЕЗПЕЧЕННЯ ДОСТУПУ - ПОДВІЙНА АВТОРИЗАЦІЯ

Забезпечити подвійну авторизацію для [*Призначення: визначених організацією привілейованих команд та/або інших дій, визначених організацією*].

Рекомендації з реалізації: Подвійна авторизація являє собою двоосібний контроль. Механізми подвійної авторизації вимагають схвалення двох уповноважених осіб для виконання дії. Механізми подвійної авторизації повинні бути спрощені у випадках, коли необхідні негайні реакції для забезпечення громадської та екологічної безпеки.

Пов'язані заходи: CP-9, MP-6.

(3) ЗАБЕЗПЕЧЕННЯ ДОСТУПУ - МАНДАТНЕ УПРАВЛІННЯ ДОСТУПОМ

Застосовувати *[Призначення: визначену організацією мандатну (mandatory) політику управління доступом]* щодо всіх суб'єктів і об'єктів доступу, у яких політика:

(a) одноманітно застосовується для всіх суб'єктів і об'єктів у межах системи;

(b) вказує, що суб'єкт, якому було надано доступ до інформації, обмежений у виконанні будь-якої з таких дій:

(1) передача інформації неавторизованим суб'єктам або об'єктам;

(2) надання іншим суб'єктам привілеїв;

(3) зміна одного чи декількох атрибутів безпеки суб'єкта, об'єкта, системи або компонентів системи;

(4) вибір атрибутів безпеки та значень атрибутів, які повинні бути пов'язані з новоствореними або зміненими об'єктами;

(5) зміна правил, що регулюють управління доступом;

(c) має бути вказано, що [*Призначення: визначеним організацією суб'єктам*] можуть бути явно надані [*Призначення: визначені організацією привілеї*], так що вони не обмежуються будь-яким з перелічених вище обмежень.

Рекомендації з реалізації: Обов'язковий (мандатний) контроль доступу — це тип недискреційного управління доступом. Вищезазначений клас обов'язкових політик контролю доступу обмежує дії, які суб'єкти можуть вжити з інформацією, отриманою з об'єктів даних, до яких їм уже надано доступ (наприклад обмеження передачі інформації неавторизованим об'єктам). Цей клас обов'язкових політик контролю доступу також обмежує дії, які суб'єкти можуть вжити щодо розповсюдження привілеїв контролю доступу, тобто суб'єкт з привілеєм не може передавати цей привілей іншим суб'єктам. Політика має поширюватися на всі суб'єкти та об'єкти системи (забезпечення цієї рекомендації можливе з використанням AC-25). Дія політики обмежена межами системи (тобто, як тільки інформація передається поза межі системи, можуть знадобитися додаткові засоби для того, щоб обмеження щодо інформації залишалися в силі).

Описані вище довірені суб'єкти отримують привілеї, що відповідають поняттю мінімізації привілею (див. AC-6). Довіреним суб'єктам надаються лише мінімальні привілеї щодо вищезазначеної політики, які необхідні для задоволення потреб організації. Цей захід є найбільш ефективним за умови, що наявний відповідний мандат, який встановлює політику доступу до інформації з обмеженим доступом, а користувачі системи не мають права доступу до всієї такої інформації, яка перебуває в системі. Цей захід може впроваджуватися спільно з AC-3(4). Суб'єкт, діяльність якого обмежена політикою відповідно до цього заходу, може діяти за менш жорстких обмежень AC-3 (4), але політика відповідно до цього заходу має перевагу над менш жорсткими обмеженнями AC-3 (4). Наприклад, обов'язкова політика контролю доступу накладає обмеження щодо передачі інформації іншому суб'єкту, який не має відповідних прав доступу. AC-3 (4) дозволяє суб'єкту передавати інформацію будь-якому іншому суб'єкту, наділеному аналогічними (достатніми для цього) правами.

Пов’язані заходи: SC-7.

(4) ЗАБЕЗПЕЧЕННЯ ДОСТУПУ - ДИСКРЕЦІЙНЕ УПРАВЛІННЯ ДОСТУПОМ

Застосовувати [*Призначення: визначену організацією дискреційну політику управління доступом*] щодо визначених суб’єктів і об’єктів доступу, для яких політика визначає, що суб’єкт, якому було надано доступ до інформації, може виконати одну чи більше з таких дій:

(a) передача інформацію будь-яким іншим суб’єктам чи об’єктам;

(b) призначення своїх привілей іншим суб’єктам;

(c) зміна атрибутів безпеки суб’єктів, об’єктів, систем або компонентів системи;

(d) вибір атрибутів безпеки, які будуть пов’язані з новоствореними або переглянутими об’єктами;

(e) зміна правил, що регулюють управління доступом.

Рекомендації з реалізації: Реалізація дискреційної політики контролю доступу не обмежує суб’єкт у діях, які він може вживати з інформацією, до якої йому вже надано доступ. Таким чином, суб’єктам, яким надано доступ до інформації, можуть передавати (тобто суб’єкти мають право на передання) інформацію іншим суб’єктам або об’єктам. Це посилення може впроваджуватися спільно з AC-3(3). Суб’єкт, обмежений у своїй діяльності політикою AC-3(3) та AC-3(15), все ще може діяти в умовах менш жорстких обмежень цього посилення. Тому, хоча AC-3 (3) накладає обмеження, що не дозволяють суб’єкту передавати інформацію іншому суб’єкту, який не має відповідних прав доступу, AC-3(4) дозволяє суб’єкту передавати інформацію будь-якому суб’єкту з однаковим рівнем прав доступу. Дія політики обмежена межами системи. Після передачі інформації за межі системи, можуть знадобитися додаткові засоби для того, щоб обмеження щодо інформації залишалися в силі. Хоча більш традиційні визначення дискреційного контролю доступу вимагають контролю доступу, заснованого на ідентичності, ця вимога не є обов’язковою для використання дискреційного контролю доступу.

Пов’язані заходи: Немає.

(5) ЗАБЕЗПЕЧЕННЯ ДОСТУПУ - ІНФОРМАЦІЯ ЩОДО БЕЗПЕКИ

Запобігати доступу до [*Призначення: інформації щодо безпеки, яка визначена організацією*], за винятком випадків, коли наявні безпечні неробочі стани системи.

Рекомендації з реалізації: Інформація щодо безпеки — це будь-яка інформація всередині систем, яка може вплинути на роботу функцій безпеки чи надання послуг з гарантування безпеки таким чином, що може призвести до неприйняття політик безпеки системи або порушення конфіденційності коду та даних. Інформація щодо безпеки містить, наприклад, правила фільтрації маршрутизаторів/брандмауерів, інформацію управління криптографічними ключами, параметри конфігурації служб безпеки та списки контролю доступу. Безпечні, непрацездатні стани системи охоплюють час, коли система не виконує функції, пов’язані з діяльністю організації; наприклад система працює в офлайн-режимі для обслуговування, усунення несправностей тощо.

Пов’язані заходи: CM-6, SC-39.

(6) ЗАБЕЗПЕЧЕННЯ ДОСТУПУ - ЗАХИСТ ІНФОРМАЦІЇ КОРИСТУВАЧА ТА СИСТЕМИ

[Вилучено: включено до MP-4 та SC-28].

(7) ЗАБЕЗПЕЧЕННЯ ДОСТУПУ - УПРАВЛІННЯ ДОСТУПОМ НА ОСНОВІ РОЛЕЙ

Застосовувати політику управління доступом на основі ролей щодо визначених суб’єктів і об’єктів та управління доступом на основі [*Призначення: визначених організацією ролей та користувачів, уповноважених приймати такі ролі*].

Рекомендації з реалізації: Контроль доступу на основі ролей (RBAC) — це політика управління доступом, яка обмежує доступ до системи для авторизованих користувачів. Конкретні ролі можуть створюватися на основі функцій завдань і дозволів (тобто привілеїв) для виконання необхідних операцій у системах, пов’язаних з визначеними організацією ролями. Коли користувачу надається організаційна роль, він успадковує права, визначені для цієї ролі. RBAC спрощує адміністрування привілеїв, оскільки привілеї не присвоюються безпосередньо кожному користувачеві (така кількість користувачів може бути досить великою), а натомість набуваються за допомогою розподілу ролей. RBAC може бути реалізований як обов’язкова або дискреційна форма контролю доступу. При застосуванні RBAC з обов’язковим контролем доступу, сфера діяльності суб’єктів і об’єктів, на які поширюється політика визначається вимогами AC-3 (3).

Пов’язані заходи: PE-2.

(8) ЗАБЕЗПЕЧЕННЯ ДОСТУПУ - АНУЛЮВАННЯ ПРАВ ДОСТУПУ

Здійснювати анулювання прав доступу в результаті змін атрибутів безпеки суб’єктів і об’єктів на основі *[Призначення: визначених організацією правил, що регулюють терміни скасування прав доступу]*.

Рекомендації з реалізації: Анулювання правил доступу може відрізнятися залежно від типу анульованого доступу. Наприклад, якщо суб’єкт (тобто користувач або процес) був видалений з групи, доступ може не бути анульовано до наступного відкриття об’єкта чи наступного разу, коли суб’єкт спробує отримати новий доступ до об’єкта. Анулювання на основі зміни міток безпеки може набрати чинності негайно. Якщо система не може забезпечити можливість негайного анулювання доступу, для цього мають бути впровадженні додаткові механізми (у разі, коли негайне анулювання необхідне).

Пов’язані заходи: Немає.

(9) ЗАБЕЗПЕЧЕННЯ ДОСТУПУ - КЕРОВАНА ПЕРЕДАЧА (ПУБЛІКАЦІЯ) ІНФОРМАЦІЇ

Передавати (публікувати) інформацію за межами встановленої межі системи можливо, якщо:

a) Приймальна [*Призначення*: *визначена організацією система або компонент системи*] забезпечує [*Призначення: визначені організацією заходи безпеки*];

b) [*Призначення: визначені організацією заходи безпеки*] використовуються для підтвердження відповідності інформації, призначеної для керованих передач (публікації).

Рекомендації з реалізації: Система може забезпечити безпеку організаційної інформації лише у своїх межах. Для забезпечення належного захисту інформації після її передачі поза встановлені межі системи можливо, знадобиться додатковий контроль. У ситуаціях, коли система не в змозі визначити адекватність захисту, що надається суб'єктами за її межами, як пом'якшувальний контроль можуть бути застосовані процедурні заходи. Засоби, що використовуються для визначення достатності рівня безпеки, що надаються зовнішніми системами, можуть містити, наприклад: проведення перевірок або періодичні випробування та оцінювання; встановлення угод між організацією та її партнерами; чи якийсь інший процес. Засоби, що використовуються зовнішніми організаціями для захисту отриманої інформації, можуть відрізнятися від тих заходів, які впроваджені в самій системі; вони мають бути достатніми для забезпечення послідовного вирішення положень політики безпеки для захисту інформації.

Це посилення вимагає від систем використання технічних чи процедурних засобів для перевірки інформації перед передаванням за власні межі. Наприклад, якщо система передає інформацію, яка належить системі іншої організації, необхідно застосовувати технічні засоби для перевірки відповідності атрибутів безпеки приймальної системи відповідно до цієї експортованої інформації.

Пов'язані заходи: CA-3, PT-7, PT-8, SA-9, SC-16.

(10) ЗАБЕЗПЕЧЕННЯ ДОСТУПУ - ПЕРЕГЛЯД АУДИТОМ МЕХАНІЗМІВ КОНТРОЛЮ ДОСТУПУ

Застосувати перегляд аудитом механізмів автоматизованого управління доступу при [*Призначення: визначених організацією умовах] [Призначення: визначеними організацією ролями*].

Рекомендації з реалізації: У певних ситуаціях, наприклад, коли є загроза життю людини або здатності організації виконувати критичні функції, можуть знадобитися механізми контролю доступу. Перелік таких ситуацій є вичерпним та визначається конкретними організаціями.

Пов'язані заходи: AU-2, AU-6, AU-10, AU-12, AU-14.

(11) ЗАБЕЗПЕЧЕННЯ ДОСТУПУ - ОБМЕЖЕННЯ ДОСТУПУ ДО СПЕЦІАЛЬНОЇ ІНФОРМАЦІЇ

Обмежити прямий доступ до сховищ даних, що містять [*Призначення: визначені організацією типи інформації*].

Рекомендації з реалізації: Це посилення покликане забезпечити гнучкість контролю доступу до конкретних фрагментів інформації всередині системи. Наприклад, доступ на основі ролей може бути використаний для отримання лише певного набору ідентифікаційної інформації з бази даних, а не доступу до бази даних у повному обсязі.

Пов'язані заходи: CM-8, CM-12, CM-13, PM-5.

(12) ЗАБЕЗПЕЧЕННЯ ДОСТУПУ - ВСТАНОВЛЕННЯ ТА ЗАБЕЗПЕЧЕННЯ ДОСТУПУ ДО ЗАСТОСУНКІВ

a) Вимагати від застосунків встановити в процесі інсталяції доступ до таких застосунків системи і функцій: [*Призначення: визначених організацією програм та функції системи*];

b) Впровадити механізм примусового застосування, щоб запобігти доступу, відмінному від заявленого.

c) Схвалити зміни доступу після початкового встановлення застосунків.

Рекомендації з реалізації: Це посилення призначене для програм, які потребують доступу до чинних застосунків і функцій системи, включно з, наприклад, контактами користувачів, глобальною системою позиціювання, камерою, клавіатурою, мікрофоном, контактами чи іншими файлами.

Пов'язані заходи: CM-7.

(13) ЗАБЕЗПЕЧЕННЯ ДОСТУПУ - УПРАВЛІННЯ ДОСТУПОМ НА ОСНОВІ АТРИБУТІВ

Здійснювати політику управління доступу на основі атрибутів (atribute-based) для визначених суб'єктів і об'єктів доступу й управляти доступом на основі [*Призначення: визначених організацією атрибутів для ухвалення рішень про доступ*].

Рекомендації з реалізації: Управління доступом на основі атрибутів (ABAC) — це політика управління доступом, яка обмежує доступ до системи авторизованих користувачів на основі їхніх атрибутів, таких як посадові функції; екологічні ознаки (наприклад час доби); атрибути ресурсу (класифікація документа). Можуть створюватися конкретні правила на основі атрибутів і дозволів (тобто привілеїв) для виконання необхідних операцій у системі, пов'язаних з визначеними атрибутами та правилами. Коли користувачам призначаються атрибути, які визначені в політиці чи правилах, вони можуть отримати доступ до системи з відповідними привілеями або їм може надаватися динамічний доступ до захищеного ресурсу. ABAC може бути реалізований як обов'язкова чи дискреційна форма контролю доступу. У разі використання ABAC з обов'язковим контролем доступу, вимоги AC-3(3) визначають сферу діяльності суб'єктів і об'єктів, на які поширюється політика.

Пов'язані заходи: Немає.

(14) ЗАБЕЗПЕЧЕННЯ ДОСТУПУ - ІНДИВІДУАЛЬНИЙ ДОСТУП

Надайте [*Призначення: механізми, визначені організацією*], щоб дозволити особам мати доступ до певних елементів їх особистої інформації: [*Призначення: елементи, визначені організацією*]

Рекомендації з реалізації: Індивідуальний доступ надає особам можливість переглядати особисту інформацію про них, яка зберігається в записах організації, незалежно від формату. Доступ допомагає людям зрозуміти, як обробляється їх особиста інформація та переконатися, що їхні дані точні.

Механізми доступу можуть включати форми запитів та інтерфейси додатків. Для федеральних агентств процеси приватності можна знайти в системах сповіщень про записи та на вебсайтах агентств. Доступ до певних типів записів може бути невідповідним (наприклад, для федеральних агентств записи правоохоронних органів у системі записів можуть бути звільнені від розголошення відповідно до приватності або вимагати певних рівнів гарантії автентифікації. Персонал організації консультується зі старшою посадовою особою агентства щодо конфіденційності та з юрисконсультантом для визначення відповідних механізмів та прав чи обмежень доступу.

Пов'язані заходи: IA-8, PM-22, PM-20, PM-21, PT-6.

(15) ЗАБЕЗПЕЧЕННЯ ДОСТУПУ - ДИСКРЕЦІЙНИЙ ТА ОБОВ'ЯЗКОВИЙ ДОСТУП

(a) Застосовувати [*Призначення: визначену організацією політику обов'язкового контролю доступу*] до набору охоплених суб'єктів і об'єктів, указаних у політиці;

(b) Застосування [*Призначення: визначена організацією дискреційна політика контролю доступу*] до набору охоплених суб'єктів і об'єктів, указаних у політиці.

Рекомендації з реалізації: Одночасне впровадження політики обов'язкового контролю доступу та політики контролю доступу на власний розсуд може забезпечити додатковий захист від несанкціонованого виконання коду користувачами або процесами, що діють від імені користувачів. Це допомагає запобігти компрометації всієї системи одним скомпрометованим користувачем або процесом.

Пов'язані заходи: SC-2, SC-3, AC-4.

Посилання: [OMB A-130], [SP 800-57-1], [SP 800-57-2], [SP 800-57-3], [SP 800-162], [SP 800-178], [IR 7874].

## AC-4 УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ

Заходи захисту:

Застосувати затверджені повноваження для управління потоком інформації всередині системи та між пов'язаними системами на основі [*Призначення: визначеними організацією політиками управління інформаційним потоком*].

Рекомендації з реалізації: Управління інформаційними потоками регулює межі пересування інформації як всередині системи, так і між взаємопов'язаними системами без явного врахування подальшого доступу до цієї інформації. Обмеження управління потоками охоплюють, наприклад, запобігання передачі інформації в Інтернеті, блокування зовнішнього трафіку, обмеження вебзапитів в Інтернеті, які не відповідають обмеженням внутрішніми проксі-серверами, та обмеження передачі інформації між організаціями на основі структури даних і вмісту. Передача інформації між системами з різними політиками безпеки створює ризик того, що такий режим передачі порушує одну або декілька політик безпеки домену. У таких ситуаціях власники інформації мають надавати вказівки у визначених пунктах впровадження політики між взаємопов'язаними системами. Конкретні архітектурні рішення можуть

застосовуватися в разі, якщо потрібне впровадження певної політики безпеки. Наприклад, за потреби контролю одностороннього інформаційного потоку між двома взаємопов'язаними системами можуть використовуватися апаратні засоби, визначатися атрибути та механізми доступу.

Управління інформаційними потоками має впроваджуватися з урахуванням характеристик інформації, що обробляється, а також із врахуванням інформаційного шляху. Примусові заходи можуть застосовуватися, наприклад, у пристроях захисту периметру, включно з наборами правил, конфігураціями, які обмежують системні послуги, надають можливість фільтрування пакетів на основі заголовка або можливість фільтрації повідомлень на основі вмісту. Надійність таких механізмів має бути визначена за результатами проведеного оцінювання. Посилення заходу (3)-(22) загалом стосуються управління інформаційними потоками, які передаються між декількома системами (вони базуються на глибокому аналізі, вдосконалених методах фільтрації, апаратних рішеннях). Такі можливості можуть бути відсутніми в системах комерційного призначення.

Пов'язані заходи: AC-3, AC-6, AC-16, AC-17, AC-19, AC-21, AU-10, CA-3, CA-9, CM-7, PL-9, PM-24, SA-17, SC-4, SC-7, SC-16, SC-31.

Посилення заходів:

(1) УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - АТРИБУТИ БЕЗПЕКИ ОБ'ЄКТУ

Використовувати [*Призначення: визначені організацією атрибути безпеки*], пов'язані з [*Призначення: визначеними організацією інформацією, джерелами та об'єктами призначення*], щоб запровадити [*Призначення: визначену організацією політику управління потоками інформації*] як основу для ухвалення рішень щодо управління потоками.

Рекомендації з реалізації: Механізми управління інформаційними потоками оперують атрибутами безпеки інформації (вміст і структура даних) та об'єктами джерела та призначення. На основі цих атрибутів визначаються ситуації, які можуть суперечити політикам безпеки. Наприклад, інформаційному об'єкту, який має гриф «таємно», дозволено потік до об'єкта призначення з грифом «таємно», але інформаційному об'єкту з грифом «цілком таємно» заборонено надходити до об'єкта призначення з грифом «таємно». Атрибути безпеки можуть також містити джерела й адреси призначення, використовувані в брандмауерах. Управління потоками за допомогою явних атрибутів безпеки може використовуватися для контролю певних типів інформації.

Пов'язані заходи: Немає.

(2) УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ДОМЕНИ ОБРОБКИ ДАНИХ

Використовувати захищені домени обробки даних для забезпечення [*Призначення: визначеної організацією політики управління потоками інформації*] як основу для ухвалення рішень щодо управління потоками.

Рекомендації з реалізації: Захищені домени обробки — це простори обробки, які контролюють взаємодію з іншими просторами обробки для забезпечення управління інформаційними потоками між ними, а також від/до об'єктів даних. Захищена обробка домену може бути забезпечена, наприклад, шляхом

впровадження домену та типового примусового виконання. Системні процеси присвоюються доменам, інформація ідентифікується за типами, а інформаційні потоки контролюються на основі дозволеного доступу до інформації (визначається доменом і типом інформації).

Пов'язані заходи: SC-39.

(3) УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ДИНАМІЧНЕ УПРАВЛІННЯ ІНФОРМАЦІЙНИМ ПОТОКОМ

Здійснювати динамічне управління потоком інформації на основі [*Призначення: визначених організацією політик (правил)*].

Рекомендації з реалізації: Політика динамічного управління інформаційними потоками містить дозвіл або заборону інформаційних потоків на основі умов, що змінюються, або експлуатаційних міркувань. Умови, що змінюються, охоплюють зміни в потребах організації, зміни в навколишньому інформаційному середовищі та в разі виявлення потенційно шкідливих чи несприятливих подій тощо.

Пов'язані заходи: SI-4.

(4) УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - УПРАВЛІННЯ ПОТОКОМ ЗАШИФРОВАНОЇ ІНФОРМАЦІЇ

Запобігати обходу [*Призначення: механізмів управління потоками, визначених організацією*] зашифрованої інформації шляхом [*Вибір (один або декілька): дешифрування інформації; блокування потоку зашифрованої інформації; завершення сеансів зв'язку, що намагаються передавати зашифровану інформацію*; [*Призначення: визначеними організацією процедурою або методом*]].

Рекомендації з реалізації: Механізмами управління можуть бути: перевірка вмісту, фільтри, політики безпеки та ідентифікатори типів даних.

Пов'язані заходи: SI-4.

(5) УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ВБУДОВУВАННЯ ТИПІВ ДАНИХ

Впровадити [*Призначення: визначені організацією обмеження*] для вбудовування типів даних в інші типи даних.

Рекомендації з реалізації: Вбудовування типів даних в інші типи даних може призвести до зниження ефективності управління потоком. Вбудовування типу даних охоплює: вставлення виконуваних файлів (exe файлів) як об'єктів у текстові файли; вставлення посилань або описової інформації в медіафайл, а також архівовані типи даних, які можуть містити кілька вбудованих типів даних. Обмеження щодо вбудовування типів даних повинні враховувати рівні вбудовування та заборону таких, що виходять за межі можливостей інструментів перевірки.

Пов'язані заходи: Немає.

(6) УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - МЕТАДАНІ

Здійснювати управління інформаційним потоком на основі [*Призначення:*

*визначених організацією метаданих*].

Рекомендації з реалізації: Метадані — це службова інформація, яка використовується для опису характеристик даних. Метадані можуть бути структурними (описують структури даних) або загальними (описують вміст даних). Впровадження дозволених потоків інформації на основі метаданих дозволяє реалізувати простіше й ефективніше управління. Метадані мають бути проаналізовані щодо точності (значення метаданих є правильними щодо даних), цілісності (захист від несанкціонованих змін тегів метаданих) та прив'язки метаданих до корисного навантаження даних (тобто забезпечення методів зв'язування з відповідним рівнем упевненості).

Пов'язані заходи: AC-16, SI-7.

(7) УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - МЕХАНІЗМИ ОДНОСТОРОННЬОГО ПОТОКУ

Впровадити [*Призначення: визначені організацією односторонні інформаційні потоки*] за допомогою апаратних механізмів.

Рекомендації з реалізації: Механізми одностороннього потоку також можуть називатися односпрямованою мережею, односпрямованим шлюзом безпеки або діодом даних. Механізми одностороннього потоку можна використовувати, щоб запобігти експорту даних із домену або системи з більшим впливом або класифікованим, одночасно дозволяючи імпортувати дані з системи з меншим впливом або з некласифікованого домену.

Пов'язані заходи: Немає.

(8) УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ – ФІЛЬТРИ ПОЛІТИКИ БЕЗПЕКИ

a) Забезпечити контроль над потоком інформації, використовуючи [*Призначення: визначені організацією фільтри безпеки або політики конфіденційності*] як основу для рішень щодо керування потоком для [*Призначення: визначені організацією потоки інформації*];

b) [*Вибір (один або кілька): Блокування; Зміна; Карантин*] даних після помилки обробки фільтра відповідно до [*Призначення: політика безпеки або конфіденційності, визначена організацією*].

Рекомендації з реалізації: Фільтри політик безпеки стосуються як структури даних, так і вмісту. Наприклад, фільтри політик безпеки щодо структур даних можуть накладати обмеження на максимальну довжину файлів, максимальний розмір поля та типи даних/файлів. Фільтри політик безпеки щодо вмісту даних можуть перевіряти наявність певних значень або діапазонів даних і вмісту. Вміст структурованих даних може інтерпретуватися застосунками. До неструктурованих даних належить цифрова інформація без структури даних або з такою структурою, яка не може бути оброблена відповідно до визначеного набору правил (растрові зображення, відео, аудіоконтейнери, рукописні тексти тощо). Кількість фільтрів, яка впроваджується, має залежати від цілей управління.

Пов'язані заходи: Немає.

(9) УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ – ПЕРЕВІРКИ, ЩО ПРОВОДИТЬ ПЕРСОНА

Примусово використовувати перевірку персоналом [*Призначення: потоки інформації, визначені організацією*] за таких умов: [*Призначення: умови, визначені організацією*].

Рекомендації з реалізації: Фільтри політик безпеки мають бути визначені для всіх ситуацій, коли можливі автоматизовані рішення управління потоком. У разі, якщо організація повністю автоматизованого управління потоком неможлива, може бути використане додаткове ручне управління (як замість автоматизованого, так і в ролі додаткового ступеня управління). Рішення щодо організації ручного управління персоналом має ухвалюватися залежно від конкретних умов функціонування.

Пов'язані заходи: Немає.

(10) УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - АКТИВАЦІЯ ТА ДЕАКТИВАЦІЯ ФІЛЬТРІВ ПОЛІТИКИ БЕЗПЕКИ

Впровадити можливість для привілейованих адміністраторів активувати та деактивувати [*Призначення: фільтри політики безпеки, що визначаються організацією*] за таких умов: [*Призначення: визначені організацією умови*].

Рекомендації з реалізації: Наприклад, якщо це не суперечить принципам авторизації, адміністратори можуть встановлювати фільтри політики безпеки для розміщення затверджених типів даних. Адміністратори також мають можливість вибирати фільтри, необхідні для певного потоку на основі типу даних, що передаються, доменів безпеки джерела та призначення та інших функцій, пов'язаних із безпекою чи конфіденційністю, якщо це необхідно.

Пов'язані заходи: Немає.

(11) УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ – КОНФІГУРАЦІЯ ФІЛЬТРІВ ПОЛІТИКИ БЕЗПЕК

Впровадити можливість для привілейованих адміністраторів налаштувати [*Призначення: визначені організацією фільтри політики безпеки*] для підтримки різних політик безпеки.

Рекомендації з реалізації: Документація містить детальну інформацію щодо налаштування фільтрів безпеки та політики конфіденційності. Наприклад, адміністратори можуть налаштувати фільтри політики безпеки або конфіденційності, щоб включити список невідповідних слів, які механізми безпеки або політики конфіденційності перевіряють відповідно до визначень, наданих організаціями.

Пов'язані заходи: Немає.

(12) УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ – ІДЕНТИФІКАТОРИ ТИПУ ДАНИХ

При передачі інформації між різними захищеними доменами використовувати [*Призначення: визначені організацією ідентифікатори типів даних*] для перевірки даних, необхідних для ухвалення рішень щодо інформаційного потоку.

Рекомендації з реалізації: Ідентифікаторами типів даних можуть виступати: імена файлів, типи файлів, підписи файлів/токени. Системи можуть дозволити передачу даних лише відповідно до специфікацій формату типу даних. Ім'я та номер файлу не використовуються для ідентифікації типу даних. Вміст перевіряється синтаксично та семантично відповідно до його специфікації, щоб переконатися, що це належний тип даних.

Пов'язані заходи: Немає.

(13) УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ – ДЕКОМПОЗИЦІЯ НА ВІДПОВІДНІ ПОЛІТИЦІ СУБКОМПОНЕНТИ

При передачі інформації між різними захищеними доменами здійснювати декомпозицію інформації на [*Призначення: визначені організацією субкомпоненти, що відповідають політиці*] для представлення в механізмах реалізації політики.

Рекомендації з реалізації: Механізми виконання політики можуть застосовувати правила фільтрації до відповідних підкомпонентів інформації для полегшення управління потоком. Декомпозиція файлів полегшує рішення щодо політики, сертифікатів, класифікації, вкладених файлів та інших диференціаторів компонентів щодо безпеки.

Пов'язані заходи: Немає.

(14) УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ОБМЕЖЕННЯ ФІЛЬТРА ПОЛІТИКИ БЕЗПЕКИ

При передачі інформації між різними захищеними доменами реалізувати [*Призначення: визначені організацією фільтри політики безпеки*], що вимагають повного переліку форматів, які обмежують структуру та зміст даних.

Рекомендації з реалізації: Структурування даних і обмеження вмісту зменшують діапазон потенційно шкідливого чи несанкціонованого вмісту в міждоменних транзакціях. Фільтри політики безпеки, що обмежують структуру даних, можуть містити обмеження розмірів файлів та довжини поля. Фільтри політики безпеки щодо вмісту даних можуть охоплювати: формати кодування; обмеження символьних полів (наприклад наявність лише буквено-цифрових символів); заборону використання спеціальних символів; валідацію структур тощо.

Пов'язані заходи: Немає.

(15) УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ВИЯВЛЕННЯ НЕСАНКЦІОНОВАНОЇ ІНФОРМАЦІЇ

При передачі інформації між різними захищеними доменами перевіряти інформацію на наявність [*Призначення: визначеної організацією несанкціонованої інформації*] та забороняти передачу такої інформації відповідно до [*Призначення: визначеної організацією політики безпеки*].

Рекомендації з реалізації: Несанкціонована інформація може включати зловмисний код, інформацію, яку не можна оприлюднити з вихідної мережі, або виконуваний код, який може порушити або зашкодити службам або системам мережі.

Пов’язані заходи: SI-3.

(16) УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ПЕРЕДАЧА ІНФОРМАЦІЇ ПРО ВЗАЄМОПОВ’ЯЗАНІ СИСТЕМИ

[Вилучено: включено до AC-4].

(17) УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - АВТЕНТИФІКАЦІЯ ДОМЕНУ

Унікально ідентифікувати й автентифікувати джерела та пункти призначення за допомогою [*Вибір (один або декілька): організації, системи, програми, служби, індивідуума*] для передачі інформації.

Рекомендації з реалізації: Процедура призначення атрибутів є найважливішим компонентом концепції безпеки операцій. Можливість ідентифікації джерела та пунктів призначення потоку інформації в системах дозволяє в разі необхідності проводити реконструкцію подій і може встановити порушників, що своєю чергою заохочує посадових осіб дотримуватися політики. Успішна автентифікація домену вимагає, щоб мітки системи розрізняли системи, організації та осіб, які беруть участь у підготовці, передачі, отриманні чи поширенні інформації. Процедура призначення атрибутів також дозволяє краще обробляти персональну інформацію, що проходить через системи, і полегшувати відстеження згоди, запитів на виправлення, видалення або доступу від окремих осіб.

Пов’язані заходи: IA-2, IA-3, IA-9.

(18) УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ПРИВ’ЯЗКА АТРИБУТУ БЕЗПЕКИ

[Вилучено: включено в AC-16].

(19) УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ПЕРЕВІРКА МЕТАДАНИХ

Під час передачі інформації між різними захищеними доменами застосовувати до метаданих ту ж політику безпеки фільтрації, що й для корисних даних.

Рекомендації з реалізації: Це посилення заходу вимагає перевірки метаданих на рівні з даними, до яких вони застосовуються. Метадані можуть вноситися або не вноситися до складу корисного навантаження даних. Незалежно від цього, уся інформація (включно з метаданими та даними, до яких вони застосовуються) підлягає фільтруванню та перевірці.

Пов’язані заходи: Немає.

(20) УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ЗАТВЕРДЖЕНІ РІШЕННЯ

Впровадити [*Призначення: визначені організацією рішення про схвалені конфігурації*] для керування потоком [*Призначення: інформації, визначеної організацією*] через захищені домени.

Рекомендації з реалізації: Затверджені рішення та конфігурації в міждоменній політиці та керівництвах відповідно до типів потоків інформації можуть

визначатися через межі класифікації. Наявність єдиного кросс-доменного менеджменту може забезпечити базовий список затверджених рішень для міждоменних рішень.

Пов'язані заходи: Немає.

(21) УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ФІЗИЧНЕ ТА ЛОГІЧНЕ ВІДДІЛЕННЯ ІНФОРМАЦІЙНИХ ПОТОКІВ

Відокремлювати потоки інформації логічно або фізично, використовуючи [*Призначення: визначені організацією механізми та/або методи*] для досягнення [*Призначення: визначеного організацією необхідного поділу за типами інформації*].

Рекомендації з реалізації: Відокремлення інформаційних потоків за типом може підвищити захист, гарантуючи, що інформація не перемішується під час передачі. Це дозволить управляти шляхами передачі потоку (за неможливості організації іншого виду управління). Типи, за якими інформація може відокремлюватися: вхідний і вихідний трафік, запити на послуги та відповіді й інформацію, яка належить до різних категорій безпеки.

Пов'язані заходи: SC-32.

(22) УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ЄДИНИЙ ДОСТУП

Забезпечити доступ з одного пристрою до обчислювальних платформ, застосунків або даних, що розташовуються в декількох різних захищених доменах, одночасно запобігаючи передачі будь-якого потоку інформації між різними захищеними доменами.

Рекомендації з реалізації: Наприклад, забезпечення єдиного робочого стола для доступу користувачів до кожного підключеного домену безпеки, не надаючи механізмів, що дозволяють переносити інформацію між різними доменами безпеки.

Пов'язані заходи: Немає.

Посилання: Немає.

(23) УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - МОДИФІКОВАНА ІНФОРМАЦІЯ, ЯКА НЕ ПІДЛЯГАЄ ОПРИЛЮДНЕННЮ

Під час передачі інформації між різними доменами безпеки змінюйте інформацію, яка не підлягає оприлюдненню, реалізувавши [*Призначення: визначена організацією дія модифікації*]

Рекомендації з реалізації: Зміна інформації, яка не підлягає оприлюдненню, може допомогти запобігти витоку даних або атаці, коли інформація передається між доменами безпеки. Дії модифікації включають маскування, перестановку, зміну, видалення або редагування.

Пов'язані заходи: Немає.

(24) УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ВНУТРІШНІЙ НОРМАЛІЗОВАНИЙ ФОРМАТ

Під час передачі інформації між різними доменами безпеки аналізуйте вхідні дані у внутрішньому нормалізованому форматі та повторно генеруйте дані, щоб вони відповідали призначеній специфікації.

Рекомендації з реалізації: Перетворення даних у нормалізовані форми є одним із найбільш ефективних механізмів для припинення зловмисних атак і викрадання великих класів даних.

Пов'язані заходи: Немає.

(25) УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ОЧИЩЕННЯ ДАНИХ

Під час передачі інформації між різними доменами безпеки очищуйте дані, щоб мінімізувати [*Вибір (один або кілька): доставка зловмисного вмісту, керування та керування зловмисним кодом, доповнення зловмисного коду та стеганографічно закодовані дані; витік конфіденційної інформації*] відповідно до [*Призначення: політика, визначена організацією*]].

Рекомендації з реалізації: Очищення даних — це процес безповоротного видалення або знищення даних, що зберігаються на пристрої пам'яті (наприклад, на жорстких дисках, флеш-пам'яті/твердотільних накопичувачах, мобільних пристроях, компакт-дисках і DVD-дисках) або у вигляді паперових копій.

Пов'язані заходи: MP-6.

(26) УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ДІЇ З ФІЛЬТРАЦІЇ АУДИТУ

Під час передачі інформації між різними доменами безпеки записуйте та перевіряйте дії фільтрації вмісту та результати для інформації, що фільтрується.

Рекомендації з реалізації: Фільтрування вмісту — це процес перевірки інформації під час проходження міждоменного рішення та визначення відповідності інформації попередньо визначеній політиці. Дії фільтрації вмісту та результати дій фільтрації записуються для окремих повідомлень, для визначення правильності застосованих дій фільтра. Звіти про вміст фільтрів використовуються, щоб допомогти у вирішенні проблем, наприклад, визначаючи, чому вміст повідомлення було змінено та/або чому він не пройшов процес фільтрації. Події аудиту визначені в AU-2. Записи аудиту створюються в AU-12.

Пов'язані заходи: AU-2, AU-3, AU-12.

(27) УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - НАДЛИШКОВІ/НЕЗАЛЕЖНІ ФІЛЬТРУЮЧІ МЕХАНІЗМИ

Під час передачі інформації між різними доменами безпеки впроваджуйте рішення фільтрації вмісту, які забезпечують надлишкові та незалежні механізми фільтрації для кожного типу даних.

Рекомендації з реалізації: Фільтрування вмісту — це процес перевірки інформації під час проходження міждоменного рішення та визначення відповідності інформації попередньо визначеній політиці. Надлишкова та незалежна фільтрація вмісту усуває єдину систему фільтрації збоїв.

Незалежність визначається як реалізація фільтра вмісту, який використовує іншу кодову базу та допоміжні бібліотеки (наприклад, два фільтри JPEG із використанням бібліотек JPEG різних постачальників) і кілька незалежних процесів системи.

Пов'язані заходи: Немає.

(28) УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ЛІНІЙНІ ФІЛЬТРУВАЛЬНІ КАНАЛИ

Під час передачі інформації між різними доменами безпеки запровадьте конвеєр лінійного фільтрування вмісту, який забезпечується дискреційним і обов'язковим контролем доступу.

Рекомендації з реалізації: Фільтрування вмісту — це процес перевірки інформації під час проходження міждоменного рішення та визначення відповідності інформації попередньо визначеній політиці. Використання конвеєрів лінійного фільтрування вмісту гарантує, що процеси фільтрації не можна обійти. Загалом, використання архітектур паралельної фільтрації для фільтрації вмісту одного типу даних створює проблеми з обходом і невикликом.

Пов'язані заходи: Немає.

(29) УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ФІЛЬТР МЕХАНІЗМІВ ОРКЕСТРОВКИ

Під час передачі інформації між різними доменами безпеки використовуйте механізми оркестровки фільтрів вмісту, щоб забезпечити:

a. Механізми фільтрації вмісту успішно завершують виконання без помилок;

b. Дії фільтрації вмісту виконуються в правильному порядку та відповідають [*Призначення: політика, визначена організацією*]

Рекомендації з реалізації: Фільтрування вмісту — це процес перевірки інформації під час проходження міждоменного рішення та визначення відповідності інформації попередньо визначеній політиці безпеки. Механізм оркестровки координує послідовність дій (ручну та автоматизовану) у процесі фільтрації вмісту. Помилки визначаються як аномальні дії або несподіване завершення процесу фільтрації вмісту. Це не те саме, що вміст, який не вдається відфільтрувати через невідповідність політиці. Звіти фільтрів вмісту – це механізм, який зазвичай використовується для забезпечення успішного виконання очікуваних дій фільтрації.

Пов'язані заходи: Немає.

(30) УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - МЕХАНІЗМИ ФІЛЬТРАЦІЇ З ВИКОРИСТАННЯМ КІЛЬКОХ ПРОЦЕСІВ

Під час передачі інформації між різними доменами безпеки реалізуйте механізми фільтрації вмісту за допомогою кількох процесів.

Рекомендації з реалізації: Використання кількох процесів для впровадження механізмів фільтрації вмісту зменшує ймовірність єдиної точки збою.

Пов'язані заходи: Немає.

(31) УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ЗАПОБІГАННЯ СПРОБАМ ПЕРЕДАЧІ ВМІСТУ, ЯКИЙ НЕ ПРОЙШОВ ПЕРЕВІРКУ ФІЛЬТРАЦІЇ

Під час передачі інформації між різними доменами безпеки запобігайте передачі вмісту, який не пройшов перевірку фільтрації до домену-одержувача.

Рекомендації з реалізації: Вміст, який не пройшов перевірку фільтрації, може пошкодити систему, якщо його передати в домен-одержувач.

Пов'язані заходи: Немає.

(32) УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ - ВИМОГИ ДО ПРОЦЕСУ ПЕРЕДАЧІ ІНФОРМАЦІЇ

Під час передачі інформації між різними доменами безпеки, процес, який передає інформацію між конвеєрами фільтрації:

a. не фільтрує вміст повідомлення;
b. перевіряє метадані фільтрації;
c. забезпечує успішне завершення фільтрації вмісту, пов'язаного з метаданими фільтрації; і
d. передає вміст до цільового фільтруючого конвеєра.

Рекомендації з реалізації: Процеси, що передають інформацію між фільтруючими конвеєрами, повинні мати мінімальну складність і функціональність для гарантування того, що процеси працюють правильно.

Пов'язані заходи: Немає.

## AC-5 РОЗМЕЖУВАННЯ ОБОВ'ЯЗКІВ

Заходи захисту:

a. Розмежувати і документувати [*Призначення: визначені організацією обов'язки окремих осіб*].

b. Установити правила авторизації доступу для підтримки розмежування обов'язків.

Рекомендації з реалізації: Розмежування обов'язків запобігає можливості зловживання уповноваженими привілеями та сприяє зниженню ризику зловмисної діяльності без змови. Розмежування обов'язків може охоплювати розподіл функцій, включно з функціями підтримки системи, між різними особами та/або ролями, а також забезпеченням того, щоб персонал служби безпеки, який здійснює функції управління доступом, не виконував функції аудиту. При розробці політики розмежування доступу необхідно проводити аналіз всієї організаційної системи та її компонентів. Розподіл обов'язків забезпечується діями керування обліковими записами в AC-2, механізмами контролю доступу в AC-3 та діями керування ідентифікацією в IA-2, IA-4 та IA-12.

Пов'язані заходи: AC-2, AC-3, AC-5, AU-9, CM-5, CM-11, CP-9, IA-2, IA-4, IA-5, IA-12, MA-3, MA-5, PS-2, SA-8, SA-17.

Посилення заходів: Немає.

Посилання: Немає.

## AC-6 МІНІМІЗАЦІЯ ПОВНОВАЖЕНЬ

Заходи захисту:

Впровадити принцип мінімізації повноважень, який дозволяє користувачам (або процесам, що діють від імені користувачів) здійснювати лише такі авторизовані звернення, які необхідні для виконання визначених завдань відповідно до цілей (призначення, місії) організації та функцій.

Рекомендації з реалізації: Рекомендується запровадження принципу мінімізації повноважень для конкретних обов'язків і систем. Принцип мінімізації повноважень застосовується також до процесів системи для забезпечення їхнього функціонування на рівнях привілеїв не вищих, ніж це необхідно для виконання її функцій організації. Для досягнення мінімізації повноважень може розглядатися потреба у виділенні додаткових процесів, ролей або облікових записів системи. Принцип мінімізації повноважень також застосовується щодо розробки, впровадження та функціонування систем організації.

Пов'язані заходи: AC-2, AC-3, AC-5, AC-16, CM-5, CM-11, PL-2, PM-12, SA-15, SA-17, SC-38.

Посилення заходів:

(1) МІНІМІЗАЦІЯ ПОВНОВАЖЕНЬ - АВТОРИЗОВАНИЙ ДОСТУП ДО ФУНКЦІЙ БЕЗПЕКИ

Авторизуваний доступ для [*Призначення: особи або ролі, визначені організацією*] до:

a) [*Призначення: функції безпеки, визначені організацією (розгорнуті в апаратному, програмному та мікропрограмному забезпеченні*)];

b) [*Призначення: визначена організацією інформація, необхідна для забезпечення безпеки]*.

Рекомендації з реалізації: Функції захисту можуть охоплювати встановлення облікових записів системи; налаштування авторизацій доступу (тобто дозволів, привілеїв); визначення подій, що підлягають аудиту, та встановлення параметрів виявлення вторгнень. Інформація, що стосується безпеки, може містити правила фільтрації маршрутизаторів/брандмауерів, інформацію про управління криптографічними ключами, параметри конфігурації служб безпеки та списки контролю доступу. До уповноваженого персоналу можуть належати адміністратори безпеки, системні адміністратори й адміністратори мереж, працівники служби захисту інформації, персонал з обслуговування системи, системні програмісти та інші привілейовані користувачі.

Пов’язані заходи: AC-17, AC-18, AC-19, AU-9, PE-2.

(2) МІНІМІЗАЦІЯ ПОВНОВАЖЕНЬ - НЕПРИВІЛЕЙОВАНИЙ ДОСТУП ДО НЕЗАХИЩЕНИХ ФУНКЦІЙ

Вимагати від користувачів облікових записів системи або ролей, які мають доступ до [*Призначення: визначених організацією функцій безпеки або інформації, що стосується безпеки*], використовувати непривілейовані облікові записи чи ролі під час доступу до незахищених функцій.

Рекомендації з реалізації: Це посилення заходу обмежує сферу дії під час роботи з привілейованих облікових записів або ролей. Впровадження ролей організується в разі реалізації рольової політики контролю доступу (rolle-based). При цьому зміна ролі має гарантувати однаковий ступінь зміни дозволів на доступ як для користувача, так і для всіх процесів від його імені аналогічно тому, якби це було передбачено зміною привілейованого облікового запису на непривілейований.

Пов’язані заходи: AC-17, AC-18, AC-19, PL-4.

(3) МІНІМІЗАЦІЯ ПОВНОВАЖЕНЬ - МЕРЕЖЕВИЙ ДОСТУП ДО ПРИВІЛЕЙОВАНИХ КОМАНД

Авторизувати мережевий доступ до [*Призначення: визначених організацією привілейованих команд*] тільки для [*Призначення: визначених організацією невідкладних операційних потреб*] та задокументувати обґрунтування необхідності такого доступу в плані безпеки системи.

Рекомендації з реалізації: Мережевий доступ — це будь-який доступ через мережеве з’єднання (тобто коли користувач не має фізичного доступу, наприклад, до робочої станції).

Пов’язані заходи: AC-17, AC-18, AC-19.

(4) МІНІМІЗАЦІЯ ПОВНОВАЖЕНЬ - РОЗДІЛЬНІ ДОМЕНИ ОБРОБКИ

Надати окремі домени обробки даних для забезпечення більш точного розподілу повноважень користувача.

Рекомендації з реалізації: Забезпечення роздільних доменів обробки для розподілу привілеїв користувача може містити використання віртуальних машин для надання додаткових привілеїв користувачу, при цьому обмежуючи привілеї інших віртуальних/фізичних машин; використання апаратних/програмних механізмів розділення домену та реалізацію окремих фізичних доменів.

Пов’язані заходи: AC-4, SC-2, SC-3, SC-30, SC-32, SC-39.

(5) МІНІМІЗАЦІЯ ПОВНОВАЖЕНЬ - ПРИВІЛЕЙОВАНІ ОБЛІКОВІ ЗАПИСИ

Обмежити привілейовані облікові записи в системі згідно з [*Призначення: визначеним організацією персоналом або ролями*].

Рекомендації з реалізації: Привілейовані облікові записи можуть містити облікові записи суперкористувачів (наприклад обліковий запис системного

адміністратора) Використання привілейованих облікових записів лише конкретними посадовими особами виключає можливість доступу до таких облікових записів всіх інших штатних працівників. Застосування цього посилення заходу щодо управління привілеями локальних облікових записів і облікових записів доменів може відрізнятися залежно від організаційної структури, за умови збереження можливості контролю конфігурації системи за ключовими параметрами безпеки.

Пов'язані заходи: IA-2, MA-3, MA-4.

(6) МІНІМІЗАЦІЯ ПОВНОВАЖЕНЬ - ПРИВІЛЕЙОВАНИЙ ДОСТУП КОРИСТУВАЧАМИ, ЩО НЕ НАЛЕЖАТЬ ДО ОРГАНІЗАЦІЇ

Заборонити привілейований доступ до системи користувачам, які не належать до організації.

Рекомендації з реалізації: Користувач в організації — це працівник або особа, яку організація вважає еквівалентним статусу працівника. Організаційні користувачі включають підрядників, запрошених дослідників або окремих осіб з інших організацій. Політика та процедури надання статусу співробітників окремим особам включають інформацію про громадянство та стосунки з організацією таких осіб.

Пов'язані заходи: AC-18, AC-19, IA-2, IA-8.

(7) МІНІМІЗАЦІЯ ПОВНОВАЖЕНЬ - ПЕРЕГЛЯД ПОВНОВАЖЕНЬ КОРИСТУВАЧА

a) Переглядати [*Призначення: з визначеною організацією частотою*] повноваження призначених для [*Призначення: визначених організацією посад або класів користувачів*] для перевірки необхідності таких повноважень;

b) За необхідності перепризначити або зняти повноваження, для правильного відображення цілей (місії) організації та потреб організації.

Рекомендації з реалізації: Потреба в призначених привілеях користувача може змінюватися з часом, відображаючи зміни в цілях (місіях) організації і функціях, середовищах роботи, технологіях чи загрозах. Необхідно проводити періодичний перегляд призначених привілеїв користувача, щоб визначити, чи залишається обґрунтованим призначення таких привілеїв.

Пов'язані заходи: CA-7.

(8) МІНІМІЗАЦІЯ ПОВНОВАЖЕНЬ - РІВНІ ПРИВІЛЕЇВ ДЛЯ ВИКОНАННЯ КОДУ

Запобігати виконанню програмного забезпечення на рівні привілеїв вищому, ніж доступний користувачеві, який використовує програмне забезпечення [*Призначення: визначене організацією програмне забезпечення*].

Рекомендації з реалізації: У певних ситуаціях програмне забезпечення / програмний продукт має виконуватися з підвищеними привілеями для виконання необхідних функцій. Однак якщо привілеї, необхідні для виконання, перебувають на вищому рівні, ніж привілеї, призначені користувачам, які використовують таке програмне забезпечення / програмний продукт, виникає

ситуація, що цим користувачам опосередковано надаються більші привілеї, ніж призначені.

Пов'язані заходи: Немає.

(9) МІНІМІЗАЦІЯ ПОВНОВАЖЕНЬ - АУДИТ ВИКОРИСТАННЯ ПРИВІЛЕЙОВАНИХ ФУНКЦІЙ

Реєструвати виконання привілейованих функцій.

Рекомендації з реалізації: Навмисне чи ненавмисне зловживання привілейованими функціями уповноваженими користувачами або сторонніми організаціями, які мають компрометовані системні облікові записи, є серйозною загрозою та може мати значні негативні наслідки для організацій. Аудит використання привілейованих функцій — це один зі способів виявлення подібних зловживань, який допомагає зменшити ризик від інсайдерських загроз.

Пов'язані заходи: AU-2, AU-3, AU-12.

(10) МІНІМІЗАЦІЯ ПОВНОВАЖЕНЬ - ЗАБОРОНА НЕПРИВІЛЕЙОВАНИМ КОРИСТУВАЧАМ ВИКОНУВАТИ ПРИВІЛЕЙОВАНІ ФУНКЦІЇ

Вжити заходи для запобігання можливості виконувати привілейовані функції непривілейованими користувачами.

Рекомендації з реалізації: До привілейованих функцій можуть належати: відключення, обхід або зміна впровадженого заходу безпеки, створення облікових записів системи, проведення перевірок цілісності системи або адміністрування криптографічних ключів. Непривілейовані користувачі — це особи, які не мають відповідних дозволів. Механізми виявлення та запобігання вторгненням або механізми захисту від шкідливого коду є прикладами привілейованих функцій, які потребують захисту від непривілейованих користувачів. Заборона непривілейованим користувачам у виконанні привілейованих функцій забезпечується AC-3.

Пов'язані заходи: Немає.

Посилання: Немає.

## AC-7 НЕВДАЛІ СПРОБИ ВХОДУ В СИСТЕМУ

Заходи захисту:

a. Встановити обмеження на [*Призначення: визначену організацією кількість*] послідовних неуспішних спроб входу користувача в систему впродовж [*Призначення: визначеного організацією часового періоду*].

b. Автоматично виконати [*Вибір (один або декілька): блокування облікового запису/вузла на* [*Призначення: визначений організацією часовий період*]; *блокування облікового запису/вузла, доки він не буде розблокований адміністратором; затримання наступної команди входу в систему за* [*Надання: визначеним організацією алгоритмом затримки*]; виконати [*Призначення: визначені організацією дії*]], коли перевищено максимальну кількість невдалих спроб входу в систему.

Рекомендації з реалізації: Необхідність обмежити невдалі спроби входу в систему та вжити подальших заходів, коли максимальна кількість спроб входу перевищена, застосовується незалежно від того, через локальне або мережеве з'єднання відбувається вхід. Через потенційну відмову в обслуговуванні автоматичне блокування, ініційоване системами, зазвичай є тимчасовим і автоматично відновлюється через визначений період часу. Якщо вибрано алгоритм затримки, організації можуть використовувати різні алгоритми для різних компонентів системи на основі можливостей цих компонентів. Реакція на невдалі спроби входу може бути реалізована на рівні операційної системи та програми. Визначені організацією дії, які можуть бути виконані, коли перевищено дозволену кількість спроб входу, включають прохання користувача відповісти на секретне запитання на додаток до імені користувача та пароля, виклик режиму блокування з обмеженими можливостями користувача (замість повного блокування) , дозволяючи користувачам входити лише із вказаних IP-адрес та вимагаючи CAPTCHA для запобігання автоматичним атакам або застосовуючи профілі користувачів, такі як місцезнаходження, час доби, IP-адреса, пристрій або MAC-адреса. Якщо автоматичне блокування системи або виконання алгоритму затримки не реалізовано, організації розглядають комбінацію інших дій, щоб допомогти запобігти атакам грубою силою. На додаток до вищезазначеного, організації можуть запропонувати користувачам відповісти на секретне запитання до того, як кількість невдалих спроб входу буде перевищена. Автоматичне розблокування облікового запису після певного періоду часу зазвичай не дозволяється. Однак можуть знадобитися винятки залежно від операційної місії або потреби.

Пов'язані заходи: AC-2, AC-9, AU-2, AU-6, IA-5.

Посилення заходів:

(1) НЕВДАЛІ СПРОБИ ВХОДУ В СИСТЕМУ - АВТОМАТИЧНЕ БЛОКУВАННЯ ОБЛІКОВОГО ЗАПИСУ

[Вилучено: включено в AC-7].

(2) НЕВДАЛІ СПРОБИ ВХОДУ В СИСТЕМУ - ОЧИЩЕННЯ АБО СТИРАННЯ МОБІЛЬНОГО ПРИСТРОЮ

Очистити або стерти інформацію з [*Призначення: визначених організацією мобільних пристроїв*] на основі [*Призначення: визначених організацією вимог та методик очищення чи стирання*] після [*Призначення: визначеної організацією кількості*] послідовних невдалих спроб входу в систему з пристрою.

Рекомендації з реалізації: Це посилення заходу стосується лише мобільних пристроїв, з яких відбувається вхід. Вхід на мобільний пристрій не має означати вхід в обліковий запис. Успішні входи в облікові записи на мобільних пристроях мають обнуляти кількість невдалих входів. Якщо інформація на мобільному пристрої захищена досить сильними механізмами шифрування, додаткові засоби забілювання інформації можуть бути опущені.

Пов'язані заходи: AC-19, MP-5, MP-6.

(3) НЕВДАЛІ СПРОБИ ВХОДУ В СИСТЕМУ - ОБМЕЖЕННЯ НА СПРОБИ БІОМЕТРИЧНОГО ВХОДУ

Обмежити кількість невдалих спроб входу за допомогою біометрики

[*Призначення: визначена організацією кількість*].

Рекомендації з реалізації: Біометрика має ймовірнісний характер. На успішність автентифікації може впливати безліч факторів, включно з ефективністю механізмів порівняння та методів виявлення атак. Відповідно до цих показників має бути вибрана відповідна кількість спроб та механізми відмови у вході.

Пов'язані заходи: IA-3.

(4) НЕВДАЛІ СПРОБИ ВХОДУ В СИСТЕМУ - ВИКОРИСТАННЯ АЛЬТЕРНАТИВНОГО ФАКТОРА

a) Дозволити використання [*Призначення: визначені організацією фактори автентифікації*], які відрізняються від основних факторів автентифікації після перевищення визначеної організацією кількості послідовних невдалих спроб входу в систему;

b) Обмежити [*Призначення: визначена організацією кількість*] послідовних невдалих спроб входу за допомогою використання альтернативних факторів користувачем протягом [*Призначення: визначеного організацією періоду часу*].

Рекомендації з реалізації: Це посилення заходу дозволяє користувачеві, який випадково був заблокований, використовувати додаткові фактори автентифікації для обходу блокування.

Пов'язані заходи: IA-3.

Посилання: [SP 800-63-3], [SP 800-124].

## AC-8 ПОПЕРЕДЖЕННЯ ПРО ВИКОРИСТАННЯ СИСТЕМИ

Заходи захисту:

a. Демонструвати користувачам [*Призначення: визначене організацією сповіщення або банер про використання системи*] перед тим, як надавати доступ до системи, що забезпечує безпеку та приватність відповідно до чинних законів, нормативних документів, наказів, директив, політик, правил, стандартів і керівних принципів, які зазначають, що:

   1. користувачі здійснюють доступ до урядової системи;

   2. використання системи може контролюватися, реєструватися та підлягати аудиту;

   3. несанкціоноване використання системи забороняється та приводить до кримінальної та цивільної відповідальності;

   4. використання системи означає згоду на моніторинг і запис дій користувача.

b. Зберігати сповіщення або банер на екрані, доки користувачі не визнають умови використання та не приймуть явних дій для входу в систему або подальшого доступу до системи.

c. Для загальнодоступних систем:

1. демонструвати інформацію про умови використання системи [*Призначення: визначені організацією умови*], перш ніж надавати подальший доступ до загальнодоступної системи;

2. демонструвати посилання, якщо такі є, на моніторинг, запис або аудит, які узгоджуються з акомодацією приватності для таких систем, які зазвичай забороняють такі дії;

3. мати опис авторизованого використання системи.

Рекомендації з реалізації: Сповіщення про використання системи можуть бути реалізовані за допомогою повідомлень або банерів попередження, що відображаються перед тим, як користувач входить у систему. Сповіщення про використання системи мають бути присутніми лише в тому разі, якщо в систему входить користувач (наприклад, такі сповіщення не потрібні, якщо до системи звертається процес). На основі оцінки ризику організації розглядають, чи потрібне сповіщення про використання вторинної системи для доступу до програм або інших ресурсів системи після початкового входу в мережу. Залежно від потреб, сповіщення можуть відображатися декількома мовами.

Пов'язані заходи: AC-14, PL-4, SI-4.

Посилення заходів: Немає.

Посилання: Немає.

## AC-9 СПОВІЩЕННЯ ПРО ПОПЕРЕДНІЙ ВХІД (ДОСТУП)

Заходи захисту:

Сповіщати користувача після успішного входу (доступу) до системи про дату та час останнього входу (доступу).

Рекомендації з реалізації: Цей захід безпеки застосовується при вході до системи користувачів незалежно від типу архітектур.

Пов'язані заходи: AC-7, PL-4.

Посилення заходів:

(1) СПОВІЩЕННЯ ПРО ПОПЕРЕДНІЙ ВХІД (ДОСТУП) - НЕВДАЛІ СПРОБИ ВХОДУ ДО СИСТЕМИ

Сповіщати користувача, після успішного входу/доступу, про кількість невдалих спроб входу/доступу після останнього успішного входу/доступу.

Рекомендації з реалізації: Інформація про кількість невдалих спроб входу з моменту останнього успішного входу дозволяє користувачеві визначити, чи кількість невдалих спроб входу відповідає фактичним спробам користувача.

Пов’язані заходи: Немає.

(2) СПОВІЩЕННЯ ПРО ПОПЕРЕДНІЙ ВХІД (ДОСТУП) - УСПІШНІ ТА НЕВДАЛІ СПРОБИ ВХОДУ ДО СИСТЕМИ

Сповіщати користувача, після успішного входу/доступу до системи про кількість [*Вибір: успішних спроб доступу/входу; невдалих спроб входу/доступу; обидва варіанти*] за [*Призначення: визначений організацією період часу*].

Рекомендації з реалізації: Інформація про кількість успішних і невдалих спроб входу в систему протягом певного періоду часу дозволяє користувачеві визначити, чи кількість і тип спроб входу відповідають фактичним спробам користувача.

Пов’язані заходи: Немає.

(3) СПОВІЩЕННЯ ПРО ПОПЕРЕДНІЙ ВХІД (ДОСТУП) - ПОВІДОМЛЕННЯ ПРО ЗМІНИ В ОБЛІКОВОМУ ЗАПИСІ

Сповіщати користувача, після успішного входу/доступу, про внесення змін до [*Призначення: певних характеристик/параметрів облікового запису користувача, визначених організацією*] протягом [*Призначення: визначеного організацією періоду часу*].

Рекомендації з реалізації: Інформація про зміни в пов’язані із безпекою характеристиках облікового запису протягом визначеного періоду часу дозволяє користувачам розпізнати, чи зміни були внесені без їх відома.

Пов’язані заходи: Немає.

(4) СПОВІЩЕННЯ ПРО ПОПЕРЕДНІЙ ВХІД (ДОСТУП) - ДОДАТКОВА ІНФОРМАЦІЯ ПРО ВХІД

Повідомляти користувачеві, після успішного входу/доступу, наступну додаткову інформацію: [*Призначення: інформація, визначена організацією, яка повинна бути включена на додаток до дати та часу останнього входу/доступу*].

Рекомендації з реалізації: Це посилення заходу дозволяє визначати додаткову інформацію, яка повинна надаватися користувачам під час входу, включно з, наприклад, місцем останнього входу. Місцеперебування користувача — це інформація, яка може бути визначена системами, наприклад, адресами Інтернет-протоколу (IP), з яких відбулися входи в мережу, сповіщення локальних систем або ідентифікаторів пристроїв.

Пов’язані заходи: Немає.

Посилання: Немає.

## AC-10 УПРАВЛІННЯ ПАРАЛЕЛЬНОЮ СЕСІЄЮ

Заходи захисту:

Обмежити кількість одночасних сеансів для кожного [*Призначення: визначеного організацією облікового запису та/або типу облікового запису*] до [*Призначення:*

*визначеної організацією кількості*].

Рекомендації з реалізації: Організації можуть визначати максимальну кількість одночасних сеансів для облікових записів системи у всьому світі, за типом облікового запису, за самим обліковим записом або будь-якою їх комбінацією. Наприклад, організації можуть обмежити кількість одночасних сеансів для адміністраторів системи або інших осіб, які працюють в особливо чутливих доменах або критично важливих програмах. Керування одночасним сеансом стосується облікових записів системи, а не одночасні сеанси окремих користувачів через кілька облікових записів системи.

Пов'язані заходи: SC-23.

Посилення заходів: Немає.

Посилання: Немає.

## AC-11 БЛОКУВАННЯ ПРИСТРОЮ

Заходи захисту:

a. Заборонити подальший доступ до системи шляхом ініціювання блокування пристрою після [*Призначення: визначеного організацією періоду*] бездіяльності або після отримання запиту від користувача.

b. Зберігати блокування пристрою, поки користувач не відновить доступ, використовуючи встановлені процедури ідентифікації та автентифікації.

Рекомендації з реалізації: Блокування пристроїв — це тимчасові дії, що вживаються для запобігання доступу до інформаційних систем у разі, коли користувачі тимчасово припиняють виконання своїх повноважень, але не хочуть виходити із системи. Блокування пристроїв може бути реалізовано лише за можливості відстежування сеансів. Здебільшого це реалізується на рівні операційної системи, але може бути реалізовано на рівні програм. Блокування пристроїв не може бути дозволено як заміна виходу із системи в разі, коли є вимоги, наприклад щодо обов'язковості виходу із системи в кінці робочого дня.

Пов'язані заходи: AC-2, AC-7, IA-11, PL-4.

Посилення заходів:

(1) БЛОКУВАННЯ ПРИСТРОЮ - ПРИХОВАНІ ДИСПЛЕЇ

Приховувати, через блокування пристрою, інформацію, раніше видиму на дисплеї, із загальнодоступним зображенням.

Рекомендації з реалізації: На дисплеї блокування можуть відображатися статичні або динамічні зображення, візерунки, фотографічні зображення, суцільні кольори, годинник, індикатор ресурсу акумулятора чи порожній екран, який запобігає відображенню змістовно критичної інформації.

Пов'язані заходи: Немає.

Посилання: Немає.

## AC-12 ПРИПИНЕННЯ СЕАНСУ

Заходи захисту:

Сеанс користувача має завершуватися автоматично після [*Призначення: визначених організацією умов або тригерних подій, що вимагають припинення сеансу*].

Рекомендації з реалізації: На відміну від заходу SC-10 (який стосується відключення мережі), цей захід безпеки стосується припинення ініційованих користувачем логічних сеансів. Логічний сеанс (для локального, мережевого та віддаленого доступу) починається щоразу, коли користувач (або процес, що діє від імені користувача), отримує доступ до системи. Такі сеанси користувача можуть бути спинені без припинення мережевих сеансів. Закінчення сеансу припиняє всі процеси, пов'язані з логічним сеансом користувача, за винятком тих процесів, які спеціально створені користувачем (тобто власником сеансу) для продовження після закінчення сеансу. Умови або тригерні події, що вимагають автоматичного припинення сеансу, можуть містити визначені періоди бездіяльності користувача, реакції на певні типи інцидентів, обмеження часу використання системи.

Пов'язані заходи: MA-4, SC-10, SC-23.

Посилення заходів:

(1) ПРИПИНЕННЯ СЕАНСУ - ІНІЦІЙОВАНЕ КОРИСТУВАЧЕМ БЛОКУВАННЯ

Забезпечити можливість припинення сеансів зв'язку з ініціативи користувача, коли автентифікація використовується для отримання доступу до [*Призначення: визначених організацією інформаційних ресурсів*].

Рекомендації з реалізації: Інформаційні ресурси, до яких користувачі отримують доступ після процедури проходження автентифікації, можуть охоплювати локальні робочі станції, бази даних та захищені паролем вебсайти/вебсервіси.

Пов'язані заходи: Немає.

(2) ПРИПИНЕННЯ СЕАНСУ - ПОВІДОМЛЕННЯ ПРО ПРИПИНЕННЯ СЕАНСУ

Відобразити виразне повідомлення для користувача, що вказує на достовірне припинення автентифікованих сеансів зв'язку.

Рекомендації з реалізації: Повідомлення про припинення доступу до вебсторінок, наприклад, можуть відображатися після завершення сесій автентифікації. Однак для деяких типів інтерактивних сеансів, включно з сеансами протоколу передачі файлів (FTP), системи зазвичай надсилають повідомлення про припинення доступу у вигляді останніх повідомлень до завершення сеансів.

Пов'язані заходи: Немає.

(3) ПРИПИНЕННЯ СЕАНСУ - ЗАСТЕРЕЖНЕ ПОВІДОМЛЕННЯ ПРО ТЕ, ЩО ЧАС СЕСІЇ ДОБІГАЄ КІНЦЯ

Відобразити виразне повідомлення користувачам, що вказує, що сесія добігає кінця [*Завдання: визначений організацією час до кінця сесії*].

Рекомендації з реалізації: Для збільшення зручності можливо повідомити

користувачів про завершення поточного сеансу. У разі потреби продовження роботи користувач має направити запит на подовження сеансу. Період часу завершення сеансу, що очікує, базується на параметрах, визначених у базовому контролі AC-12.

Пов'язані заходи: Немає.

Посилання: Немає.

## AC-13 НАГЛЯД ТА ОГЛЯД — УПРАВЛІННЯ ДОСТУПОМ

[Вилучено: включено в AC-2 й AU-6].

## AC-14 ДОЗВОЛЕНІ ДІЇ БЕЗ ІДЕНТИФІКАЦІЇ АБО АВТЕНТИФІКАЦІЇ

Заходи захисту:

a. Визначити [*Призначення: дозволені організацією дії користувачів*], які можуть виконуватися в системі без ідентифікації або автентифікації відповідно до завдань та функцій організації.

b. Документувати та визначити відповідне обґрунтування в плані безпеки системи дій користувача, які не потребують ідентифікації або автентифікації.

Рекомендації з реалізації: Цей захід безпеки стосується ситуацій, коли визначено, що процедури ідентифікації або автентифікації не потрібні. Обмежена кількість дій користувачів (наприклад доступ до відкритих вебсайтів або доступ до інших відкритих систем, приймання телефонних дзвінків чи факсів). Також мають бути визначені дії, які зазвичай вимагають ідентифікації або автентифікації, але з певних обставин ці процедури можуть бути опущені (наприклад при доступі через фізичний бар'єр, який самостійно здатен забезпечити захист від несанкціонованого доступу). Цей захід безпеки повинен застосовуватися на етапі, коли процедури ідентифікації або автентифікації ще не були пройдені. Може бути визначено, що в системі немає допустимих дій користувачів, які не пройшли ідентифікацію та автентифікацію.

Пов'язані заходи: AC-8, IA-2, PL-2.

Посилення заходів: Немає.

(1) ДОЗВОЛЕНІ ДІЇ БЕЗ ІДЕНТИФІКАЦІЇ АБО АВТЕНТИФІКАЦІЇ - НЕОБХІДНЕ ВИКОРИСТАННЯ

[Вилучено: включено до AC-14].

Посилання: Немає.

## AC-15 АВТОМАТИЗОВАНЕ МАРКУВАННЯ

[Вилучено: включено до MP-3].

## AC-16 АТРИБУТИ БЕЗПЕКИ ТА ПРИВАТНОСТІ

Заходи захисту:

a. Визначити засоби для асоціювання (пов'язання) [*Призначення: визначених організацією типів атрибутів безпеки та приватності*], що приймають [*Призначення: визначені організацією значення атрибутів безпеки та приватності*] з інформацією, яка зберігається, обробляється та/або передається.

b. Пов'язані атрибути безпеки та приватності мають створюватися і зберігатися разом з інформацією.

c. Встановити дозволені [*Призначення: визначені організацією атрибути безпеки*] для [*Призначення: систем, визначених організацією*].

d. Визначити дозволені [*Призначення: визначені організацією значення або діапазони*] для кожного з встановлених атрибутів безпеки та приватності.

Рекомендації з реалізації: Інформація, яка міститься в системі, являє собою структури даних. Внутрішні структури даних можуть бути представлені двома видами сутностей: активні та пасивні. Активні сутності зазвичай називають суб'єктами — вони асоціюються з особами, пристроями або процесами, що діють від їхнього імені. Пасивними сутностями виступають об'єкти, які асоціюються зі структурами даних, такими як записи, буфери, таблиці, файли, порти зв'язку. Атрибути безпеки — це форма метаданих, що становлять основні властивості або характеристики активних і пасивних сутностей щодо захисту інформації. Атрибути приватності, які можуть використовуватися незалежно або в поєднанні з атрибутами безпеки, становлять основні властивості чи характеристики суб'єкта господарювання щодо персональних даних. Такі атрибути використовуються для забезпечення фіксації факту виконання обов'язків, зв'язку персональних даних всередині об'єктів даних та встановлення меж дозволеного використання особистої інформації. Атрибути можуть бути явно чи неявно пов'язані з інформацією, що міститься в системах або компонентах системи організації.

Атрибути безпеки та приватності призначаються активним сутностям (тобто суб'єктам), які можуть надсилати чи отримувати інформацію, ініціювати переміщення потоку інформації серед об'єктів або впливати на зміну стану системи. Ці атрибути можуть також бути пов'язані з пасивними сутностями (тобто об'єктами), які містять чи отримують інформацію. Призначення атрибутів безпеки та приватності суб'єктам або об'єктам є обов'язковим і не охоплює значення атрибута та його тип. Зв'язок атрибутів безпеки та приватності з даними чи інформацією дозволяє застосовувати політику безпеки для контролю доступу й управління потоком інформації, а також політику приватності, включно з обмеженнями щодо збереження даних та дозволеним використанням особистої інформації. Методи прив'язки визначаються особливостями системами та впливають на міцність зв'язку атрибутів з інформацією. Методи зв'язування можуть впливати на ступінь необхідних додаткових заходів. Зміст і значення атрибутів безпеки та приватності можуть безпосередньо впливати на доступність інформації.

Типи атрибутів повинні обиратися залежно від конкретної системи, враховуючи її місію та функції. Може бути наявний широкий діапазон значень конкретного атрибута безпеки. Назви атрибутів безпеки та приватності мають відображати їх зв'язок із сутностями та структурами даних системи. Це дозволяє реалізовувати політики безпеки та приватності. Назви можуть містити дозволи на доступ, національність, дані щодо захисту життєвого циклу (тобто шифрування та закінчення строку дії даних), згоди суб'єкта даних, дозволене використання даних, класифікацію інформації відповідно до законодавчих актів. З іншого боку, назви атрибутів безпеки та приватності мають бути зрозумілими для посадових осіб. Це дає змогу вручну виконувати положення політик безпеки та приватності на основі

ручного чи процедурного процесів.

Пов'язані заходи: AC-3, AC-4, AC-6, AC-21, AC-25, AU-2, AU-10, MP-3, PE-22, PT-2, PT-3, PT-4, SC-11, SC-16, SI-18, SI-12.

Посилення заходів:

(1) АТРИБУТИ БЕЗПЕКИ ТА ПРИВАТНОСТІ - ДИНАМІЧНЕ ПОВ'ЯЗАННЯ АТРИБУТІВ

Динамічно пов'язувати атрибути безпеки та приватності з *[Призначенням: визначеними організацією суб'єктами й об'єктами]* відповідно до *[Призначення: визначених організацією політик безпеки та приватності]*, у міру створення та об'єднання інформації.

Рекомендації з реалізації: Динамічне пов'язування атрибутів безпеки та приватності є доцільним, коли характеристики безпеки та приватності інформації можуть змінюватися з часом. Атрибути можуть змінюватися, наприклад, через проблеми агрегації інформації (у ситуаціях, коли характеристики безпеки та приватності окремих елементів інформації відрізняються від комбінованих елементів), зміни в індивідуальних дозволах доступу (тобто привілеях), зміни категорії безпеки інформації, зміни в політиці безпеки та приватності.

Пов'язані заходи: Немає.

(2) АТРИБУТИ БЕЗПЕКИ ТА ПРИВАТНОСТІ - ЗМІНА ЗНАЧЕНЬ АТРИБУТІВ АВТОРИЗОВАНИМИ ОСОБАМИ

Надати уповноваженим особам (або процесам, що діють від імені фізичних осіб) можливість визначати або змінювати значення відповідних атрибутів безпеки та приватності.

Рекомендації з реалізації: Зміст або значення атрибутів безпеки та приватності можуть безпосередньо впливати на здатність людей отримувати доступ до інформації. Тому важливо, щоб системи могли обмежувати можливість створювати або змінювати атрибути уповноваженим особам.

Пов'язані заходи: Немає.

(3) АТРИБУТИ БЕЗПЕКИ ТА ПРИВАТНОСТІ - ПІДТРИМКА СИСТЕМОЮ ПОВ'ЯЗАННЯ АТРИБУТІВ

Підтримати пов'язання та цілісність *[Призначення: визначених організацією атрибутів безпеки та приватності]* з *[Призначення: визначених організацією суб'єктів і об'єктів]*.

Рекомендації з реалізації: Підтримка пов'язання та цілісності атрибутів безпеки та приватності з достатньою впевненістю допомагає забезпечити використання пов'язання атрибутів як основи автоматизованих дій, визначених політикою. Такі автоматизовані дії можуть впливати на терміни зберігання, терміни надання доступу та рішення щодо управління потоком інформації.

Пов'язані заходи: Немає.

(4) АТРИБУТИ БЕЗПЕКИ ТА ПРИВАТНОСТІ - ПОВ'ЯЗАННЯ АТРИБУТІВ АВТОРИЗОВАНИМИ ОСОБАМИ

Впровадити можливість пов'язувати [*Призначення: визначені організацією атрибути безпеки та приватності*] з [*Призначення: визначеними організацією суб'єктами та об'єктами*] уповноваженими особами (або процесами, що діють від імені фізичних осіб).

Рекомендації з реалізації: Система має надавати можливість спонукання користувачів вибирати конкретні атрибути безпеки або приватності, які будуть пов'язані з конкретними інформаційними об'єктами; використання автоматизованих механізмів для категоризації інформації за відповідними атрибутами безпеки та приватності на основі визначених політик; або забезпечення валідності комбінації вибраних атрибутів безпеки чи приватності. Об'єднання атрибутів уповноваженими особами описано в проектній документації. Підтримка, що надається системами, може включати запити користувачів щодо вибору атрибутів безпеки та конфіденційності, які будуть пов'язані з інформаційними об'єктами, використання автоматизованих механізмів для класифікації інформації за допомогою атрибутів на основі визначених політик або забезпечення того, що комбінація вибраних атрибутів безпеки та конфіденційності є дійсною. Під час визначення подій, які підлягають перевірці, організації враховують створення, видалення або зміну атрибутів

Пов'язані заходи: Немає.

(5) АТРИБУТИ БЕЗПЕКИ ТА ПРИВАТНОСТІ - ВІДОБРАЖЕННЯ АТРИБУТІВ НА ПРИСТРОЯХ ВИВЕДЕННЯ

Відображати атрибути безпеки та приватності в зручній для людини формі для кожного об'єкту, який система передає на пристрої виведення, щоб ідентифікувати *[Призначення: визначені організацією спеціальні інструкції щодо поширення, обробки чи наступного розподілу інформації]*, використовуючи *[Призначення: визначену організацією ідентифікацію, у зручній для людини формі про стандартні угоди про присвоєння імен]*.

Рекомендації з реалізації: До виходів системи можуть належати екрани, сторінки тощо. Пристрої виведення системи можуть містити принтери, ноутбуки, відеодисплеї на робочих станціях та персональні цифрові помічники. Для запобігання несанкціонованому доступу (наприклад методом підглядання, англ. «shoulder surfing») на екрані пристрою виведення має відображатися повне значення атрибутів (крім випадків, якщо значення атрибутів також має гриф доступу).

Пов'язані заходи: Немає.

(6) АТРИБУТИ БЕЗПЕКИ ТА ПРИВАТНОСТІ - ПІДТРИМКА ПОВ'ЯЗАННЯ АТРИБУТІВ ОРГАНІЗАЦІЄЮ

Вимагати від персоналу пов'язувати та підтримувати асоціацію *[Призначення: визначених організацією атрибутів безпеки та приватності]* з *[Призначенням: визначеними організацією суб'єктами та об'єктами]* відповідно до *[Призначення: визначеної організацією політики безпеки та приватності]*.

Рекомендації з реалізації: Це посилення заходу вимагає від окремих користувачів (на відміну від системи) підтримувати пов'язування атрибутів

безпеки та приватності із суб'єктами та об'єктами.

Пов'язані заходи: Немає.

(7) АТРИБУТИ БЕЗПЕКИ ТА ПРИВАТНОСТІ - ПОСЛІДОВНА ІНТЕРПРЕТАЦІЯ АТРИБУТІВ

Забезпечити послідовну інтерпретацію атрибутів безпеки та приватності, що передаються між розподіленими компонентами системи.

Рекомендації з реалізації: Для застосування політики безпеки та приватності в різних компонентах розподілених систем, атрибутам доступу має надаватися послідовна інтерпретація. Мають бути впроваджені процеси для забезпечення реалізації атрибутів безпеки та приватності з послідовною інтерпретацією щодо автоматизованого доступу та управління потоком інформації для всіх компонентів розподіленої системи.

Пов'язані заходи: Немає.

(8) АТРИБУТИ БЕЗПЕКИ ТА ПРИВАТНОСТІ - ТЕХНІКИ ТА ТЕХНОЛОГІЇ ПОВ'ЯЗАННЯ АТРИБУТІВ

Реалізація [*Призначення: методи та технології, визначені організацією*] для пов'язування атрибутів безпеки та конфіденційності з інформацією.

Рекомендації з реалізації: Прив'язка атрибутів безпеки та приватності до інформації є важливою для проведення автоматизованих дій щодо забезпечення доступу та виконання потоків. Об'єднання таких атрибутів може бути досягнуто за допомогою технологій і технік, які забезпечують різні рівні впевненості. Наприклад, можуть використовуватися криптографічні методи, такі як цифрові підписи (за умови надійного зберігання ключових даних на захищених апаратно-програмних носіях).

Пов'язані заходи: SC-12, SC-13.

(9) АТРИБУТИ БЕЗПЕКИ ТА ПРИВАТНОСТІ - ПЕРЕПРИЗНАЧЕННЯ АТРИБУТІВ

Перепризначення атрибутів безпеки та приватності, пов'язаних з інформацією, здійснювати лише за допомогою механізмів перегляду, перевірених з використанням *[Призначення: визначених організацією технік або процедур]*.

Рекомендації з реалізації: Для забезпечення необхідного рівня впевненості в коректності перепризначення атрибутів безпеки та приватності мають діяти затверджені механізми перегляду. Це досягається за умови, що такі механізми перегляду мають єдину мету та обмежений набір функцій. Перепризначення атрибутів може безпосередньо впливати на заходи щодо забезпечення безпеки та приватності, тому використання надійних механізмів перегляду необхідне для забезпечення ефективності таких механізмів у послідовному та правильному режимі роботи.

Пов'язані заходи: Немає.

(10) АТРИБУТИ БЕЗПЕКИ ТА ПРИВАТНОСТІ - КОНФІГУРАЦІЯ АТРИБУТІВ УПОВНОВАЖЕНИМИ ОСОБАМИ

Надати уповноваженим особам можливість визначати або змінювати тип і значення атрибутів безпеки та приватності, доступних для пов'язання із суб'єктами та об'єктами.

Рекомендації з реалізації: Тип або значення атрибутів безпеки та приватності можуть безпосередньо впливати на здатність людей отримувати доступ до інформації. Важливо мати можливість обмежувати створювання або зміну атрибутів лише авторизованими особами.

Пов'язані заходи: Немає.

Посилання: FIPS Publications 140-2, 186-4. [OMB A-130], [FIPS 140-3], [FIPS 186-4], [SP 800-162], [SP 800-178].

## AC-17 ВІДДАЛЕНИЙ ДОСТУП

Заходи захисту:

a. Встановити та задокументувати обмеження на використання, вимоги до конфігурації/підключення та рекомендації щодо здійснення кожного типу віддаленого доступу.

b. Авторизувати віддалений доступ до системи, перш ніж будуть дозволені такі підключення.

Рекомендації з реалізації: Віддалений доступ — це доступ до систем організації (або процесів, що діють від імені користувачів), який відбувається через зовнішні мережі, такі як Інтернет. Методи віддаленого доступу можуть містити комутований, широкосмуговий і бездротовий доступ. Для підвищення конфіденційності та цілісності можуть використовуватися зашифровані VPN з'єднання. Використання зашифрованих VPN забезпечує достатню впевненість, що використовувані криптографічні механізми будуть реалізовані відповідно до чинного законодавства, виконавчих розпоряджень, директив, положень, політик, стандартів і рекомендацій. Проте VPN з'єднання проходять через зовнішні мережі, а зашифровані VPN погіршують доступність віддалених з'єднань. VPN з'єднання із зашифрованими тунелями також можуть впливати на можливість адекватного контролю трафіку мережевих комунікацій на предмет зловмисного коду. Управління віддаленим доступом має застосовуватися до всіх систем, за винятком загальнодоступних (включно з вебсерверами). Авторизація кожного типу віддаленого доступу стосується авторизації перед дозволом віддаленого доступу без визначення конкретних форматів для такої авторизації. У той час як організації можуть використовувати обмін інформацією та угоди про безпеку підключення до системи для керування віддаленим доступом до інших систем, такі угоди розглядаються як частина CA-3. Цей захід контролю вимагає наявність процедури авторизації перед використанням віддаленого доступу (проте не вказує на конкретні механізми авторизації). Обмеження, що стосуються віддаленого доступу, наведені в AC-3.

Пов'язані заходи: AC-2, AC-3, AC-4, AC-18, AC-19, AC-20, CA-3 CM-10, IA-2, IA-3, IA-8, MA-4, PE-17, PL-2, PL-4, SC-10, SC-12, SC-13, SI-4.

Посилення заходів:

(1) ВІДДАЛЕНИЙ ДОСТУП - АВТОМАТИЗОВАНИЙ МОНІТОРИНГ ТА УПРАВЛІННЯ

Проводити моніторинг та управління методами віддаленого доступу.

Рекомендації з реалізації: Автоматизований моніторинг і управління методами віддаленого доступу дозволяють виявляти атаки та забезпечувати відповідність політиці віддаленого доступу, шляхом перевірки діяльності віддалених користувачів на різних компонентах системи, включно із серверами, робочими станціями, ноутбуками, смартфонами та планшетами. Журнал аудиту для віддаленого доступу забезпечується AU-2. Події аудиту визначені в AU-2a.

Пов'язані заходи: AU-2, AU-6, AU-12, AU-14.

(2) ВІДДАЛЕНИЙ ДОСТУП - ЗАХИСТ КОНФІДЕНЦІЙНОСТІ ТА ЦІЛІСНОСТІ ЗА ДОПОМОГОЮ ШИФРУВАННЯ

Запровадити криптографічні механізми для захисту конфіденційності та цілісності сесій віддаленого доступу.

Рекомендації з реалізації: Надійність механізму шифрування має вибиратися, виходячи з результатів процедури категоризації оброблюваної інформації.

Пов'язані заходи: SC-8, SC-12, SC-13.

(3) ВІДДАЛЕНИЙ ДОСТУП - КЕРОВАНІ ТОЧКИ КОНТРОЛЮ ДОСТУПУ

Виконувати маршрутизацію всього віддаленого доступу через авторизовані та керовані точки контролю управління доступом до мережі.

Рекомендації з реалізації: Обмеження переліку точок контролю доступу для віддаленого доступу зменшує кількість вразливих до атак точок.

Пов'язані заходи: SC-7.

(4) ВІДДАЛЕНИЙ ДОСТУП - ПРИВІЛЕЙОВАНІ КОМАНДИ ТА ДОСТУП

(a) Авторизувати виконання привілейованих команд і доступ до інформації, що стосується безпеки, за допомогою віддаленого доступу тільки для [*Призначення: визначених організацією потреб*];

(b) Задокументувати обґрунтування такого доступу в плані захисту інформації для системи

Рекомендації з реалізації: Віддалений доступ до систем є значною потенційною вразливістю, якою можуть скористатися зловмисники. Таким чином, обмеження виконання привілейованих команд і доступу до інформації, важливої для безпеки, через віддалений доступ зменшує вразливість організації та сприйнятливість до загроз з боку зловмисників.

Пов'язані заходи: AC-6, SC-12, SC-13.

(5) ВІДДАЛЕНИЙ ДОСТУП - МОНІТОРИНГ ДЛЯ НЕАВТОРИЗОВАНИХ ПІДКЛЮЧЕНЬ

[Вилучено: включено до SI-4].

(6) ВІДДАЛЕНИЙ ДОСТУП - ЗАХИСТ ІНФОРМАЦІЇ

Забезпечити захист інформації щодо механізмів віддаленого доступу від неавторизованого використання та розкриття.

Рекомендації з реалізації: Віддалений доступ до інформації іншими організаціями може збільшити ризик несанкціонованого використання та розголошення механізмів віддаленого доступу. За можливості розглядається можливість включення вимог віддаленого доступу в угоди про обмін інформацією з такими організаціями. Вимоги щодо віддаленого доступу також можуть бути включені в правила поведінки (див. PL-4) і угоди про доступ (див. PS-6).

Пов'язані заходи: AT-2, AT-3, PS-6.

(7) ВІДДАЛЕНИЙ ДОСТУП - ДОДАТКОВИЙ ЗАХИСТ ДЛЯ ДОСТУПУ ДО ФУНКЦІЙ БЕЗПЕКИ

[Вилучено: включено до AC-3(10)].

(8) ВІДДАЛЕНИЙ ДОСТУП - ДЕАКТИВАЦІЯ НЕЗАХИЩЕНИХ ПРОТОКОЛІВ МЕРЕЖІ

[Вилучено: включено до CM-7].

(9) ВІДДАЛЕНИЙ ДОСТУП - ВІДКЛЮЧЕННЯ АБО ДЕАКТИВАЦІЯ ДОСТУПУ

Забезпечити можливість швидкого відключення або деактивації віддаленого доступу до системи в межах [*Призначення: визначеного організацією періоду часу*].

Рекомендації з реалізації: Це посилення заходу вимагає наявності можливості швидко від'єднувати поточних користувачів, віддалено отримуючи доступ до системи, або деактивувати подальший віддалений доступ. Швидкість відключення або деактивації може змінюватися залежно від критичності місій або функцій і необхідності усунення негайного чи майбутнього віддаленого доступу до систем.

Пов'язані заходи: Немає.

Посилання: Немає.

(10) АВТЕНТИФІКАЦІЯ ВІДДАЛЕНИХ КОМАНД

Запровадити [*Призначення: механізми, визначені організацією*] для автентифікації [*Призначення: віддалені команди, визначені організацією*]

Рекомендації з реалізації: Автентифікація віддалених команд захищає від несанкціонованих команд і повторного відтворення авторизованих команд. Здатність автентифікувати віддалені команди важлива для віддалених систем, для яких втрата, несправність, неправильне спрямування або використання можуть мати негайні або серйозні наслідки, такі як травми, смерть, пошкодження майна, втрата цінних активів, збій місії або бізнес-функцій, або компрометація секретної чи контрольованої несекретної інформації. Механізми автентифікації для віддалених команд гарантують, що системи приймають і виконують команди в передбаченому порядку, виконують лише авторизовані команди та відхиляють несанкціоновані команди. Як приклад, можна

використовувати для автентифікації віддалених команд криптографічні механізми.

Пов'язані заходи: SC-12, SC-13, SC-23.

Посилання: [SP 800-46], [SP 800-77], [SP 800-113], [SP 800-114], [SP 800-121], [IR 7966].

## AC-18 БЕЗДРОТОВИЙ ДОСТУП

Заходи захисту:

a. Установити обмеження на використання, вимоги до конфігурації/підключення та рекомендації щодо здійснення бездротового доступу.

b. Авторизувати бездротовий доступ до системи, перш ніж будуть дозволені такі підключення.

Рекомендації з реалізації: До бездротових технологій належать: використання мікрохвиль, пакетний радіозв'язок, положення стандартів 802.11x та Bluetooth. Бездротові мережі використовують протоколи автентифікації, які забезпечують захист облікових даних і взаємну автентифікацію.

Повязані заходи: AC-2, AC-3, AC-17, AC-19, CA-9, CM-7, IA-2, IA-3, IA-8, PL-4, SC-40, SC-43, SI-4.

Посилення заходів:

(1) БЕЗДРОТОВИЙ ДОСТУП - АВТЕНТИФІКАЦІЯ ТА ШИФРУВАННЯ

Забезпечити захист бездротового доступу до системи за допомогою автентифікації [*Вибір (один або кілька): користувачів; пристроїв*] та шифрування.

Рекомендації з реалізації: Бездротові мережі є значною потенційною вразливістю, якою можуть скористатися зловмисники. Щоб захистити системи з бездротовими точками доступу, надійна автентифікація користувачів і пристроїв разом із надійним шифруванням може зменшити сприйнятливість до загроз з боку зловмисників.

Пов'язані заходи: SC-8, SC-12, SC-13.

(2) БЕЗДРОТОВИЙ ДОСТУП - МОНІТОРИНГ НЕАВТОРИЗОВАНИХ ПІДКЛЮЧЕНЬ

[Вилучено: включено до SI-4].

(3) БЕЗДРОТОВИЙ ДОСТУП - ВІДКЛЮЧЕННЯ БЕЗДРОТОВОЇ МЕРЕЖІ

Відключати, у разі відсутності необхідності у використанні, вбудовані в системні компоненти можливості бездротових мереж до їх виклику та розгортання.

Рекомендації з реалізації: Бездротові мережі, вбудовані в системні компоненти, є значною потенційною вразливістю, якою можуть скористатися зловмисники. Вимкнення бездротових можливостей, коли вони не потрібні для виконання важливих місій або функцій організації, може зменшити сприйнятливість до

загроз з боку зловмисників.

Пов'язані заходи: Немає.

(4) БЕЗДРОТОВИЙ ДОСТУП - ОБМЕЖЕННЯ НАЛАШТУВАННЯ КОРИСТУВАЧАМИ

Встановити та явно авторизувати користувачів, яким дозволено самостійно налаштовувати можливості бездротових мереж.

Рекомендації з реалізації: Уповноваженим користувачам може бути дозволено налаштовувати можливості бездротових мереж у рамках чинних механізмів управління доступом.

Пов'язані заходи: SC-7, SC-15.

(5) БЕЗДРОТОВИЙ ДОСТУП - АНТЕНИ ТА РІВЕНЬ ПОТУЖНОСТІ ПЕРЕДАЧІ

Вибрати радіоантени та калібрувати рівень потужності передачі, щоб зменшити ймовірність того, що сигнали від бездротових точок доступу можуть бути отримані за межами контрольованих організацією меж.

Рекомендації з реалізації: Дії, що можуть бути вжиті для обмеження несанкціонованого використання бездротового зв'язку поза межами контрольованих меж, охоплюють: зменшення потужності бездротових передач (для зниження ймовірності випромінювання сигналу поза фізичним периметром організації); застосування заходів контролю бездротових випромінювань; використання спрямованих або променевих форматних антен, які знижують імовірність того, що сторонні приймачі зможуть перехоплювати сигнали.

Пов'язані заходи: PE-19.

Посилання: [SP 800-94], [SP 800-97].

## AC-19 КОНТРОЛЬ ДОСТУПУ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ

Заходи захисту:

a. Встановити обмеження на використання, вимоги до конфігурації, вимоги до підключення і рекомендації щодо впровадження мобільних пристроїв, контрольованих організацією.

b. Авторизувати підключення мобільних пристроїв до систем, які експлуатуються організацією.

Рекомендації з реалізації: Мобільний пристрій — це обчислювальний пристрій, який: має малий форм-фактор; може легко транспортуватися однією особою; призначений для роботи без фізичного з'єднання; володіє локальним сховищем даних; має автономне джерело живлення. Функціональність мобільного пристрою може містити можливості голосового зв'язку, вбудовані датчики, які дозволяють пристрою отримувати інформацію, та/або вбудовані функції для синхронізації місцевих даних. Прикладами можуть виступати смартфони, електронні зчитувачі та планшети. Мобільні пристрої, як правило, асоціюються з однією особою, і зазвичай мобільний пристрій перебуває поруч з особою. Однак ступінь близькості може змінюватися залежно від форм-фактора та розміру пристрою. Контрольовані райони — це зони, для

яких може бути забезпечена відповідність вимогам, встановленим для захисту інформації та систем (за допомогою фізичних чи процедурних заходів).

Через велику різноманітність мобільних пристроїв з різними характеристиками та можливостями організаційні обмеження можуть відрізнятися для різних класів/типів таких пристроїв. Обмеження використання мобільних пристроїв можуть містити: управління конфігурацією, ідентифікацію та автентифікацію пристрою, інсталяцію (з подальшим обов'язковим оновленням) обов'язкового антивірусного програмного забезпечення, сканування пристроїв на наявність шкідливого коду, сканування критичних оновлень програмного, проведення перевірок цілісності первинної операційної системи (та, можливо, іншого програмного забезпечення) та відключення зайвого обладнання.

Обмеження щодо використання та дозвіл на підключення можуть залежати від конкретних систем. Наприклад, підключення мобільних пристроїв до організаційної мережі може бути дозволено при виконанні набору обмежень щодо використання, або система може відмовитись від авторизації підключення мобільних пристроїв до конкретних програм, або система може встановити додаткові обмеження використання перед тим, як дозволити підключення мобільних пристроїв до системи. Питання забезпечення належної безпеки для мобільних пристроїв виходить за рамки вимог цього заходу безпеки. Багато вимог для мобільних пристроїв містяться в інших засобах безпеки (передбачається виділення на початку вихідних точок для розробки планів безпеки з подальшою адаптацією). Захід безпеки AC-20 стосується мобільних пристроїв, які не контролюються організацією.

Пов'язані заходи: AC-3, AC-4, AC-7, AC-11, AC-17, AC-18, AC-20, CA-9, CM-2, CM-6, IA-2, IA-3, MP-2, MP-4, MP-5, MP-7, PL-4, SC-7, SC-34, SC-43, SI-3, SI-4.

Посилення заходів:

(1) КОНТРОЛЬ ДОСТУПУ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ - ВИКОРИСТАННЯ ЗАПИСУВАНИХ ТА ПЕРЕНОСНИХ ЗАПАМ'ЯТОВУВАЛЬНИХ ПРИСТРОЇВ

[Вилучено: включено до MP-7].

(2) КОНТРОЛЬ ДОСТУПУ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ - ВИКОРИСТАННЯ ПЕРСОНАЛЬНИХ ПЕРЕНОСНИХ ЗАПАМ'ЯТОВУВАЛЬНИХ ПРИСТРОЇВ

[Вилучено: включено до MP-7].

(3) КОНТРОЛЬ ДОСТУПУ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ - ВИКОРИСТАННЯ ПЕРЕНОСНИХ ЗАПАМ'ЯТОВУВАЛЬНИХ ПРИСТРОЇВ З НЕІДЕНТИФІКОВАНИМ ВЛАСНИКОМ

[Вилучено: включено до MP-7].

(4) КОНТРОЛЬ ДОСТУПУ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ - ОБМЕЖЕННЯ ДЛЯ ЗАСЕКРЕЧЕНОЇ ІНФОРМАЦІЇ

a) Заборонити використання незахищених мобільних пристроїв на об'єктах, де експлуатуються системи, що обробляють, зберігають або передають секретну інформацію, якщо це спеціально не дозволено уповноваженою особою.

b) Забезпечити наступні обмеження на осіб, яким дозволено уповноваженою особою використовувати незахищені мобільні пристрої в установах, що містять системи обробки, зберігання або передачі секретної інформації:

(1) підключення незахищених мобільних пристроїв до засекречених систем заборонено;

(2) підключення незахищених мобільних пристроїв до незасекречених систем вимагає схвалення уповноваженої посадової особи;

(3) використання внутрішніх або зовнішніх модемів або бездротових інтерфейсів у незахищених мобільних пристроях заборонено;

(4) незахищені мобільні пристрої та інформація, що зберігається на цих пристроях, підлягають випадковим перевіркам та перевіркам [*Призначення: визначеними організацією посадовими особами із захисту інформації*], і якщо секретна інформація знайдена, застосовується політика обробки інцидентів.

c) Обмежити підключення захищених мобільних пристроїв до засекречених систем відповідно до [*Призначення: визначеної організацією політики безпеки*].

Рекомендації з реалізації: Немає.

Пов'язані заходи: CM-8, IR-4.

(5) КОНТРОЛЬ ДОСТУПУ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ - ПОВНЕ ШИФРУВАННЯ ПРИСТРОЇВ ТА СХОВИЩ ІНФОРМАЦІЇ

Організація має застосувати [*Вибір: повне шифрування пристроїв; шифрування сховищ інформації*] для захисту конфіденційності та цілісності інформації на [*Призначення: визначених організацією мобільних пристроях*].

Рекомендації з реалізації: Шифрування на основі контейнерів забезпечує тонший підхід до шифрування даних/інформації на мобільних пристроях, включно з, наприклад, шифруванням вибраних структур даних, таких як файли, записи чи поля.

Пов'язані заходи: SC-13, SC-28.

Посилання: [SP 800-114], [SP 800-124].

## AC-20 ВИКОРИСТАННЯ ЗОВНІШНІХ СИСТЕМ

Заходи захисту:

a. [*Вибір (один або кілька): Встановіть [Призначення: умови, визначені організацією*]; Визначте [*Призначення: визначені організацією засоби контролю, які, як стверджується, будуть реалізовані на зовнішніх системах*]], узгоджені з довірчими відносинами, встановленими з іншими організаціями, які володіють, експлуатують та/або обслуговують зовнішні системи, дозволяючи уповноваженим особам:

1. доступ до системи із зовнішніх систем;

2. обробляти, зберігати або передавати керовану організацією інформацію за допомогою зовнішніх систем;

b. Заборонити використання [*Призначення: організаційно-визначені типи зовнішніх систем*].

Рекомендації з реалізації: Зовнішні системи — це системи або компоненти систем, які перебувають поза авторизованими межами, встановленими організаціями, і щодо яких організації, як правило, не мають безпосередньої можливості нагляду та повноважень щодо застосування необхідного заходу безпеки або оцінювання його ефективності. До зовнішніх систем належать: персональні системи, компоненти або пристрої; приватні обчислювальні пристрої та пристрої зв'язку в комерційних або громадських об'єктах; системи, що належать або контролюються недержавними організаціями; а також державні системи, які не перебувають у власності, під управлінням або під безпосереднім наглядом організації. Цей захід безпеки стосується використання зовнішніх систем для обробки, зберігання або передачі організаційної інформації, включно з, наприклад, доступом до хмарних служб.
Для деяких зовнішніх систем (тобто систем, якими керують інші відомства та організації, підпорядковані ним), довірчі відносини, що були встановлені між ними, можуть не містити чітких умов. Системи в межах цих організацій не можна вважати зовнішніми (наприклад, коли між такими організаціями наявні попередні угоди чи коли такі відносини регулюються чинним законодавством, директивами або іншими розпорядженнями). До уповноважених осіб належать штатні працівники, підрядники або інші особи, які мають дозвіл на доступ до систем організації і щодо яких організації мають право встановлювати конкретні правила поведінки щодо доступу до системи. Обмеження, які накладаються на уповноважених осіб, не повинні бути уніфікованими, оскільки ці обмеження можуть змінюватися залежно від довірчих відносин.
Цей захід безпеки не застосовується до зовнішніх систем, які використовуються для доступу до публічних інтерфейсів до систем організації. Конкретні умови використання зовнішніх систем мають бути встановлені відповідно до політик і заходів безпеки. Загальні положення та умови мають стосуватися: конкретних типів застосунків, до яких в системах організації можна отримати доступ із зовнішніх систем; найвищої категорії безпеки інформації, яка може оброблятися, зберігатися або передаватися в зовнішніх системах. Також можуть бути накладені додаткові обмеження на працівників, які можуть використовувати зовнішні системи.

Пов'язані заходи: AC-2, AC-3, AC-17, AC-19, CA-3, PL-2, PL-4, SA-9, SC-7.

Посилення заходів:

(1) ВИКОРИСТАННЯ ЗОВНІШНІХ СИСТЕМ - ОБМЕЖЕННЯ НА АВТОРИЗОВАНЕ ВИКОРИСТАННЯ

Дозволити авторизованим особам використовувати зовнішню систему для доступу до системи або для обробки, зберігання чи передачі інформації, що контролюється організацією, лише після:

a) перевірки виконання необхідних заходів безпеки та приватності щодо зовнішніх систем, як зазначено в політиці безпеки та приватності організації, а також планах безпеки та приватності;

b) збереження погоджених угод про підключення або обробку системи з організаційною структурою, на якій розміщена зовнішня система.

Рекомендації з реалізації: Це посилення заходу регулює випадки, коли користувачам, які використовують зовнішні системи, потрібно отримати доступ до систем організації. У таких ситуаціях необхідні гарантії наявності в зовнішніх системах необхідних заходів безпеки, які мінімізують можливі наслідки (компрометація, пошкодження) на організаційну систему. Перевірка того, що необхідний захід безпеки впроваджено, може бути проведена, наприклад, шляхом зовнішнього незалежного оцінювання, атестацією чи в інший спосіб, залежно від рівня довіри.

Пов'язані заходи: CA-2.

(2) ВИКОРИСТАННЯ ЗОВНІШНІХ СИСТЕМ - ПЕРЕНОСНІ ПРИСТРОЇ ЗБЕРІГАННЯ ДАНИХ

Обмежити використання портативних пристроїв зберігання даних авторизованими особами на зовнішніх системах за допомогою [*Призначення: обмеження, визначені організацією*].

Рекомендації з реалізації: Обмеження на використання переносних пристроїв зберігання даних у зовнішніх системах можуть містити повну заборону використання таких пристроїв або обмеження їхнього використання за визначених умов.

Пов'язані заходи: MP-7, SC-41.

(3) ВИКОРИСТАННЯ ЗОВНІШНІХ СИСТЕМ - СИСТЕМИ ТА КОМПОНЕНТИ, ЩО НЕ ПЕРЕБУВАЮТЬ У ВЛАСНОСТІ ОРГАНІЗАЦІЇ

Обмежити використання систем або компонентів системи, які не перебувають у власності організації, для обробки, зберігання або передачі організаційної інформації за допомогою [*Призначення: обмеження, визначені організацією*]

Рекомендації з реалізації: До систем або компонентів, що не перебувають у власності організації, належать такі, що є власністю інших організацій, а також персональні системи та компоненти. Використання систем або компонентів, що не належать організації, несе потенційні ризики (у деяких випадках ризик є досить високим і треба повністю заборонити використання систем або компонентів, що не належать організації; в інших випадках використання таких систем або компонентів може бути дозволено з певними обмеженнями). Обмеження можуть містити вимоги до: впровадження затвердженого заходу безпеки та приватності; обмеження доступу до певних типів інформації, послуг чи застосунків; обмеження діяльності з обробки та зберігання на серверах або інших компонентах системи, передбачених організацією.

Пов'язані заходи: Немає.

(4) ВИКОРИСТАННЯ ЗОВНІШНІХ СИСТЕМ - ПРИСТРОЇ ДЛЯ ЗБЕРІГАННЯ ДАНИХ, ЯКІ МОЖУТЬ МАТИ ДОСТУП ДО МЕРЕЖІ

Заборонити використання [*Призначення: визначених організацією пристроїв для зберігання даних, які можуть мати доступ до мережі*] у зовнішніх системах.

Рекомендації з реалізації: До пристроїв для зберігання даних, які можуть мати доступ до мережі, належать онлайн-пристрої зберігання даних у загальнодоступних, гібридних або приватних хмарних системах.

Пов’язані заходи: Немає.

(5) ВИКОРИСТАННЯ ЗОВНІШНІХ СИСТЕМ - ПОРТАТИВНІ ПРИСТРОЇ ДЛЯ ЗБЕРІГАННЯ ДАНИХ – ЗАБОРОНА ВИКОРИСТАННЯ

Заборонити використання уповноваженими особами портативних пристроїв зберігання даних, підконтрольних організації, у зовнішніх системах.

Рекомендації з реалізації: Обмеження на використання портативних пристроїв зберігання даних, підконтрольних організації, у зовнішніх системах включає повну заборону на використання таких пристроїв. Заборона такого використання забезпечується за допомогою технічних та/або нетехнічних методів.

Пов’язані заходи: MP-7, PL-4, PS-6, SC-41.

Посилання: [FIPS 199], [SP 800-171], [SP 800-172].

## AC-21 РОЗПОВСЮДЖЕННЯ ІНФОРМАЦІЇ

Заходи захисту:

a. Спростити обмін інформацією, надаючи авторизованим користувачам змогу визначати, чи відповідають повноваження на доступ, що призначені партнерам для обміну, обмеженням доступу та повноваженням з приватності щодо інформації для [*Призначення: визначених організацією обставин обміну інформацією, коли це необхідно користувачу*].

b. Використовувати [*Призначення: визначені організацією автоматизовані механізми або ручні процеси*], щоб допомогти користувачам в ухваленні рішень щодо обміну інформацією та співпраці.

Рекомендації з реалізації: Цей захід безпеки застосовується до інформації, доступ до якої може бути певним чином обмежений на основі формального чи адміністративного заходу. Прикладами такої інформації може бути: інформація, що стосується договорів; конфіденційна інформація; інформація, що стосується спеціальних програм або відділень доступу; привілейована медична інформація та особиста інформація. Віднесення інформації до одного з перерахованих типів можливо на основі аналізу можливих ризиків у разі компрометації таких даних, а також за результатами аналізу впливу на приватність у разі настання таких інцидентів. Залежно від обставин обміну інформацією, спільне використання інформації може бути обмежене в рамках організації чи групи користувачів, або можуть бути визначені лише конкретні авторизовані особи, які можуть мати доступ до такої інформації.

Пов’язані заходи: AC-3, AC-4, AC-16, PT-2, PT-7, RA-3, SC-15.

Посилення заходів:

(1) РОЗПОВСЮДЖЕННЯ ІНФОРМАЦІЇ - АВТОМАТИЧНА ПІДТРИМКА УХВАЛЕННЯ РІШЕНЬ

Використовувати [*Призначення: автоматизовані механізми, визначені організацією*], щоб забезпечити виконання рішень щодо обміну інформацією авторизованими користувачами на основі авторизації доступу партнерів з обміну та обмежень доступу до інформації що підлягає обміну.

Рекомендації з реалізації: Немає.

Пов'язані заходи: Немає.

(2) РОЗПОВСЮДЖЕННЯ ІНФОРМАЦІЇ - ПОШУК І ПЕРЕВІРКА ІНФОРМАЦІЇ

Впровадити сервіси пошуку та перевірки інформації, які забезпечують [*Призначення: визначені організацією обмеження обміну інформацією*].

Рекомендації з реалізації: Служби пошуку та відновлення інформації ідентифікують ресурси інформаційної системи, що відповідають інформаційній потребі.

Пов'язані заходи: Немає.

Посилання: [OMB A-130], [SP 800-150], [IR 8062].

## AC-22 ПУБЛІЧНО ДОСТУПНИЙ КОНТЕНТ

Заходи захисту:

a. Призначити осіб, що уповноважені на розміщення інформації в загальнодоступній системі.

b. Навчати уповноважених осіб тому, щоб загальнодоступна інформація не містила інформацію з обмеженим доступом.

c. Переглядати запропонований зміст інформації до публікації в загальнодоступній системі, щоб гарантувати, що там не міститься інформація з обмеженим доступом.

d. Переглядати вміст загальнодоступної системи на предмет наявності там інформації з обмеженим доступом з [*Призначення: визначеною організацією частотою*]; така інформація має бути видалена в разі її виявлення.

Рекомендації з реалізації: Відповідно до чинного законодавства, наказів, директив, політик, громадськість не має права доступу до непублічної інформації. Цей захід безпеки стосується систем, які контролюються організацією та надають доступ до неї населенню здебільшого без процедур ідентифікації чи автентифікації. Правила розміщення інформації на базі систем, що не належать організації, мають базуватися на політиках організації.

Пов'язані заходи: AC-3, AT-2, AT-3, AU-13.

Посилення заходів: Немає.

Посилання: Немає.

## AC-23 ЗАХИСТ ВІД НЕСАНКЦІОНОВАНОГО ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ДАНИХ

Заходи захисту:

Використовувати [*Призначення: визначені організацією техніки виявлення та попередження витоку даних*] для [*Призначення: визначених організацією об'єктів зберігання даних*] для виявлення та захисту від несанкціонованого інтелектуального аналізу даних.

Рекомендації з реалізації: Інтелектуальний аналіз даних – це аналітичний процес, який намагається знайти кореляції або шаблони у великих наборах даних з метою виявлення даних або знань. До об'єктів зберігання даних належать, наприклад, бази даних, записи бази даних і поля бази даних. Конфіденційну інформацію можна отримати за допомогою операцій інтелектуального аналізу даних. Аналіз персональних даних може призвести до неочікуваних відкриттів щодо окремих осіб і створити ризики для конфіденційності. Перед виконанням аналізу даних організації визначають, чи є така діяльність дозволеною. На організації можуть поширюватися відповідні закони, виконавчі накази, директиви, нормативні акти чи політики, які стосуються вимог до аналізу даних. Персонал організації консультується зі старшим представником агентства щодо конфіденційності та юридичним консультантом щодо таких вимог. Методи запобігання та виявлення передачі даних можуть містити: обмеження типів відповідей, що надаються на запити до бази даних; обмеження кількості та частоти запитів до бази даних; повідомлення персоналу про нетипові запити до бази даних або звернення до них. Цей захід безпеки забезпечує захист організаційної інформації від витоку зі сховищ даних. Захід безпеки AU-13 стосується моніторингу інформації, яка, можливо, була отримана (санкціоновано або несанкціоновано) у сховищах даних і тепер є доступною (наприклад на зовнішніх сайтах). [ЕО 13587] вимагає створення програми внутрішніх загроз для стримування, виявлення та пом'якшення внутрішніх загроз, включаючи захист конфіденційної інформації від використання, компрометація або несанкціонованого розголошення. Захист від інтелектуального аналізу даних вимагає впровадження відповідних методів його запобігання та виявлення.

Пов'язані заходи: PM-12, PT-2.

Посилення заходів: Немає.

Посилання: [ЕО 13587].

## AC-24 РІШЕННЯ ЩОДО УПРАВЛІННЯ ДОСТУПОМ

Заходи захисту:

[*Вибір: Встановити процедури; Запровадити механізми*], щоб забезпечити застосування [*Призначення: визначені організацією рішення щодо контролю доступу*] до кожного запиту щодо доступу до виконання доступу.

Рекомендації з реалізації: Рішення щодо управління доступом (також відомі як рішення про авторизацію) мають бути забезпечені у випадках, коли для отримання конкретного доступу вимагається певна авторизаційна інформація. Зауважимо, що забезпечення доступу відбувається у випадках, коли в системі впроваджені заходи безпеки щодо управління доступом. Попри те, що рішення щодо управління доступом і заходи щодо управління доступом часто покладені на один суб'єкт, — це не завжди оптимальне розподілення обов'язків. Наприклад, для деяких архітектур і розподілених систем такі функції можуть бути покладені на різні сутності.

Пов'язані заходи: AC-2, AC-3.

Посилення заходів:

(1) РІШЕННЯ ЩОДО УПРАВЛІННЯ ДОСТУПОМ - ІНФОРМАЦІЯ ПРО ПЕРЕДАЧУ АВТОРИЗОВАНОГО ДОСТУПУ

Передавати [*Призначення: визначену організацією інформацію щодо авторизації доступу*] за допомогою [*Призначення: визначених організацією заходів безпеки*] до [*Призначення: визначених організацією систем*], які

забезпечують ухвалення рішень щодо управління доступом.

Рекомендації з реалізації: У розподілених системах процеси авторизації та рішення щодо управління доступом можуть відбуватися в окремих частинах систем. У таких випадках інформація про авторизацію має передаватися надійно, тому рішення щодо управління доступом мають бути впроваджені у відповідних місцях. Для виконання рішень щодо управління доступом може знадобитися передача атрибутів безпеки у складі авторизаційної інформації. Це пояснюється тим, що в розподілених системах можуть бути впроваджені різні рішення щодо управління доступом, так само як можуть бути наявні різні суб'єкти, що ухвалюють такі рішення послідовно (при цьому кожен з таких суб'єктів вимагає наявність атрибутів безпеки для ухвалення рішення). Посилення заходу щодо захисту авторизаційної інформації гарантує, що така інформація не може бути підроблена або порушена в процесі передачі.

Пов'язані заходи: AU-10.

(2) РІШЕННЯ ЩОДО УПРАВЛІННЯ ДОСТУПОМ - ВІДСУТНІСТЬ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧА АБО ПРОЦЕСУ, ЩО ДІЄ ВІД ІМЕНІ КОРИСТУВАЧА

Здійснювати ухвалення рішень щодо управління доступом, засновуючись на [*Призначення: визначених організацією атрибутах безпеки*], які не охоплюють ідентифікацію користувача або процесу, що діє від імені користувача.

Рекомендації з реалізації: У певних ситуаціях необхідно, щоб рішення щодо управління доступом ухвалювалися без інформації щодо особи, яка надає запит. Здебільшого таке виникає у випадках, коли вимагається збереження конфіденційності користувача. В інших ситуаціях ідентифікаційна інформація користувача просто непотрібна для ухвалення рішень щодо управління доступом і, особливо у випадку розподілених систем, передача такої інформації з необхідним ступенем надійності може бути дуже дорогою або такою, що складно реалізовується.

Пов'язані заходи: Немає.

Посилання: [SP 800-162], [SP 800-178].

## AC-25 ДИСПЕТЧЕР ДОСТУПУ

Заходи захисту:

Впровадити диспетчер доступу для [*Призначення: визначеної організацією політики контролю доступу*], який захищений від несанкціонованого доступу, завжди був доступний для виклику та досить компактний, щоб бути підданим аналізу й тестуванню, надійність якого може бути гарантована.

Рекомендації з реалізації: Інформація, що міститься в системі, являє собою структури даних. Внутрішні структури даних можуть бути представлені двома видами сутностей: активні та пасивні. Активні сутності зазвичай називають суб'єктами — вони асоціюються з особами, пристроями або процесами, що діють від їх імені. Пасивними сутностями виступають об'єкти, які асоціюються зі структурами даних, такими як записи, буфери, таблиці, файли, порти зв'язку. Диспетчери доступу застосовують обов'язкові політики управління доступом — тип контролю доступу, який обмежує доступ до об'єктів суб'єктів на основі ідентичності груп, до яких вони належать.

Управління доступом є обов’язковим, оскільки суб’єктам з певними привілеями (тобто дозволами доступу) заборонено передавати ці привілеї будь-яким іншим суб’єктам (прямо чи опосередковано), тобто система має забезпечувати чітке виконання політики управління доступом. Диспетчер доступу перешкоджає порушенню роботи механізму.

Пов’язані заходи: AC-3, AC-16, SA-8, SA-17, SC-3, SC-11, SC-39, SI-13.

Посилення заходів: Немає.

Посилання: Немає.

## 10.2 Клас заходів захисту АТ — ОБІЗНАНІСТЬ ТА НАВЧАННЯ

### АТ-1 ПОЛІТИКА ТА ПРОЦЕДУРИ ПІДВИЩЕННЯ ОБІЗНАНОСТІ ТА НАВЧАННЯ

Заходи захисту:

a. Розробити, задокументувати та поширити [*Призначення: серед визначеного організацією персоналу або ролей*]:

   1. [*Вибір (один або декілька): Рівень організації; Рівень місії/бізнес-процесу; рівень системи*] політики обізнаності та навчання у сфері забезпечення безпеки та приватності, яка:

      (a) містить мету, сферу застосування, ролі, обов'язки, відповідальність керівництва, координацію між організаційними підрозділами та систему контролю відповідності (complaince);

      (b) відповідає чинним законам, нормативним документам, директивам, нормам, політикам, стандартам та керівним документам.

   2. Процедури, що сприяють реалізації політики підвищення обізнаності та професійної підготовки в галузі безпеки, приватності, а також пов'язаних з ними заходів захисту інформації та персональних даних.

b. Призначити [*Призначення: визначену організацією посадову особу*] для управління політикою та процедурами підвищення обізнаності та навчання у сфері забезпечення безпеки та приватності.

c. Переглядати та оновлювати:

   1. Поточну політика [*Призначення: частота, визначена організацією*] і наступне [*Призначення: події, визначені організацією*];

   2. Процедури [*Призначення: частота, визначена організацією*] та наступні [*Призначення: події, визначені організацією*].

Рекомендації з реалізації: Цей захід захисту стосується встановлення політики та процедур для ефективного здійснення заходів та їх посилень у класі АТ. Стратегія управління ризиками є важливим фактором у встановленні політики та процедур обізнаності та навчання. За наявності політики, а також планів захисту інформації та персональних даних на рівні організації, конкретні системні політики та процедури можуть бути непотрібні. Політика може бути внесена до складу загальної політики безпеки та приватності або може бути представлена кількома політиками (у випадках складної архітектури). Процедури описують, як має реалізуватися політика чи заходи захисту та як вони можуть бути спрямовані на персонал або роль, яка є об'єктом процедури. Процедури можуть бути задокументовані в планах захисту інформації та персональних даних (як один чи декілька документів). Події, які можуть спричинити оновлення політики й процедур підвищення обізнаності та навчання, включають висновки оцінки чи аудиту, інциденти чи порушення безпеки або зміни у чинних законах, розпорядженнях, директивах, постановах, політиках, стандартах і вказівках. Повторне встановлення засобів контролю не є організаційною політикою чи процедурою.

Пов'язані заходи: PM-9, PS-8, SI-12.

Посилення заходів: Немає.

Посилання: [OMB A-130], [SP 800-12], [SP 800-30], [SP 800-39], [SP 800-50], [SP 800-100].

## AT-2 НАВЧАННЯ З ПІДВИЩЕННЯ ОБІЗНАНОСТІ

Заходи захисту:

Впровадити базові тренінги з підвищення обізнаності у сфері безпеки та приватності для користувачів системи (включно з менеджерами, керівниками компаній і підрядниками):

a. Забезпечити навчання грамотності з питань безпеки та конфіденційності для користувачів системи (включаючи менеджерів, керівників вищої ланки та підрядників):

    1. як частину початкового навчання для нових користувачів і [*Призначення: частота, визначена організацією*] після цього;

    2. якщо цього потребують системні зміни або наступні [*Призначення: події, визначені організацією*].

b. Використовувати наведені нижче методи, щоб підвищити рівень безпеки та конфіденційності користувачів системи [*Завдання: визначені організацією методи поінформованості*];

c. Оновлювати навчання грамотності та зміст обізнаності [*Завдання: частота, визначена організацією*] і наступні [*Завдання: події, визначені організацією*];

d. Включити уроки, отримані з внутрішніх або зовнішніх інцидентів безпеки або порушень, у навчання грамотності та методи підвищення обізнаності.

Рекомендації з реалізації: Зміст тренінгів з питань безпеки та приватності, а також методів обізнаності щодо безпеки та приватності має визначатися на основі конкретних вимог і систем організації, до яких персонал отримав дозвіл на доступ. Зміст має розкривати необхідність інформаційної безпеки та приватності, а також розкривати дії користувачів щодо збереження безпеки та приватності, реагування на інциденти безпеки та приватності. У тренінгах також має надаватися інформація щодо необхідності дотримання безпеки операцій. Повідомлення для підвищення обізнаності щодо безпеки та приватності можуть містити: демонстрацію плакатів, поширення матеріалів про безпеку та приватність, розсилки рекомендацій/повідомлень електронною поштою, показ повідомлень на екрані входу в систему та проведення інформаційних заходів щодо захисту інформації та приватності. Періодичність навчання з підвищення обізнаності після початкової підготовки (тобто описаного AT-2a.1) визначається чинними законами, директивами, положеннями та політиками (пропонується принцип збільшення періоду між тренінгами). Таке навчання може проводитися сесійно й охоплювати актуальну інформацію про зміни в політиці безпеки та приватності організації, переглянуті очікування щодо безпеки та приватності та/або теми з початкового навчання.

Пов'язані заходи: AC-3, AC-17, AC-22, AT-3, AT-4, CP-3, IA-4, IR-2, IR-7, IR-9, PL-4, PM-13, PM-21, PS-7, PT-2, SA-8, SA-16.

Посилення заходів:

(1) НАВЧАННЯ З ПІДВИЩЕННЯ ОБІЗНАНОСТІ - ПРАКТИЧНІ ЗАНЯТТЯ

Ввести до програми навчання практичні заняття (вправи) з тренування обізнаності, які імітують інциденти в області безпеки та приватності.

Рекомендації з реалізації: Практичні вправи можуть містити використання засобів соціальної інженерії та бути направлені на: збір інформації; отримання несанкціонованого доступу; імітування несприятливого впливу відкриття зловмисних вкладень електронної пошти або перехід за шкідливим вебпосиланнями. Практичні вправи, пов'язані з приватністю, можуть містити, наприклад, практичні модулі з тестами щодо обробки персональної інформації.

Пов'язані заходи: CA-2, CA-7, CP-4, IR-3.

(2) НАВЧАННЯ З ПІДВИЩЕННЯ ОБІЗНАНОСТІ - ВНУТРІШНІ ЗАГРОЗИ

Ввести до програми навчання вправи з розпізнавання та виявлення потенційних індикаторів внутрішніх загроз.

Рекомендації з реалізації: Потенційними індикаторами наявності внутрішніх загроз можуть бути такі ознаки: довготривале незадоволення роботою; спроби отримати доступ до інформації, яка не є потрібною для виконання службових обов'язків; нез'ясований доступ до фінансових ресурсів; знущання чи сексуальне домагання колег; насильство на робочому місці та інші серйозні порушення організаційної політики, процедур, директив і правил. Навчання з питань безпеки та приватності має містити рекомендації, як повідомляти про занепокоєння працівників і керівництва щодо потенційних індикаторів внутрішніх загроз через організаційні канали відповідно до встановленої політики та процедур.

Пов'язані заходи: PM-12.

(3) НАВЧАННЯ З ПІДВИЩЕННЯ ОБІЗНАНОСТІ - СОЦІАЛЬНА ІНЖЕНЕРІЯ ТА СОЦІАЛЬНИЙ ІНТЕЛЕКТУАЛЬНИЙ АНАЛІЗ ДАНИХ

Ввести до програми навчання вправи з підвищення обізнаності щодо розпізнавання та повідомлення про потенційні та фактичні атаки, з використанням методів соціальної інженерії та інтелектуального аналізу соціальних даних.

Рекомендації з реалізації: Соціальна інженерія — це методи спонукання (обману) когось на розкриття інформації або вживання дій, які можуть бути використані для нападу чи компрометації систем. Прикладами соціальної інженерії може виступати фішинг, претекстинг і хейдгайтинг. Соціальний інтелектуальний аналіз даних — це спроба в соціальному середовищі зібрати інформацію про організацію, яка може бути використана для майбутніх атак. Навчання з питань безпеки та приватності має містити відомості про те, як повідомляти про занепокоєння працівників і керівництва щодо потенційних і реальних випадків соціального інжинірингу та інтелектуального аналізу даних через організаційні канали на основі встановленої політики та процедур.

Пов'язані заходи: Немає.

(4) НАВЧАННЯ З ПІДВИЩЕННЯ ОБІЗНАНОСТІ - ПІДОЗРІЛІ ПОВІДОМЛЕННЯ ТА АНОМАЛЬНА ПОВЕДІНКА СИСТЕМИ

Провести навчання грамотності щодо розпізнавання підозрілих комунікацій і аномальної поведінки в системах організації за допомогою [*Завдання: визначені організацією індикатори шкідливого коду*]

Рекомендації з реалізації: Добре навчений персонал забезпечує ще один контроль організації, який можна використовувати як частину стратегії поглибленого захисту від зловмисного коду, який потрапляє в організації через електронну пошту або вебдодатки. Персонал, який навчений розпізнавати ознаки потенційно підозрілої електронної пошти (наприклад, отримання несподіваного електронного листа, отримання електронного листа з дивною чи поганою граматикою або отримання електронного листа від незнайомого відправника, адреса якого схожа на відому компанію чи підрядника) та правильно реагувати на підозрілу електронну пошту чи вебповідомлення. Щоб цей процес працював ефективно, персонал проходить навчання та інформує про такі підозрілі повідомлення. Навчання персоналу тому, як розпізнавати аномальну поведінку в системах, може забезпечити організації завчасне попередження про наявність шкідливого коду. Визнання аномальної поведінки персоналом організації може доповнити інструменти та системи виявлення шкідливого коду та захисту, які використовують в організації.

Пов’язані заходи: Немає.

(5) НАВЧАННЯ З ПІДВИЩЕННЯ ОБІЗНАНОСТІ - ВДОСКОНАЛЕНА СТІЙКА ЗАГРОЗА

Забезпечити навчання грамотності щодо стійкої постійної загрози.

Рекомендації з реалізації: Ефективним способом виявлення вдосконалених стійких загроз (APT) і запобігання успішним атакам є проведення спеціального навчання для окремих осіб. Навчання включає різні способи, якими APT можуть проникнути в організацію (наприклад, через вебсайти, електронні листи, спливаючі рекламні вікна, статті та соціальну інженерію) та прийоми розпізнавання підозрілих електронних листів, використання знімних систем у незахищених налаштуваннях і потенційне націлювання на людей удома.

Пов’язані заходи: Немає.

(6) НАВЧАННЯ З ПІДВИЩЕННЯ ОБІЗНАНОСТІ - СЕРЕДОВИЩЕ КІБЕРЗАГРОЗ

a. Забезпечити навчання грамотності щодо середовища кіберзагроз; і

b. Відображати поточну інформацію про кіберзагрози в операціях системи.

Рекомендації з реалізації: Оскільки загрози продовжують змінюватися з часом, навчання грамотності в організації є динамічним. Крім того, навчання щодо загроз не проводиться ізольовано від операцій системи, які підтримують місію організації та бізнес-функції.

Пов’язані заходи: RA-3.

Посилання: [OMB A-130], [SP 800-50], [SP 800-160-2], [SP 800-181], [ODNI CTF].

## AT-3 РОЛЬОВЕ НАВЧАННЯ

Заходи захисту:

a. Забезпечити проведення навчання з питань безпеки та приватності на основі ролей для працівників з ролями та обов'язками: [*Призначення: визначені організацією ролі та обов'язки*]:

   1. перед авторизацією доступу до системи, інформації або виконанням призначених обов'язків і [*Призначення: частота, визначена організацією*] після цього;

   2. коли цього потребують системні зміни.

b. Оновити навчальний контент на основі ролей [*Призначення: частота, визначена організацією*] і наступні [*Призначення: події, визначені організацією*];

c. Включіть у рольове навчання, інформацію, отриману з внутрішніх або зовнішніх інцидентів та порушень безпеки.

Рекомендації з реалізації: Відповідний зміст тренінгів з безпеки та приватності на основі ролей має бути визначений на основі обов'язків осіб і конкретних вимог щодо безпеки та приватності організації та інформаційних систем, до яких персонал має доступ, включно з технічною підготовкою, пов'язаною з безпекою, спеціально розробленою для виконання покладених на них обов'язків. Ролі, які можуть вимагати навчання з безпеки та приватності: власники системи; уповноважені посадові особи; працівники служби безпеки (захисту інформації); посадові особи, відповідальні за проєктування архітектори підприємств; посадові особи з питань закупівель; системні інженери; розробники систем і програмного забезпечення; системні адміністратори; адміністратори мереж; адміністратори баз даних; персонал, що здійснює діяльність з управління конфігурацією; аудитори; персонал, що має доступ до програмного забезпечення на рівні системи; персонал, який має обов'язки з планування дій у надзвичайних ситуаціях та реагування на надзвичайні ситуації; персонал, що відповідає за управління приватністю; персонал, що має доступ до персональних даних. Комплексне рольове навчання стосується менеджерських, експлуатаційних і технічних ролей, що охоплюють фізичні, кадрові й технічні гарантії та контрзаходи. Таке навчання може містити огляд політики, процедур, інструментів і методів для визначених ролей. Організації проводять навчання, необхідне для виконання посадовими особами своїх обов'язків, пов'язаних з операціями та безпекою ланцюгів постачання, у контексті програм інформаційної безпеки та приватності. Рольове навчання з питань безпеки та приватності повинні також проходити підрядники. Типи навчання включають веб- та комп'ютерне навчання, навчання в аудиторії та практичне навчання (включаючи мікронавчання). Регулярне оновлення навчального матеріалу на основі ролей допомагає гарантувати, що його зміст залишається доречним і ефективним. Події, які можуть спричинити оновлення змісту навчання на основі ролей, включають, але не обмежуються ними, висновки оцінки або аудиту, інциденти безпеки або порушення, або зміни в застосовних законах, розпорядженнях, директивах, постановах, політиках, стандартах і інструкціях.

Пов'язані заходи: AC-3, AC-17, AC-22, AT-2, AT-4, CP-3, IR-2, IR-7, IR-9, PL-4,

PM-13, PM-23, PS-7, PS-9, SA-3, SA-8, SA-11, SA-16, SR-6, SR-11.

Посилення заходів:

(1) РОЛЬОВЕ НАВЧАННЯ - ЗАХОДИ ЗАХИСТУ РОБОЧОГО СЕРЕДОВИЩА

Надати [*Призначення: визначеним організацією персоналу чи посадам*] з початку роботи та з [*призначенням: визначеною організацією частотою*] підготовку з питань застосування заходів захисту робочого середовища.

Рекомендації з реалізації: Заходи захисту робочого середовища охоплюють пристрої/системи пожежогасіння та системи виявлення пожеж, спринклерні системи, ручні вогнегасники, нерухомі пожежні шланги, детектори диму, контролери температури/вологості, опалення, вентиляції та кондиціонування повітря всередині об'єкта. Організації визначають персонал з конкретними ролями й обов'язками, пов'язаними із заходами безпеки робочого середовища, який має проходити спеціалізовану підготовку.

Пов'язані заходи: PE-1, PE-11, PE-13, PE-14, PE-15.

(2) РОЛЬОВЕ НАВЧАННЯ - ФІЗИЧНІ ЗАХОДИ БЕЗПЕКИ

Надати [*Призначення: визначеним організацією персоналу чи ролям*] з початку роботи та з [*Призначення: визначеною організацією частотою*] підготовку з питань застосування та експлуатації заходів фізичної безпеки.

Рекомендації з реалізації: Фізичні заходи безпеки охоплюють пристрої контролю фізичного доступу, фізичну сигналізацію, обладнання для контролю/спостереження та охорону безпеки (процедури розгортання й експлуатації). Організації визначають персонал з конкретними ролями та обов'язками, пов'язаними з фізичними заходами безпеки, який має проходити спеціалізовану підготовку.

Пов'язані заходи: PE-2, PE-3, PE-4.

(3) РОЛЬОВЕ НАВЧАННЯ - ПРАКТИЧНІ ЗАНЯТТЯ

Ввести до програми навчання практичні заняття з безпеки та приватності, які мають підкріпити досягнення цілей навчання.

Рекомендації з реалізації: Практичні заняття з безпеки можуть охоплювати тренінги з безпеки для розробників програмного забезпечення. Такі тренінги мають містити вправи з протидії імітованим кібератакам, що використовують загальні вразливості програмного забезпечення, або фішинг-атакам, націленим на старших керівників. Практичні заняття щодо приватності можуть містити модулі з тестами щодо обробки персональних даних у різних сценаріях та методи оцінювання шкідливого впливу на приватність.

Пов'язані заходи: Немає.

(4) РОЛЬОВЕ НАВЧАННЯ - ПІДОЗРІЛІ ЗВ'ЯЗКИ ТА АНОМАЛЬНА ПОВЕДІНКА СИСТЕМИ

[Вилучено: включено до AT-2(4)].

(5) РОЛЬОВЕ НАВЧАННЯ - ОБРОБКА ПЕРСОНАЛЬНИХ ДАНИХ

Забезпечити [*Призначення: персонал або посади, визначені організацією*] початкове та [*Призначення: частота, визначену організацією*] навчання з використання та управління обробкою персональних даних та контролю прозорості.

Рекомендації з реалізації: Обробка персональної інформації та контроль прозорості включають повноваження організації обробляти персональну інформацію та цілі її обробки. Рольове навчання для федеральних агентств розглядає типи інформації, яка може становити персональні дані, а також ризики, міркування та зобов'язання, пов'язані з її обробкою. Таке навчання також передбачає повноваження обробляти персональні дані, задокументовану в політиках конфіденційності та повідомленнях, повідомленнях про систему записів, угодах і повідомленнях про комп'ютерне зіставлення, оцінці впливу на конфіденційність, заявах приватності, контрактах, угодах про обмін інформацією, меморандумах про взаєморозуміння та/ або іншу документацію.

Пов'язані заходи: PT-2, PT-3, PT-5, PT-6.

Посилання: [OMB A-130], [SP 800-50], [SP 800-181].

## AT-4 НАВЧАЛЬНІ ЗАПИСИ

Заходи захисту:

a. Документувати та відстежувати індивідуальні навчальні заходи із забезпечення безпеки та приватності, включно з базовою підготовкою з питань безпеки та приватності, а також спеціальною підготовкою з питань безпеки та приватності визначених посадових осіб.
b. Зберігати індивідуальні записи про навчання впродовж [*Призначення: визначеного організацією періоду часу]*.

Рекомендації з реалізації: Документацію щодо спеціалізованого навчання можуть вести окремі керівники за бажанням організації.

Пов'язані заходи: AT-2, AT-3, CP-3, IR-2, PM-14, SI-12.

Посилення заходів: Немає.

Посилання: [OMB A-130].

## AT-5 КОНТАКТИ З ГРУПАМИ БЕЗПЕКИ ТА АСОЦІАЦІЯМИ

[Вилучено: Включено до PM-15]

## AT-6 ВІДГУКИ ПРО ПРОВЕДЕНІ НАВЧАННЯ

Заходи захисту: Надати відгук про результати організаційного навчання наступному персоналу [*Призначення: з визначеною організацією частотою та визначеному організацією персоналу*]

Рекомендації з реалізації: Зворотний зв'язок із навчанням включає результати тренінгу

з підвищення обізнаності та результати тренінгу на основі ролей. Результати навчання, особливо невдачі персоналу на критичних посадах, можуть свідчити про потенційно серйозну проблему. Тому важливо, щоб керівники вищої ланки були поінформовані про такі ситуації, та могли вжити відповідних заходів. Зворотний зв'язок із навчанням підтримує оцінку та оновлення організаційного навчання, описаного в AT-2b та AT-3b

Пов'язані заходи: Немає.

Посилення заходів: Немає.

Посилання: Немає.

### 10.3 Клас заходів захисту AU — АУДИТ ТА ПІДЗВІТНІСТЬ

## AU-1 ПОЛІТИКА ТА ПРОЦЕДУРИ АУДИТУ ТА ПІДЗВІТНОСТІ

Заходи захисту:

a. Розробити, задокументувати та поширити [*Призначення: серед персоналу або ролей, що їх визначила організація*]:

1. [*Вибір (один або декілька): Рівень організації; Рівень місії/бізнес-процесу; рівень системи*] політика аудиту та підзвітності, яка:

(a) містить мету, сферу застосування, ролі, обов'язки, відповідальність керівництва, координацію між організаційними підрозділами та систему контролю відповідності (complaince);

(b) відповідає чинним законам, нормативним документам, директивам, нормам, політикам, стандартам та керівним документам.

2. Процедури, що сприяють здійсненню політики аудиту та підзвітності, а також пов'язані з ними заходи аудиту та підзвітності.

b. Призначити [*Призначення: визначену організацією старшу посадову особу*] для управління політикою та процедурами аудиту та підзвітності.

c. Переглядати та оновлювати поточний аудит та підзвітність:

1. політику [*Призначення: частота, визначена організацією*] та наступне [*Призначення: події, визначені організацією*];

2. процедури аудиту [*Призначення: визначеною організацією частотою*] та [*Завдання: події, визначені організацією*].

Рекомендації з реалізації: Цей захід захисту стосується встановлення політики та процедур для ефективного здійснення заходів та їх посилень у класі AU. Стратегія управління ризиками є важливим фактором у встановленні політики та процедур. Комплексна політика та процедури допомагають забезпечити безпеку та приватність. За наявності політики, а також планів захисту інформації та персональних даних на рівні організації, конкретні системні політики та процедури можуть бути не потрібні. Політика може бути внесена до складу загальної політики безпеки та приватності або може бути представлена кількома політиками (у випадках складної архітектури). Процедури описують, як має реалізуватися політика чи заходи захисту та як вони можуть бути спрямовані на персонал або роль, що є об'єктом процедури. Процедури можуть бути задокументовані в планах захисту інформації та персональних даних (як один або декілька документів). Події, які можуть спричинити оновлення політики та процедур аудиту та підзвітності, включають висновки оцінки або аудиту, інциденти чи порушення безпеки або зміни у чинних законах, розпорядженнях, директивах, положеннях, політиках, стандартах і вказівках. Просте повторне встановлення засобів контролю не є організаційною політикою чи процедурою.

Пов'язані заходи: PM-9, PS-8, SI-12.

Посилення заходів: Немає.

Посилання: [SP 800-12], [SP 800-30], [SP 800-39], [SP 800-100].

## AU-2 ПОДІЇ АУДИТУ

Заходи захисту:

a. Визначити типи подій, які система може реєструвати для підтримки функції аудиту: [*Призначення: типи подій, визначені організацією, які система здатна реєструвати*];

b. Координувати функції аудиту безпеки з іншими організаційними підрозділами, які вимагають інформації, пов'язаної з аудитом, для посилення взаємної підтримки та допомоги у виборі типів подій, що перевіряються;

c. Визначити, які типи подій підлягають аудиту: [*Призначення: визначені організацією події, що підлягають аудиту (підмножина подій, що підлягають аудиту, визначених в AU-2 а.), а також частота (або ситуація, що вимагає) проведення аудиту для кожної ідентифікованої події*]

d. Обґрунтувати, чому типи подій, що перевіряються, вважаються достатніми для підтримки розслідувань інцидентів (постфактум), пов'язаних з безпекою та приватністю;

e. Перегляньте й оновіть типи подій, вибрані для журналювання [*Призначення: частота, визначена організацією*].

Рекомендації з реалізації: Подія — це будь-яке явище, що відбувається в системі. Організації ідентифікують типи подій аудиту як такі події, що мають значення та стосуються безпеки систем і середовища, у яких ці системи функціонують. Типи подій аудиту можуть містити: зміни паролів; невдалі входи в систему або невдалий доступ; зміна атрибутів безпеки, використання адміністративних привілеїв. Після визначення типів подій аудиту для кожного з них призначаються заходи безпеки, які мають бути реалізовані. Визначаючи набір типів подій, які будуть реєструватися, організації вважають, що моніторинг і аудит є відповідними для кожного засобу контролю, який необхідно запровадити. Для повноти реєстрація подій включає всі протоколи, які працюють і підтримуються системою.

Для того щоб збалансувати вимоги до аудиту з іншими потребами системи, цей захід безпеки також вимагає виявити ту підмножину типів подій аудиту, які мають перевірятися в певний момент часу. Наприклад, може бути визначено, що в системі повинна бути можливість запису кожного доступу до файлів — як успішного, так і невдалого, але разом з тим, має бути можливість активації/деактивації такої функції за конкретних обставин. Типи подій, які організації бажають реєструвати, можуть змінюватися. Перегляд і оновлення набору зареєстрованих подій є необхідним, щоб переконатися, що події залишаються актуальними та продовжують підтримувати потреби організації. Організації розглядають, які типи подій журналювання можуть виявити персональні дані, що може спричинити загрозу конфіденційності, а також як пом'якшити такі ризики. Наприклад, існує ймовірність виявлення персональних даних в контрольному сліді, особливо якщо подія журналювання базується на шаблонах або часу використання.

Вимоги до аудиту, включно з необхідністю обробки подій аудиту, можуть посилатися на інші засоби безпеки та конфіденційності й посилення, наприклад AC-2 (4), AC-3 (10), AC-6 (9), AC-17 (1), CM-3f, CM-5 (1), IA-3 (3.b), MA-4 (1), MP-4 (2), PE-3, PM-21, RA-8, SC-7 (9), SC-7 (15), SI-3 (8), SI-4 (22), SI-7 (8) та SI-10 (1). Також можуть бути визначені типи заходів, що підлягають аудиту (регулюється чинним законодавством, наказами, директивами та політиками). Записи аудиту можуть створюватися на різних рівнях, у тому числі на рівні пакетів (у випадках, коли інформація проходить через мережу). Вибір відповідного рівня аудиту є важливим аспектом і може сприяти виявленню першопричин інцидентів (зокрема

потенційних). Визначаючи типи подій, організації розглядають журналювання, необхідне для охоплення пов'язаних типів подій, таких як кроки в розподілених процесах на основі транзакцій і дії, які відбуваються в сервіс-орієнтованих архітектурах.

Пов'язані заходи: AC-2, AC-3, AC-6, AC-7, AC-8, AC-16, AC-17, AU-3, AU-4, AU-5, AU-6, AU-7, AU-11, AU-12, CM-3, CM-5, CM-6, CM-13, IA-3, MA-4, MP-4, PE-3, PM-21, PT-2, PT-7, RA-8, SA-8, SC-7, SC-8, SC-18, SI-3, SI-4, SI-7, SI-10, SI-11.

Посилення заходів:

(1) ПОДІЇ АУДИТУ - УЗАГАЛЬНЕННЯ ЗАПИСІВ ПРО АУДИТ З ДЕКІЛЬКОХ ДЖЕРЕЛ

[Вилучено: Включено до AU-12]

(2) ПОДІЇ АУДИТУ - ВИБІР ПОДІЇ АУДИТУ ЗА КОМПОНЕНТАМИ

[Вилучено: Включено до AU-12]

(3) ПОДІЇ АУДИТУ - ПЕРЕГЛЯД ТА ОНОВЛЕННЯ

[Вилучено: Включено до AU-2]

(4) ПОДІЇ АУДИТУ - ПРИВІЛЕЙОВАНІ ФУНКЦІЇ

[Вилучено: Включено до AC-6(9)]

Посилання: [OMB A-130], [SP 800-92].

## AU-3 ЗМІСТ ЗАПИСІВ АУДИТУ

Заходи захисту:

Переконатися, що записи аудиту містять інформацію, яка встановлює наступне:

a. який тип події стався;

b. коли відбулася подія;

c. де відбулася подія;

d. джерело події;

e. наслідки події;

f. результат події та ідентифікатор будь-яких осіб або суб'єктів, пов'язаних з подією.

Рекомендації з реалізації: Зміст записів аудиту, який може бути необхідний для задоволення вимог цього заходу, може містити: часові позначки, джерела подій, ідентифікатори користувача або процесу, описи подій, маркери успіху/відмови, пов'язані імена файлів і управління доступом або правила управління потоком, що викликаються. Результати подій можуть місити маркери успішності чи відмови події та конкретні результати, наприклад стан безпеки та приватності системи після події. Організації розглядають, як записи аудиту можуть виявити інформацію про осіб, яка може спричинити загрозу конфіденційності, і як найкраще пом'якшити такі ризики. Наприклад, у журналі аудиту існує ймовірність виявлення інформації, що дозволяє

ідентифікувати особу, особливо якщо журнал записує вхідні дані або ґрунтується на моделях чи часу використання.

Пов'язані заходи: AU-2, AU-8, AU-12, AU-14, MA-4, PL-9, SA-8, SI-7, SI-11.

Посилення заходів:

(1) ЗМІСТ ЗАПИСІВ АУДИТУ - ДОДАТКОВА ІНФОРМАЦІЯ ПРО АУДИТ

Формувати записи аудиту, що містять наступну додаткову інформацію: [*Призначення: визначену організацією додаткову, більш детальну інформацію*].

Рекомендації з реалізації: Реалізація цього посилення заходу безпеки залежить від функціональності системи для налаштування змісту записів аудиту. Додаткова інформація, яка може враховуватися в записах аудиту, може містити: повнотекстовий запис привілейованих команд або індивідуальні ідентичності користувачів, які належать до групових облікових записів. Рішення щодо можливості обмеження додаткової інформації про аудит може бути ухвалено залежно від умов функціонування системи. Рішення про невключення до записів і журналів аудиту інформації, яка потенційно може ввести в оману чи ускладнити пошук важливої інформації, може полегшити їхнє використання.

Пов'язані заходи: Немає.

(2) ЗМІСТ ЗАПИСІВ АУДИТУ - ЦЕНТРАЛІЗОВАНЕ УПРАВЛІННЯ ПЛАНОВАНИМ ЗМІСТОМ ЗАПИСІВ АУДИТУ

[Вилучено: Включено до PL-9]

(3) ЗМІСТ ЗАПИСІВ АУДИТУ - ОБМЕЖЕННЯ ЕЛЕМЕНТІВ ПЕРСОНАЛЬНИХ ДАНИХ

Обмежити персональні дані, що міститься в записах аудиту, до таких елементів, які визначені в оцінці ризику приватності: [*Призначення: визначені організацією елементи*].

Рекомендації з реалізації: Обмеження персональних даних у записах аудиту (у випадках, коли така інформація не потрібна для оперативних цілей) сприяє зниженню рівня ризику порушення приватності.

Пов'язані заходи: RA-3.

Посилання: [OMB A-130], [IR 8062].

## AU-4 МІСТКІСТЬ СХОВИЩА ЗАПИСІВ АУДИТУ

Заходи захисту:
Розподіляти місткість сховища записів аудиту у відповідності до [*Призначення: визначених організацією вимог до зберігання записів аудиту*].

Рекомендації з реалізації: Розгляду підлягають види аудиту, які мають бути проведені, та вимоги щодо процедур аудиту з метою обґрунтування місткості сховища для зберігання записів аудиту. Надання достатнього розміру сховища для зберігання записів аудиту знижує ймовірність того, що таке сховище буде переповнене, що своєю чергою може призвести до потенційної втрати або зниження ефективності аудиту.

Пов’язані заходи: AU-2, AU-5, AU-6, AU-7, AU-9, AU-11, AU-12, AU-14, SI-4.

Посилення заходів:

(1) МІСТКІСТЬ СХОВИЩА ЗАПИСІВ АУДИТУ - ПЕРЕДАЧА ДО АЛЬТЕРНАТИВНОГО СХОВИЩА

Проводити передачу записів аудиту [*Призначення: з визначеною організацією частотою*] в іншу систему або носій інформації, відмінний від системи або системного компонента, який веде аудит.

Рекомендації з реалізації: Передача журналу аудиту, також відома як розвантаження, є звичайним процесом у системах з обмеженою ємністю для зберігання журналу аудиту та підтримання їх доступності. Початкове сховище журналу аудиту використовується лише тимчасово, поки система не зможе зв’язатися з вторинною або альтернативною системою, призначеною для зберігання журналу аудиту, після чого журнали аудиту передаються до альтернативного сховища (як в AU-9(2)). Однак метою вибору AU-9(2) є захист конфіденційності та цілісності записів аудиту. Організації можуть вибрати будь-яке покращення контролю, щоб отримати вигоду від збільшення ємності журналу аудиту та збереження конфіденційності, цілісності та доступності записів і журналів аудиту.

Пов’язані заходи: Немає.

Посилання: Немає.

## AU-5 РЕАГУВАННЯ НА ВІДМОВИ ОБРОБКИ ДАНИХ АУДИТУ

Заходи захисту:

a. Сповіщати [*Призначення: визначені організацією персонал або посади*] у разі збою обробки даних аудиту в [*Призначення: визначений організацією період часу*].

b. Виконати наступні додаткові дії: [*Призначення: визначені організацією дії, які необхідно зробити*].

Рекомендації з реалізації: Збої процесу журналювання аудиту включають помилки програмного та апаратного забезпечення, збої в механізмах запису журналу аудиту та досягнення або перевищення ємності зберігання журналу аудиту. Дії можуть охоплювати: вимкнення системи, перезапис найстаріших записів аудиту, припинення генерації записів аудиту. Прикладами збоїв обробки аудиту можуть бути: помилки програмного та апаратного забезпечення, збої в механізмах аудиту, перевищення місткості сховища записів аудиту. Залежно від типу відмови, місця відмови або інших факторів, можуть бути вибрані додаткові дії для виконання. Цей захід безпеки може застосовуватися як до конкретного сховища даних аудиту (тобто, окремої системної складової, де зберігаються записи аудиту), так і до загального сховища записів аудиту організації (тобто всіх сховищ даних аудиту).

Пов’язані заходи: AU-2, AU-4, AU-7, AU-9, AU-11, AU-12, AU-14, SI-4, SI-12.

Посилення заходів:

(1) РЕАГУВАННЯ НА ВІДМОВИ ОБРОБКИ ДАНИХ АУДИТУ - МІСТКІСТЬ СХОВИЩА ЗАПИСІВ АУДИТУ

Забезпечити попередження [*Призначення: визначених організацією персоналу, ролей та/або місць*] у межах [*Призначення: визначеного організацією періоду часу*], коли обсяг записів аудиту, що зберігаються, досягає максимуму місткості сховища.

Рекомендації з реалізації: Організації можуть мати кілька сховищ для зберігання даних аудиту, розподілених по декількох компонентах системи, причому кожне сховище може мати різну місткість.

Пов'язані заходи: Немає.

(2) РЕАГУВАННЯ НА ВІДМОВИ ОБРОБКИ ДАНИХ АУДИТУ - ТРИВОЖНЕ СПОВІЩЕННЯ В РЕАЛЬНОМУ ЧАСІ

Забезпечити сповіщення в [*Призначення: визначений організацією період реального часу*] [*Призначення: визначених організацією персоналу, ролей та/або місць*], коли відбуваються такі події збою аудиту: [*Призначення: визначені організацією події, пов'язані зі збоями та помилками аудиту, які вимагають тривоги в реальному часі*].

Рекомендації з реалізації: Попередження мають містити термінові повідомлення. Повідомлення в режимі реального часу мають надаватися зі швидкістю інформаційних технологій (тобто час від виявлення події до оповіщення не повинен перевищувати секунду).

Пов'язані заходи: Немає.

(3) РЕАГУВАННЯ НА ВІДМОВИ ОБРОБКИ ДАНИХ АУДИТУ - НАЛАШТУВАННЯ ПОРОГОВОГО ОБСЯГУ ТРАФІКУ

Здійснювати налаштування порогових значень обсягу трафіку комунікаційних мереж, що відображають обмеження на можливості аудиту та [*Вибір: відхиляти; затримувати*] мережевий трафік, якщо він перевищує цей поріг.

Рекомендації з реалізації: Обробка мережевого трафіку може затримуватися (або відхилятися), якщо об'єм трафіку перевищує можливості системи аудиту. Відповідь про відхилення або затримку надається на основі встановлених порогових обсягів трафіку, які можна налаштувати на основі змін у ємності зберігання журналу аудиту.

Пов'язані заходи: Немає.

(4) РЕАГУВАННЯ НА ВІДМОВИ ОБРОБКИ ДАНИХ АУДИТУ - ВИМКНЕННЯ В РАЗІ ВІДМОВИ

Застосовувати [*Вибір: повне вимикання системи; часткове вимикання системи; знижений режим роботи з обмеженням доступної/цільової функціональності*] у разі [*Призначення: визначених організацією збоїв аудиту*], якщо немає альтернативної можливості аудиту.

Рекомендації з реалізації: Мають бути визначені типи збоїв аудиту, які можуть спричиняти автоматичне відключення системи. Через важливість забезпечення місії та безперервності діяльності організації можуть визначити, що характер невдачі аудиту не є настільки серйозним, що вимагає повного вимкнення системи. У таких випадках альтернативними рішеннями можуть бути часткове

вимкнення системи або робота в деградованому режимі зі зниженою працездатністю.

Пов'язані заходи: AU-15.

(5) РЕАГУВАННЯ НА ВІДМОВИ ОБРОБКИ ДАНИХ АУДИТУ - МОЖЛИВІСТЬ АЛЬТЕРНАТИВНОГО ЖУРНАЛЮВАННЯ АУДИТУ

Надання альтернативної можливості журналювання аудиту в разі збою основної можливості журналювання аудиту, яка реалізується [*Призначення: визначена організацією функція альтернативного журналювання аудиту*]

Пов'язані заходи: AU-9.

Посилання: Немає.

## AU-6 ОГЛЯД, АНАЛІЗ І ЗВІТНІСТЬ АУДИТУ

Заходи захисту:

a. Переглядати та аналізувати записи системного аудиту [*Призначення: з визначеною організацією частотою*] для виявлення [*Призначення: визначеної організацією неналежної або незвичайної діяльності*].

b. Відправляти звіт про аудит [*Призначення: визначеним організацією персоналу або посадам*].

c. Налаштувати рівні огляду аудиту, аналізу та звітності в рамках системи, коли змінюється рівень ризику на основі інформації від правоохоронних органів, розвідувальної інформації або від інших достовірних джерел інформації.

Рекомендації з реалізації: Огляд, аналіз і звітність аудиту стосуються аудиту, пов'язаного з інформаційною безпекою, включно з аудитом, який є результатом моніторингу використання облікового запису, віддаленого доступу, бездротового зв'язку, підключення мобільних пристроїв, налаштувань конфігурації, інвентаризації компонентів системи, використання інструментів технічного обслуговування фізичного доступу тощо. Результати можуть бути передані таким організаційним структурам: група реагування на інциденти, довідкова служба, група/відділ захисту інформації. Якщо організаціям заборонено переглядати та аналізувати інформацію про аудит (або вони не мають можливості проводити таку діяльність), огляд/аналіз можуть проводити інші організації, яким надано такі повноваження. Частота, обсяг, глибина огляду, аналізу та звітності аудиту можуть бути скориговані відповідно до потреб організації на основі нової інформації, що надійшла.

Пов'язані заходи: AC-2, AC-3, AC-6, AC-7, AC-17, AU-7, AU-16, CA-2, CA-7, CM-2, CM-5, CM-6, CM-10, CM-11, IA-2, IA-3, IA-5, IA-8, IR-5, MA-4, MP-4, PE-3, PE-6, RA-5, SC-7, SI-3, SI-4, SI-7.

Посилення заходів:

(1) ОГЛЯД, АНАЛІЗ І ЗВІТНІСТЬ АУДИТУ - АВТОМАТИЗОВАНА ІНТЕГРАЦІЯ ПРОЦЕСІВ

Інтегрувати процеси перегляду, аналізу та звітності записів аудиту за допомогою [*Призначення: автоматизовані механізми, визначені організацією*].

Рекомендації з реалізації: До процесів організації, щодо яких слід застосовувати механізми інтеграції аудиту, належать: реагування на інциденти, безперервний моніторинг, планування дій у надзвичайних ситуаціях.

Пов'язані заходи: PM-7.

(2) ОГЛЯД, АНАЛІЗ І ЗВІТНІСТЬ АУДИТУ - АВТОМАТИЗОВАНІ СПОВІЩЕННЯ ПРО ПОРУШЕННЯ БЕЗПЕКИ

[Вилучено: Включено до SI-4]

(3) ОГЛЯД, АНАЛІЗ І ЗВІТНІСТЬ АУДИТУ - ЗІСТАВЛЯННЯ СХОВИЩ АУДИТУ

Аналізувати та зіставляти записи аудиту в різних сховищах задля забезпечення ситуативної обізнаності в масштабах організації.

Рекомендації з реалізації: Ситуативна обізнаність у масштабах організації містить обізнаність на всіх трьох рівнях управління ризиками (тобто на рівні організації, на рівні місії/процесів та системному рівні).

Пов'язані заходи: AU-12, IR-4.

(4) ОГЛЯД, АНАЛІЗ І ЗВІТНІСТЬ АУДИТУ - ЦЕНТРАЛІЗОВАНИЙ ПЕРЕГЛЯД ТА АНАЛІЗ

Забезпечити та впровадити можливість централізованого перегляду та аналізу записів аудиту з декількох компонентів у системі.

Рекомендації з реалізації: Автоматизовані механізми централізованого перегляду та аналізу охоплюють, наприклад, механізми управління інформаційною безпекою.

Пов'язані заходи: AU-2, AU-12.

(5) ОГЛЯД, АНАЛІЗ І ЗВІТНІСТЬ АУДИТУ - ІНТЕГРОВАНИЙ АНАЛІЗ ЗАПИСІВ АУДИТУ

Інтегрувати аналіз записів аудиту з аналізом [*Вибір (один або більше): інформації про сканування уразливостей; даних про продуктивність; інформації про моніторинг системи;* [*Призначення: визначених організацією даних/інформації, зібраних з інших джерел*]] для подальшого підвищення здатності виявляти неприйнятну або незвичайну діяльність.

Рекомендації з реалізації: Це посилення заходу не вимагає сканування вразливостей, збору даних про продуктивність або моніторингу системи. Це посилення вимагає інтеграції аналізу інформації, яка іншим чином обробляється в цих областях, з аналізом інформації аудиту. Використання інструментів системи управління подіями та інформацією про безпеку можуть полегшити агрегацію/консолідацію записів аудиту з декількох компонентів системи, а також співвідношення та аналіз записів аудиту. Використання стандартизованих сценаріїв аналізу записів аудиту, розроблених організаціями (при необхідності локалізованих коригувань сценаріїв), забезпечує більш економічні підходи до аналізу зібраної інформації. При визначенні правдивості сканування вразливостей і співвіднесення подій виявлення атак з результатами сканування, важливим є співвіднесення інформації записів аудиту з інформацією про

сканування вразливостей. Кореляція з даними про ефективність може виявити атаку типу «відмова в обслуговуванні» або інші типи атак, що призводить до несанкціонованого використання ресурсів. Кореляція з інформацією про моніторинг системи може допомогти в розкритті атак та поліпшити зв'язок інформації аудиту з операційними ситуаціями

Пов'язані заходи: AU-12, IR-4.

(6) ОГЛЯД, АНАЛІЗ І ЗВІТНІСТЬ АУДИТУ - КОРЕЛЯЦІЯ З ФІЗИЧНИМ МОНІТОРИНГОМ

Зіставляти інформацію із записів аудиту з інформацією, отриманою від моніторингу фізичного доступу, для подальшого підвищення здатності ідентифікувати підозрілу, неприйнятну, незвичайну або зловмисну діяльність.

Рекомендації з реалізації: Кореляція з фізичним моніторингом може допомогти організаціям визначити приклади підозрілої поведінки або підтвердити докази такої поведінки. Наприклад, кореляція ідентичності особи для логічного доступу до певних систем з додатковою інформацією про фізичну безпеку, яка була присутня, коли відбувся логічний доступ, може бути корисною для розслідування.

Пов'язані заходи: Немає.

(7) ОГЛЯД, АНАЛІЗ І ЗВІТНІСТЬ АУДИТУ - ДОЗВОЛЕНІ ДІЇ

Визначити дозволені дії для кожного [*Вибір (один або кілька): системного процесу; ролі; користувача*], пов'язаного з переглядом, аналізом та поданням інформації про аудит.

Рекомендації з реалізації: Організації визначають дозволені дії для процесів системи, ролей та/або користувачів, пов'язаних з оглядом, аналізом та звітністю аудиту, за допомогою методів управління обліковими записами. Дозволені дії мають визначатися, базуючись на принципі найменших привілеїв. До дозволених дій належать, наприклад, читання, запис, додавання, видалення.

Пов'язані заходи: Немає.

(8) ОГЛЯД, АНАЛІЗ І ЗВІТНІСТЬ АУДИТУ - АНАЛІЗ ПОВНОГО ТЕКСТУ ПРИВІЛЕЙОВАНИХ КОМАНД

Виконувати повний аналіз тексту привілейованих команд аудиту у фізично окремому компоненті чи підсистемі або іншій системі, яка може виконувати такий аналіз.

Рекомендації з реалізації: Це посилення заходу регламентує наявність чіткого середовища для спеціалізованого аналізу інформації аудиту, яка стосується привілейованих користувачів (без шкоди для такої інформації в системі), у якому користувачі мають підвищені привілеї, включно з можливістю виконання привілейованих команд. Повний аналіз тексту належить до аналізу, який розглядає повний текст привілейованих команд (тобто команд та всіх параметрів) на відміну від аналізу, який враховує лише ім'я команди. Повний аналіз тексту охоплює, наприклад, використання відповідності шаблонів та евристики.

Пов’язані заходи: AU-3, AU-9, AU-11, AU-12.

(9) ОГЛЯД, АНАЛІЗ І ЗВІТНІСТЬ АУДИТУ - КОРЕЛЯЦІЯ З ІНФОРМАЦІЄЮ З НЕТЕХНІЧНИХ ДЖЕРЕЛ

Зіставляти інформацію з нетехнічних джерел з інформацією аудиту з метою посилення організаційної обізнаності.

Рекомендації з реалізації: До нетехнічних джерел належать кадрові записи, що документують порушення організаційної політики, пов’язані з випадками переслідування та неналежного використання інформаційних активів. Така інформація може сприяти виявленню потенційної зловмисної інсайдерської діяльності. Доступ до інформації з нетехнічних джерел має бути обмеженим для мінімізації вірогідності ненавмисного оприлюднення приватної інформації. Таким чином, кореляція з інформацією з нетехнічних джерел здебільшого відбувається лише тоді, коли людей підозрюють у причетності до інциденту безпеки. Організації повинні отримати юридичну консультацію для ініціювання таких дій.

Пов’язані заходи: PM-12.

(10) ОГЛЯД, АНАЛІЗ І ЗВІТНІСТЬ АУДИТУ - РЕГУЛЮВАННЯ РІВНЯ АУДИТУ

[Вилучено: Включено до AU-6]

Посилання: [SP 800-86], [SP 800-101].

## AU-7 СКОРОЧЕННЯ ЗАПИСІВ АУДИТУ ТА ФОРМУВАННЯ ЗВІТУ

Заходи захисту:
Забезпечити та реалізувати можливості скорочення записів перевірок аудитом і звітів, до рівня, який:

a. підтримує перевірку, аналіз і звітність аудиту на вимогу та розслідування (постфактум) інцидентів безпеки;

b. не змінює оригінальний вміст або час упорядкування записів аудиту.

Рекомендації з реалізації: Скорочення аудиту — це процес, який обробляє зібрану інформацію аудиту та організовує її у форматі звіту, що є більш зручним для аналітиків. Можливості скорочення аудиту та формування звітів не завжди виконуються тими ж організаційними структурами, які здійснюють діяльність аудиту. Можливість скорочення аудиту може охоплювати, наприклад, сучасні методи генерування даних з використанням удосконалених фільтрів для виявлення аномальної поведінки в записах аудиту. Упорядкування записів аудиту за часом може бути корисним, якщо деталізація мітки часу недостатня.

Пов’язані заходи: AC-2, AU-2, AU-3, AU-4, AU-5, AU-6, AU-12, AU-16, CM-5, IA-5, IR-4, PM-12, SI-4.

Посилення заходів:

(1) СКОРОЧЕННЯ ЗАПИСІВ АУДИТУ ТА ФОРМУВАННЯ ЗВІТУ - АВТОМАТИЧНА ОБРОБКА

Забезпечити та реалізувати можливість обробки записів аудиту для подій, що становлять інтерес, на основі [*Призначення: визначених організацією полів у записах аудиту*].

Рекомендації з реалізації: Події, що становлять інтерес, можна визначити за вмістом конкретних полів запису аудиту, включно з, наприклад, ідентичністю, типами подій, місцем подій, часом подій, датами подій, залученими системними ресурсами, пов'язаними адресами Інтернет-протоколу або доступом до інформаційних об'єктів. Організації можуть визначати критерії подій аудиту в будь-якій необхідній мірі деталізації.

Пов'язані заходи: Немає.

(2) СКОРОЧЕННЯ ЗАПИСІВ АУДИТУ ТА ФОРМУВАННЯ ЗВІТУ - АВТОМАТИЧНЕ СОРТУВАННЯ ТА ПОШУК

[Вилучено: Включено до AU-7(1)].

Посилання: Немає.

## AU-8 ПОЗНАЧКА ЧАСУ

Заходи захисту:

a. Використовувати внутрішньосистемний годинник для створення позначок часу для записів аудиту.

b. Застосовувати позначки часу, які відповідають [*Призначення: деталізація вимірювання часу, визначена організацією*] і використовують всесвітній координований час, мають фіксоване зміщення місцевого часу відносно всесвітнього координованого часу або включають зміщення місцевого часу як частину позначки часу.

Рекомендації з реалізації: Позначка часу містить дату та час. Час зазвичай виражається у форматі UTC, GMT або зазначається місцевий час зі зміщенням від UTC. Організації можуть визначати різні деталі часу для різних компонентів системи. Служба позначок часу може бути критичною для інших можливостей безпеки, таких як контроль доступу, ідентифікація та автентифікація.

Пов'язані заходи: AU-3, AU-12, AU-14, SC-45.
Посилення заходів:

(1) ПОЗНАЧКА ЧАСУ - СИНХРОНІЗАЦІЯ З АВТОРИТЕТНИМ ДЖЕРЕЛОМ ЧАСУ

[Вилучено: Включено до SC-45(1)]

(2) ПОЗНАЧКА ЧАСУ - ВТОРИННЕ АВТОРИТЕТНЕ ДЖЕРЕЛО ЧАСУ

[Вилучено: Включено до SC-45(2)]

Посилання: Немає.

## AU-9 ЗАХИСТ ІНФОРМАЦІЇ АУДИТУ

Заходи захисту:

a. Захист інформації аудиту та інструментів журналювання аудиту від несанкціонованого доступу, зміни та видалення;

b. Сповіщення [*Призначення: персонал або ролі, визначені організацією*] у разі виявлення несанкціонованого доступу, зміни або видалення інформації аудиту.

Рекомендації з реалізації: Інформація аудиту містить усю інформацію, наприклад, записи аудиту, настройки аудиту, звіти аудиту та персональну інформацію, необхідну для успішної діяльності системи аудиту. Інструменти журналювання аудиту – це програми та пристрої, які використовуються для проведення аудиту системи та журналювання. Захист інформації аудиту зосереджується на технічному захисті та обмежує можливість доступу та виконання інструментів журналювання аудиту лише уповноваженими особами. Фізичний захист інформації аудиту стосується способів захисту засобів масової інформації, заходів фізичного захисту та заходів захисту навколишнього середовища.

Пов'язані заходи: AC-3, AC-6, AU-6, AU-11, AU-14, AU-15, MP-2, MP-4, PE-2, PE-3, PE-6, SA-8, SC-8, SI-4.

Посилення заходів:

(1) ЗАХИСТ ІНФОРМАЦІЇ АУДИТУ - АПАРАТНІ НОСІЇ ІНФОРМАЦІЇ ОДНОРАЗОВОГО ЗАПИСУ

Журнали аудиту мають бути записані на апаратні носії інформації з одноразовим записом.

Рекомендації з реалізації: Це посилення заходу застосовується до початкового генерування журналів аудиту (тобто, до збирання записів аудиту, що надають інформацію аудиту, яка повинна використовуватися для виявлення, аналізу та звітності) та резервного копіювання цих журналів аудиту. Удосконалення не поширюється на записи аудиту до того, як вони будуть записані до журналу. До апаратних носіїв інформації з одноразовим записом належать компакт-диски (CD-R, DVD-R). Навпаки, використання змінних носіїв із захистом від запису, таких як стрічкові картриджі, дисководи з універсальною послідовною шиною (USB), компакт-диски з можливістю повторного запису (CD-RW) і цифрові багатофункціональні записи з читанням дисків (DVD-RW) є носіями, захищеними від запису, але з можливістю не одноразового запису.

Пов'язані заходи: AU-4, AU-5.

(2) ЗАХИСТ ІНФОРМАЦІЇ АУДИТУ - ЗБЕРІГАННЯ НА ОКРЕМИХ ФІЗИЧНИХ СИСТЕМАХ АБО КОМПОНЕНТАХ

Зберігати записи аудиту з [*Призначення: визначеною організацією з частотою*] у репозиторії, який є частиною фізично іншої системи або компонента системи, ніж система або компонент, який перевіряється.

Рекомендації з реалізації: Зберігання інформації про аудит в окремому сховищі може гарантувати, що компрометація системи не призведе до компрометації записів аудиту. Зберігання записів аудиту в окремих фізичних системах або

компонентах також зберігає конфіденційність і цілісність записів аудиту та полегшує керування записами аудиту в межах усієї організації. Зберігання записів аудиту в окремих системах або компонентах стосується початкового створення, а також резервного копіювання або тривалого зберігання записів аудиту.

Пов'язані заходи: AU-4, AU-5.

(3) ЗАХИСТ ІНФОРМАЦІЇ АУДИТУ - КРИПТОГРАФІЧНИЙ ЗАХИСТ

Запровадити криптографічні механізми для захисту цілісності інформації аудиту та інструментів аудиту.

Рекомендації з реалізації: Криптографічні механізми, які використовуються для захисту цілісності інформації аудиту, охоплюють використання геш-функцій у парі з асиметричною криптографією, що дозволяє розповсюджувати відкритий ключ для перевірки інформації, зберігаючи конфіденційність особистого ключа.

Пов'язані заходи: AU-10, SC-12, SC-13.

(4) ЗАХИСТ ІНФОРМАЦІЇ АУДИТУ - ДОСТУП, ЯКИЙ НАДАЄТЬСЯ ЧЕРЕЗ ЧЛЕНСТВО В ПІДМНОЖИНІ ПРИВІЛЕЙОВАНИХ КОРИСТУВАЧІВ

Авторизувати доступ до управління функціональністю аудиту тільки для [*Призначення: визначеної організацією підмножини привілейованих користувачів*].

Рекомендації з реалізації: Особи з привілейованим доступом також є предметом аудиту та можуть впливати на надійність інформації аудиту. Це посилення заходу вимагає, щоб привілейований доступ був додатково визначений між привілеями, пов'язаними з аудитом, та іншими привілеями, таким чином обмежуючи користувачів, що мають права користування аудитом.

Пов'язані заходи: AC-5.

(5) ЗАХИСТ ІНФОРМАЦІЇ АУДИТУ - ПОДВІЙНА АВТОРИЗАЦІЯ

Здійснювати подвійну авторизацію для [*Вибір (один або кілька): переміщення; видалення*] [*Призначення: визначеної організацією інформації аудиту*].

Рекомендації з реалізації: Механізми подвійного авторизації (також відомі як контроль двох осіб) вимагають затвердження двох уповноважених осіб для виконання функцій аудиту. Щоб зменшити ризик змови, організації розглядають можливість передачі подвійних повноважень іншим особам. Подвійну авторизацію не застосовують у випадках, коли необхідні негайні реакції для забезпечення громадської та екологічної безпеки.

Пов'язані заходи: AC-3.

(6) ЗАХИСТ ІНФОРМАЦІЇ АУДИТУ - ДОСТУП ТІЛЬКИ ДЛЯ ЧИТАННЯ

Авторизувати доступ лише для читання інформації аудиту для [*Призначення: визначеної організацією підмножини привілейованих користувачів*].

Рекомендації з реалізації: Обмеження привілейованих дозволів користувачів

лише для читання допомагає обмежити потенційний збиток організаціям, які можуть бути ініційовані такими користувачами, наприклад, видалення записів аудиту для приховування зловмисної діяльності.

Пов'язані заходи: Немає.

(7) ЗАХИСТ ІНФОРМАЦІЇ АУДИТУ - ЗБЕРІГАННЯ НА КОМПОНЕНТІ ІНШОЇ ОПЕРАЦІЙНОЇ СИСТЕМИ

Зберігати інформацію про аудит на компоненті, що працює з іншою операційною системою, ніж система або компонент, який проходить аудит.

Рекомендації з реалізації: Це посилення заходу допомагає зменшити ризики при компрометації системи.

Пов'язані заходи: AU-4, AU-5, AU-11, SC-29.

Посилання: FIPS Publications 140-2, 180-4, 202.

## AU-10 НЕСПРОСТОВНІСТЬ

Заходи захисту:
Надавайте неспростовні докази того, що особа (або процес, який діє від імені особи) виконала [*Призначення: дії, визначені організацією, на які поширюється принцип неспростовності*].

Рекомендації з реалізації: До дій, факти здійснення яких не можуть бути спростовані, належать: створення інформації, надсилання й отримання повідомлень та затвердження інформації. Неспростовність захищає від претензій авторів про те, що вони не є авторами певних документів, відправників про те, що вони не передавали повідомлення, одержувачів про те, що вони не отримували повідомлення, і підписантів про те, що вони не підписували документи. Послуги неспростовності можна використовувати, щоб визначити, чи інформація надійшла від особи, чи особа виконала певні дії (наприклад, надсилання електронного листа, підписання контракту, схвалення запиту на закупівлю або отримання конкретної інформації). Організації отримують послуги неспростовності, використовуючи різні техніки або механізми, зокрема цифрові підписи та цифрові квитанції про повідомлення.

Пов'язані заходи: AU-9, PM-12, SA-8, SC-8, SC-12, SC-13, SC-16, SC-17, SC-23.

Посилення заходів:

(1) НЕСПРОСТОВНІСТЬ - АСОЦІАЦІЯ ІДЕНТИЧНОСТІ

a) Зв'язати особистість джерела інформації з інформацією з [*Призначення: визначеною організацією міцністю зв'язування*].

b) Впровадити засоби, якими уповноважені особи можуть визначити особу виробника інформації.

Рекомендації з реалізації: Це посилення заходу застосовується для реалізації вимоги неспростовності створення інформації. Прив'язка ідентифікаторів до

інформації підтримує вимоги до аудиту, які надають персоналу засоби ідентифікації того, хто створив конкретну інформацію, у разі її передачі. Організації визначають і затверджують міцність зв'язку між джерелом інформації та інформацією на основі категорії безпеки інформації та відповідних факторів ризику.

Пов'язані заходи: AC-4, AC-16.

(2) НЕСПРОСТОВНІСТЬ - РАТИФІКАЦІЯ ПРИВ'ЯЗКИ ІНФОРМАЦІЇ ПРО ІДЕНТИЧНІСТЬ ВИРОБНИКА

a) Підтвердити прив'язку інформації про ідентичність джерела до інформації з [*Призначення: визначеною організацією частотою*].

b) Виконати [*Призначення: визначені організацією дії*] у разі помилки перевірки.

Рекомендації з реалізації: Це посилення заходу запобігає модифікації інформації. Валідація зв'язку може бути досягнута, наприклад, за допомогою криптографічних контрольних сум. Організації визначають, чи перевірки виконуються у відповідь на запити користувачів чи генеруються автоматично.

Пов'язані заходи: AC-3, AC-4, AC-16.

(3) НЕСПРОСТОВНІСТЬ - ЛАНЦЮЖОК ЗБЕРЕЖЕННЯ ДОКАЗІВ

Підтримувати перегляд і випуск ідентичності та повноважень у межах встановленого ланцюжка збереження доказів для всієї переглянутої або оприлюдненої інформації.

Рекомендації з реалізації: Ланцюжок збереження доказів — це процес, який відстежує рух доказів протягом його життєвого циклу. Якщо рецензент є людиною, система пов'язує особу рецензента інформації, яка підлягає передачі, з інформацією та інформаційною міткою. Це посилення заходу забезпечує організаційним службовцям засоби для визначення того, хто переглядав та оприлюднював інформацію. У випадку автоматизованих оглядів це поліпшення контролю забезпечує використання лише затверджених функцій огляду.

Пов'язані заходи: AC-4, AC-16.

(4) НЕСПРОСТОВНІСТЬ - ВАЛІДАЦІЯ ЗВ'ЯЗКУ ІДЕНТИЧНОСТІ ПЕРЕГЛЯДАЧА ІНФОРМАЦІЇ

a) Підтвердити прив'язку особистості рецензента до інформації в точках передачі або видачі до її випуску або передачі між [*Призначення: визначеними організацією домени безпеки*].

b) Виконати [*Призначення: визначені організацією дії*] у разі помилки перевірки.

Рекомендації з реалізації: Це посилення контролю запобігає зміні інформації між переглядом і передачею/випуском. Валідація зв'язку може бути досягнута, наприклад, за допомогою криптографічних контрольних сум. Організації визначають, чи перевірки виконуються у відповідь на запити користувачів чи генеруються автоматично.

Пов'язані заходи: AC-4, AC-16.

(5) НЕСПРОСТОВНІСТЬ - ЦИФРОВІ ПІДПИСИ

[Вилучено: Включено до SI-7]

Посилання: FIPS Publications 140-2, 180-4, 186-4, 202, [SP 800-177].

## AU-11 ЗБЕРЕЖЕННЯ ЗАПИСІВ АУДИТУ

Заходи захисту:
Зберігати записи аудиту впродовж *[Призначення: визначеного організацією періоду часу, відповідно політиці зберігання записів*], щоб забезпечити підтримку розслідувань (постфактум) інцидентів безпеки та приватності, а також для задоволення вимог нормативних і документів організації щодо збереження даних аудиту.

Рекомендації з реалізації: Записи аудиту мають зберігатися, поки не буде встановлено, що вони більше не потрібні для адміністративних, юридичних чи інших операційних цілей. Мають бути описані стандартні категорії записів аудиту та стандартні процеси реагування для кожного типу.

Пов'язані заходи: AU-2, AU-4, AU-5, AU-6, AU-9, AU-14, MP-6, RA-5, SI-12.

Посилення заходів:

(1) ЗБЕРЕЖЕННЯ ЗАПИСІВ АУДИТУ - ДОВГОСТРОКОВА МОЖЛИВІСТЬ ОТРИМАННЯ

Впровадити [*Призначення: визначені організацією заходи*], щоб гарантувати, що довгострокові записи аудиту, створені системою, можуть бути отримані.

Рекомендації з реалізації: Це посилення заходу забезпечує технічну можливість довгострокового доступу до записів аудиту. Заходи, які можуть використовуватися: перезаписування в актуальних форматах, збереження технічного обладнання для читання наявних форматів тощо.

Пов'язані заходи: Немає.

Посилання: [OMB A-130].

## AU-12 ГЕНЕРАЦІЯ ДАНИХ АУДИТУ

Заходи захисту:

a. Забезпечити генерацію даних аудиту для типів подій, що перевіряються в AU-2a в [*Призначення: визначених організацією компонентах системи*].

b. Дозволити [*Призначення: визначеному організацією персоналу або посадам*] вибирати, які типи подій, що перевіряються, повинні перевірятися окремими компонентами системи;

c. Генерувати записи аудиту для типів подій, визначених в AU-2c. з вмістом згідно з AU-3.

Рекомендації з реалізації: Записи аудиту можуть формуватися з багатьох різних компонентів системи. Перелік типів подій, вказаних в AU-2d, — це сукупність типів подій, стосовно яких слід проводити аудит. Ці типи подій — підмножина всіх типів подій, для яких система може генерувати записи аудиту.

Пов’язані заходи: AC-6, AC-17, AU-2, AU-3, AU-4, AU-5, AU-6, AU-7, AU-14, CM-5, MA-4, MP-4, PM-12, SA-8, SC-18, SI-3, SI-4, SI-7, SI-10.

Посилення заходів:

(1) ГЕНЕРАЦІЯ ДАНИХ АУДИТУ - ЗАГАЛЬНОСИСТЕМНИЙ ТА СИНХРОНІЗОВАНИЙ ЗА ЧАСОМ ЖУРНАЛУ АУДИТУ

Скомпонувати записи аудиту з [*Призначення: визначеними організацією системними компонентами*] в загальносистемний (логічний або фізичний) журнал аудиту, який синхронізований за часом у межах [*Призначення: визначеного організацією допустимого рівня для взаємозв’язку між мітками часу окремих записів у журналах аудиту*].

Рекомендації з реалізації: Журнал аудиту — це синхронізований за мітками часу в окремих записах аудиту каталог (організація такого каталогу можлива лише за умови, що мітки часу в кожному окремому запису аудиту можуть бути пов’язані з мітками часу в інших записах аудиту).

Пов’язані заходи: AU-8, SC-45.

(2) ГЕНЕРАЦІЯ ДАНИХ АУДИТУ - СТАНДАРТИЗОВАНІ ФОРМАТИ

Створити загальносистемний (логічний або фізичний) журнал аудиту, що складається із записів аудиту в стандартизованому форматі.

Рекомендації з реалізації: Стандартизована (відповідно до прийнятих норм) інформація щодо аудиту може сприяти взаємодії та обміну такою інформацією між різними пристроями та системами. Це сприяє виробленню інформації про події, які можна легше проаналізувати. Якщо механізми ведення журналу не відповідають стандартизованим форматам, системи можуть перетворювати окремі записи аудиту в стандартизовані формати під час формування журналів аудиту системи.

Пов’язані заходи: Немає.

(3) ГЕНЕРАЦІЯ ДАНИХ АУДИТУ - ЗМІНИ, ЩО ВНОСЯТЬ АВТОРИЗОВАНІ ОСОБИ

Забезпечити та реалізувати можливість для [*Призначення: визначених організацією окремих осіб або ролей*] змінити аудит, який виконуватиметься на [*Призначення: визначених організацією компонентах системи*] на основі [*Призначення: визначених організацією критеріїв вибору подій*] у межах [*Призначення: визначених організацією часових порогів*].

Рекомендації з реалізації: Це посилення дозволяє організаціям (за потреби) розширити або обмежити аудит. Обмежений, з метою економії ресурсів, аудит може бути розширений для ліквідації певних загроз. Крім того, аудит може бути обмежений певним набором типів подій для скорочення часу проведення аудиту, аналізу та підготовки звіту аудиту. Організації можуть встановлювати межі часу, для яких дії аудиту змінюються, наприклад, у режимі реального часу, протягом декількох хвилин або протягом години.

Пов’язані заходи: AC-3.

(4) ГЕНЕРАЦІЯ ДАНИХ АУДИТУ - АУДИТ ЗАПИТІВ ПЕРСОНАЛЬНИХ ДАНИХ

Забезпечити та реалізувати можливості аудиту параметрів подій запитів користувачів для наборів даних, що містять персональні дані.

Рекомендації з реалізації: Параметри запиту — це явні критерії, які користувач або автоматизована система надає системі для отримання даних. Аудит параметрів запитів у наборах даних, що містять персональні дані, збільшує відстежуваність (можливість такого аудиту може бути надана лише уповноваженим особам).

Пов'язані заходи: Немає.

Посилання: Немає.

## AU-13 МОНІТОРИНГ РОЗКРИТТЯ ІНФОРМАЦІЇ

Заходи захисту:

a. Моніторинг [*Завдання: визначена організацією інформація з відкритих джерел та/або інформаційних сайтів*] [*Завдання: частота, визначена організацією*] на наявність доказів неавторизованого розголошення конфіденційної інформації;

b. Якщо виявлено розголошення інформації:

1. Повідомити [*Призначення: персонал або ролі, визначені організацією*];

2. Виконайте такі додаткові дії: [*Призначення: додаткові дії, визначені організацією*].

Рекомендації з реалізації: Несанкціоноване розкриття інформації є формою витоку даних. Інформація з відкритих джерел включає сайти соціальних мереж, платформи та сховища обміну кодами. Прикладами організаційної інформації є персональні дані, що зберігаються організацією, або конфіденційна інформація, створена організацією.

Пов'язані заходи: AC-22, PE-3, PM-12, RA-5, SC-7, SI-20.

Посилення заходів:

(1) МОНІТОРИНГ РОЗКРИТТЯ ІНФОРМАЦІЇ - ВИКОРИСТАННЯ АВТОМАТИЧНИХ ЗАСОБІВ

Моніторинг відкритої інформації та інформаційних сайтів за допомогою [*Завдання: визначені організацією автоматизовані механізми*].

Рекомендації з реалізації: Автоматизовані механізми можуть містити, наприклад, автоматизовані сценарії для моніторингу нових публікацій на обраних вебсайтах, а також послуги сповіщення.

Пов'язані заходи: Немає.

(2) МОНІТОРИНГ РОЗКРИТТЯ ІНФОРМАЦІЇ - ОГЛЯД САЙТІВ, ЩО ПІДЛЯГАЮТЬ МОНІТОРИНГУ

Проводити огляд відкритих інформаційних сайтів, що підлягають моніторингу [*Призначення: з визначеною організацією частотою*].

Рекомендації з реалізації: Перегляд поточного списку інформаційних сайтів з відкритими джерелами, які регулярно підлягають моніторингу, допомагає переконатися, що вибрані ці сайти є актуальними. Огляд також надає можливість додавати нові інформаційні сайти з відкритим кодом, які потенційно можуть надати докази неавторизованого розголошення організаційної інформації. Перелік вебсайтів, які підлягають моніторингу, може ґрунтуватися на даних про загрози з інших надійних джерел інформації.

Пов'язані заходи: Немає.

(3) МОНІТОРИНГ РОЗКРИТТЯ ІНФОРМАЦІЇ - АВТОРИЗОВАНЕ КОПІЮВАННЯ ІНФОРМАЦІЇ

Використовуйте методи виявлення, процеси та інструменти, щоб визначити, чи зовнішні суб'єкти копіюють організаційну інформацію неавторизованим способом.

Рекомендації з реалізації: Несанкціоноване використання або копіювання організаційної інформації зовнішніми особами може спричинити негативний вплив на організаційні операції та активи, зокрема завдати шкоди репутації. Така діяльність може включати копіювання вебсайту організації супротивником або ворожою загрозою, яка намагається видати себе за організацію вебхостингу. Інструменти, методи та процеси виявлення, які використовуються для визначення того, чи зовнішні суб'єкти копіюють організаційну інформацію несанкціонованим чином, включають сканування зовнішніх вебсайтів, моніторинг соціальних медіа та навчання персоналу розпізнавати несанкціоноване використання інформації організації.

Пов'язані заходи: Немає.

Посилання: Немає.

## AU-14 АУДИТ СЕСІЇ

Заходи захисту:

a. Надавати та реалізувати можливість для [*Призначення: користувачів або ролей, визначених організацією]* для [*Вибору (одного або кількох): збору/запису або перегляду/прослуховування*] вмісту сесії користувача в [*Призначення: обставини, визначені організацією*];

b. Розробляти, інтегрувати та використовувати діяльність з аудиту сесії, консультуючись із юрисконсультантом щодо її відповідності до чинних законів, розпоряджень, директив, нормативних актів, політик, стандартів і вказівок.

Рекомендації з реалізації: Аудит сесії охоплює: моніторинг натискань клавіш, відстеження відвідуваних вебсайтів, запис інформації та/або передачу файлів. Можливість аудиту сесії реалізована на додаток до реєстрації подій і може передбачати спеціальної технології захоплення сесії. Аудит сесії може виявити інформацію, яка може спричинити ризик конфіденційності, а також способи пом'якшення таких ризиків. Оскільки аудит сесії може вплинути на продуктивність системи та мережі, організації активують цю можливість у чітко визначених ситуаціях (наприклад,

організація підозрює певну особу). Організації консультуються з юрисконсультантами, посадовими особами з питань громадянських свобод і конфіденційності, щоб переконатися, що будь-які юридичні проблеми, проблеми з конфіденційністю, громадянськими правами чи свободами, включно з використанням ідентифікаційної інформації, розглядаються належним чином

Пов'язані заходи: AC-3, AC-8, AU-2, AU-3, AU-4, AU-5, AU-8, AU-9, AU-11, AU-12.

Посилення заходів:

(1) АУДИТ СЕСІЇ - СИСТЕМА ЗАПУСКУ

Автоматично ініціювати аудит сесії при запуску системи.

Рекомендації з реалізації: Автоматична ініціація аудиту сеансу під час запуску допомагає переконатися, що інформація, яка збирається про вибраних осіб, є повною та не підлягає компрометації через втручання зловмисників.

Пов'язані заходи: Немає.

(2) АУДИТ СЕСІЇ - ЗАХОПЛЕННЯ ТА ЗАПИС ІНФОРМАЦІЇ

[Вилучено: Включено до AU-14]

Пов'язані заходи: Немає.

(3) АУДИТ СЕСІЇ - ВІДДАЛЕНИЙ ПЕРЕГЛЯД ТА ПРОСЛУХОВУВАННЯ

Забезпечити та реалізувати можливість авторизованих користувачів віддалено переглядати та прослуховувати вміст, пов'язаний із встановленою сесією користувача, у режимі реального часу.

Рекомендації з реалізації: Немає.

Пов'язані заходи: AC-17.

Посилання: Немає.

## AU-15 АЛЬТЕРНАТИВНА МОЖЛИВІСТЬ АУДИТУ

[Вилучено: Включено до AU-5(5)]

## AU-16 МІЖОРГАНІЗАЦІЙНИЙ АУДИТ

Заходи захисту:
Використовувати [*Призначення: визначені організацією методи*] для координації [*Призначення: визначеної організацією інформації*] серед зовнішніх організацій, коли інформація аудиту передається за межі організації.

Рекомендації з реалізації: Коли організації використовують системи та/або послуги зовнішніх організацій, можливість аудиту потребує узгодженого підходу між організаціями (наприклад, збереження ідентичності осіб, які зверталися за конкретними послугами через організаційні межі). Через те, що втрата конфіденційності іноді неможлива, часто трапляється так, що міжорганізаційний аудит

просто фіксує особу, яка надсилає запити в початковій системі, а наступні системи фіксують, що запити надходили від уповноважених осіб. Організації розглядають можливість включення процесів узгодження вимог щодо інформаційного аудиту та захисту, отриманої в процесі нього інформації, в угоди про обмін інформацією.

Пов'язані заходи: AU-3, AU-6, AU-7, CA-3, PT-7.

Посилення заходів:

(1) МІЖОРГАНІЗАЦІЙНИЙ АУДИТ - ЗБЕРЕЖЕННЯ ІДЕНТИЧНОСТІ

Вимагати, щоб ідентичність особистості зберігалася в міжорганізаційних журналах аудиту.

Рекомендації з реалізації: Це посилення застосовується, коли є необхідність відстежувати дії, які виконуються конкретною особою за межами організації.

Пов'язані заходи: IA-2, IA-4, IA-5, IA-8.

(2) МІЖОРГАНІЗАЦІЙНИЙ АУДИТ - ОБМІН ІНФОРМАЦІЄЮ АУДИТУ

Надавати інформацію про міжорганізаційний аудит до [*Призначення: організацій, визначених організацією*] на основі [*Призначення: визначеної організацією міжорганізаційної угоди про обмін*].

Рекомендації з реалізації: Через розподілений характер інформації аудиту спільний обмін може бути важливим для ефективного аналізу аудиту. Наприклад, записи аудиту однієї організації можуть не надати достатньої інформації для визначення належного або неналежного використання ресурсів особами інших організацій. У деяких випадках лише «домашні» організації мають відповідні дані для ухвалення таких рішень.

Пов'язані заходи: IR-4, SI-4.

(3) МІЖОРГАНІЗАЦІЙНИЙ АУДИТ - РОЗМЕЖУВАННЯ

Запровадити [*Призначення: заходи, визначені організацією*], щоб розмежувати людей від інформації аудиту, що передається в межах організації.

Рекомендації з реалізації: Збереження ідентичності в журналах аудиту може мати наслідки для конфіденційності, наприклад, створювати умови щодо відстеження та створення профілю осіб, які не є необов'язковими з операційної точки зору. Ці ризики можуть бути ще більше посилені при передачі інформації в межах організації. Впровадження криптографічних методів, що підвищують конфіденційність, може розмежувати людей від інформації аудиту, зменшити ризики конфіденційності та зберегти підзвітність.

Пов'язані заходи: Немає.

Посилання: Немає.

## 10.4 Клас заходів захисту CA — ОЦІНЮВАННЯ, АКРЕДИТАЦІЯ ТА МОНІТОРИНГ БЕЗПЕКИ

### CA-1 ПОЛІТИКА І ПРОЦЕДУРИ ОЦІНЮВАННЯ, АКРЕДИТАЦІЇ ТА МОНІТОРИНГУ

Заходи захисту:

a. Розробити, задокументувати та поширити серед [*Призначення: визначеного організацією персоналу або посад*]:

1. [*Вибір (один або декілька): Рівень організації; Рівень місії/бізнес-процесу; рівень системи*] політика оцінювання, авторизації та моніторингу, яка:

(a) містить мету, сферу застосування, ролі, обов'язки, відповідальність керівництва, координацію між організаційними підрозділами та систему контролю відповідності (complaince);

(b) відповідає чинним законам, нормативним документам, наказам, положенням, політиці, стандартам і керівним принципам.

2. Процедури, що сприяють реалізації політики оцінювання, авторизації та моніторингу безпеки та приватності, а також пов'язаних з ними заходів оцінювання, авторизації та моніторингу безпеки та приватності.

b. Призначити [*Призначення: посадова особа, визначена організацією*] для управління розробкою, документуванням і розповсюдженням політики та процедур оцінювання, авторизації та моніторингу;

c. Переглядати та оновлювати поточне оцінювання, авторизацію та моніторинг:

1. Політику [*Призначення: частота, визначена організацією*] та наступне [*Призначення: події, визначені організацією*];

2. Процедури [*Призначення: частота, визначена організацією*] та наступні [*Призначення: події, визначені організацією*].

Рекомендації з реалізації: Цей захід захисту стосується встановлення політики та процедур для ефективного здійснення заходів і їхніх посилень у класі CA. Стратегія управління ризиками є важливим фактором у встановленні політики та процедур. Комплексна політика та процедури допомагають забезпечити безпеку та приватність. За наявності політики, а також планів захисту інформації та персональних даних на рівні організації, конкретні системні політики та процедури можуть бути не потрібні. Політика може бути внесена до складу загальної політики безпеки та приватності або може бути представлена кількома політиками (у випадках складної архітектури). Процедури описують, як має реалізуватися політика чи заходи захисту та як вони можуть бути спрямовані на персонал або роль, яка є об'єктом процедури. Процедури можуть бути задокументовані в планах захисту інформації та персональних даних (як один або декілька документів). Події, які можуть спричинити оновлення політики та процедур оцінки, авторизації та моніторингу, включають висновки оцінювання чи аудиту, інциденти чи порушення безпеки або зміни у чинних законах, розпорядженнях, директивах, постановах, політиках, стандартах і вказівках. Просте повторне встановлення засобів контролю не є організаційною політикою чи процедурою

Пов’язані заходи: PM-9, PS-8, SI-12

Посилення заходів: Немає.

Посилання: Немає.

## CA-2 ОЦІНЮВАННЯ

Заходи захисту:

a. Виберіть відповідного оцінювача або команду з оцінки для типу оцінювання, яке буде проводитися;

b. Розробіть план контрольної оцінки, який описує обсяг оцінки, в тому числі:

   1. заходи захисту та посилені заходи, що підлягають оцінюванню;

   2. процедури оцінювання, які використовуватимуться для визначення ефективності заходів;

   3. середовище оцінювання, групу оцінювання, ролі й обов’язки з оцінювання.

c. Забезпечити розгляд і затвердження плану оцінювання уповноваженою офіційною особою або призначеним для проведення оцінювання представником;

d. Оцінити заходи захисту в системі та в її середовищі функціонування з [*Призначення: визначеною організацією частотою*] для визначення, наскільки коректно реалізовані заходи безпеки і чи працюють вони за призначенням і дають бажаний результат щодо дотримання встановлених вимог безпеки та приватності;

e. Підготовити звіт оцінювання безпеки, який документує результати оцінювання;

f. Надати результати оцінювання з безпеки [*Призначення: особам або ролям, визначеним організацією*].

Рекомендації з реалізації: Оцінювачі гарантовано мають володіти необхідними навичками та технічними знаннями для розробки результативних планів оцінювання та проведення оцінювання системно-специфічних, гібридних, загальних і програмних заходів контролю, якщо це необхідно. Необхідні навички включають загальні знання концепцій і підходів до управління ризиками, а також комплексні знання та досвід роботи з апаратним і програмним забезпеченням та системними компонентами вбудованого програмного забезпечення.
Організації оцінюють заходи захисту в системах і середовищах, у яких ці системи працюють, як частину початкових і поточних авторизацій, безперервного моніторингу, щорічних оцінок FISMA, проектування та розробку системи, розробку системи безпеки, розробку приватності та життєвого циклу системи. Оцінювання допомагає переконатися, що впроваджені заходи захисту відповідають вимогам інформаційної безпеки та приватності, виявляють слабкі місця та недоліки у проектуванні системи, надають важливу інформацію, необхідну для прийняття рішень, заснованих на ризиках в рамках процесів авторизації та мають процедури для пом’якшення вразливості. Оцінювання щодо впроваджених заходів відбувається відповідно до планів захисту інформації та персональних даних. Оцінювання також

може проводитися протягом життєвого циклу системи як частина процесів системної інженерії та розробки системної безпеки. Спроектовані засоби захисту можна оцінити під час розробки запитів на пропозиції, оцінки відповідей та проведення аналізу такого проектування. Якщо план впровадження заходів захисту та подальше впровадження відповідно до проекту оцінюється під час розробки, остаточне контрольне тестування може бути простим підтвердженням із використанням попередньо завершеної контрольної оцінки та всіх результатів.

Організації можуть розробити єдиний зведений план оцінювання безпеки та приватності для системи або окремі плани. Зведений план оцінювання чітко розмежовує ролі та відповідальність за контрольне оцінювання. Якщо в оцінці системи беруть участь кілька організацій, скоординований підхід може зменшити надмірність і пов'язані з цим витрати.

Організації можуть використовувати інші види заходів з оцінювання, такі як сканування вразливостей і моніторинг системи для підтримки безпеки та приватності протягом усього життєвого циклу. Звіти про оцінювання документуються достатньо детально, для того щоб можна було визначити: точність, повноту звітів і нехибність того, що контролювання виконано правильно, у відповідності до призначення; створити бажаний результат щодо дотримання вимог. Результати оцінювання надаються посадовим особам або ролям, відповідальним за сегменти, які проходили оцінювання.

У ході щорічного оцінювання організації можуть використовувати такі джерела: початкові або поточні результати акредитації системи, результати поточного моніторингу тощо. Організації забезпечують, щоб результати оцінювання були актуальними та отриманими з відповідним рівнем незалежності. Наявні результати контрольного оцінювання можуть бути використані повторно, якщо це потрібно. Частота проведення оцінювання встановлюється відповідно до стратегій моніторингу безпеки організації. Зовнішній аудит включно з аудитом зовнішніх організацій, таких як регулювальні органи, не входить у сферу цього заходу.

Пов'язані заходи: AC-20, CA-5, CA-6, CA-7, PM-9, RA-5, RA-10, SA-11, SC-38, SI-3, SI-12, SR-2, SR-3.

Посилення заходів:

(1) ОЦІНЮВАННЯ - НЕЗАЛЕЖНІ ЕКСПЕРТИ

Залучати незалежних експертів або групи з оцінювання для проведення оцінювання безпеки та приватності.

Рекомендації з реалізації: Незалежні експерти або групи з оцінювання — це особи або групи, які проводять неупереджене оцінювання систем. Неупередженість передбачає, що експерти не мають жодних інтересів до розробки, експлуатації, підтримки чи управління системами, що оцінюються. Для досягнення неупередженості експерти: не повинні мати взаємного чи конфліктного інтересу з організаціями, де проводяться оцінювання; не можуть оцінювати власну роботу; не можуть виконувати функції керівників або службовців організацій, у яких проводиться оцінювання. Уповноважені посадові особи визначають необхідний рівень незалежності на основі категорій безпеки систем та/або ризику для операцій організації, активів або осіб.

Уповноважені особи визначають необхідний рівень незалежності на основі категорій безпеки систем та/або ризику для операцій організації, активів або осіб та рівень незалежності оцінювача для впевненості у тому, що результати є

надійними та їх можна використовувати для ухвалення достовірних рішень.
Визначення незалежності оцінювача включає в себе те, чи мають послуги з оцінки за контрактом достатню незалежність, наприклад, коли власники системи не беруть безпосередньої участі в процесах укладання контрактів або не можуть вплинути на неупередженість оцінювачів, які проводять оцінювання. На етапі проектування та розробки системи наявність незалежних оцінювачів аналогічна наявності незалежних малих і середніх підприємств, залучених до перевірки такого проектування.
Якщо організації, які володіють системами, невеликі або структури організацій вимагають, щоб оцінювання проводили особи, які перебувають у ланцюжку розробки, експлуатації чи управління власниками системи, незалежності в процесах оцінювання можна досягти, забезпечивши ретельний аналіз результатів оцінювання, перевіривши та проаналізувавши їх незалежними групами експертів для підтвердження повноти, точності, цілісності та надійності.

Пов'язані заходи: Немає.

(2) ОЦІНЮВАННЯ - СПЕЦІАЛІЗОВАНІ ОЦІНКИ

Ввести як частину оцінювання заходів безпеки та приватності, [*Призначення: з визначеною організацією частотою*], [*Вибір: з попередженням; без попередження*], [*Вибір (один або кілька): поглиблений моніторинг; сканування уразливостей; тестування на шкідливих користувачів; оцінювання внутрішньої загрози; тестування продуктивності та навантаження;* [*Призначення: організаційно визначені інші форми оцінювання*]].

Рекомендації з реалізації: Організації можуть проводити спеціалізовані оцінювання включно з: перевіркою підтвердження інсайдерської загрози, тестуванням «зловмисних» користувачів, моніторингом системи та іншими формами тестування. Такі оцінювання можуть поліпшити готовність системи безпеки та приватності, визначити поточний рівень ефективності таких систем. Організації проводять такі типи спеціалізованих оцінювань відповідно до чинного законодавства, наказів, директив, політик, положень, стандартів і вказівок. Уповноважені посадові особи затверджують методи оцінювання згідно з виконавчою функцією щодо організаційного ризику. Організації можуть у процесах усунення вразливості враховувати виявлені під час оцінювань вразливості.

Пов'язані заходи: PE-3, SI-2.

(3) ОЦІНЮВАННЯ - ЗОВНІШНІ ОРГАНІЗАЦІЇ

Використовуйте результати контрольного оцінювання, які виконує [*Призначення: зовнішня організація, визначена організацією*] на [*Призначення: система, визначена організацією]*, коли оцінювання відповідає [*Завдання: вимоги, визначені організацією*].

Рекомендації з реалізації: Організації можуть покладатися на оцінювання безпеки та приватності систем організації, що визначені іншими (зовнішніми) організаціями. Використання таких оцінювань і повторне використання наявних результатів оцінювання може значно скоротити час і ресурси, необхідні для проведення оцінювань. Фактори, які враховують організації при визначенні того, чи приймати результати оцінювання від зовнішніх організацій, можуть

містити: минулий досвід; репутацію організації, що проводить оцінювання; рівень деталізації наданих оцінок тощо. Акредитовані випробувальні лабораторії, які підтримують Програму загальних критеріїв [ISO 15408-1], Програму перевірки криптографічного модуля NIST (CMVP) або Програму перевірки криптографічного алгоритму NIST (CAVP), можуть надавати результати незалежного оцінювання, які організації можуть використовувати.

Пов'язані заходи: SA-4.

Посилання: FIPS Publication 199. [OMB A-130], [FIPS 199], [SP 800-18], [SP 800-37], [SP 800-39], [SP 800-53A], [SP 800-115], [SP 800-137], [IR 8011-1], [IR 8062].

## CA-3 ВЗАЄМОДІЯ СИСТЕМ

Заходи захисту:

a. схвалити та керувати обміном інформацією між системою та іншими системами за допомогою [*Вибір (один або кілька): угоди безпеки взаємозв'язку; договори безпеки обміну інформацією; меморандуми про взаєморозуміння; угоди про рівень обслуговування; угоди користувача; угоди про нерозголошення; [Доручення: тип договору, визначений організацією*]];.

b. документувати, як частину угоди про обмін, характеристики інтерфейсу, вимоги до безпеки та приватності, засоби контролю та відповідальність для кожної системи, а також характер переданої інформації;

c. здійснювати перегляд та оновлення угод з [*Призначення: визначеною організацією частотою*].

Рекомендації з реалізації: Цей захід захисту застосовується до виділених з'єднань між двома або більше окремими системами. Обмін системною інформацією включає підключення через орендовані лінії або віртуальні приватні мережі, підключення до постачальників послуг Інтернету, спільне використання бази даних або обмін інформацією про транзакції баз даних, підключення та обмін із хмарними службами, обмін через вебслужби або обмін файлами через протоколи передачі файлів, мережевих протоколів (наприклад, IPv4, IPv6), електронної пошти чи іншого типу зв'язку між організаціями. Організації враховують ризики, пов'язані з новими або посиленими загрозами, які можуть виникнути, коли відбувається обмін інформацією з іншими системами, які можуть мати інші вимоги до безпеки та приватності та елементи керування. Сюди входять системи в межах однієї організації та зовнішні по відношенню до організації системи. Спільна авторизація систем, які обмінюються інформацією, як описано в CA-6(1) або CA-6(2), може допомогти налагодити зв'язок і зменшити ризики.
Уповноважені посадові особи визначають ризик, пов'язаний з обміном системною інформацією, і засоби контролю, необхідні для належного зменшення ризику. Вибрані типи угод базуються на таких факторах, як рівень впливу інформації, якою обмінюються, відносини між організаціями, які обмінюються інформацією (наприклад, уряд — уряд, уряд — бізнес, бізнес — бізнес, уряд або бізнес — постачальник послуг, уряд або бізнес для окремої особи), або рівень доступу до системи користувачам іншої системи. Якщо системи, які обмінюються інформацією, мають одну і ту саму посадову особу, організаціям не потрібно укладати угоди.

Натомість характеристики інтерфейсу між системами (наприклад, як відбувається обмін інформацією, як інформація захищена) описані у відповідних планах безпеки та приватності. Якщо системи, які обмінюються інформацією, мають різних уповноважених осіб в одній організації, організації можуть розробити угоди або надати однакову інформацію у відповідному типі угоди CA-3a та у відповідних планах безпеки та приватності для систем. Організації можуть включати інформацію про угоди в офіційні контракти, особливо для обміну інформацією між федеральними агентствами та нефедеральними організаціями (включно з постачальниками послуг, підрядниками, розробниками систем і системними інтеграторами). У рамках оцінювання ризику, організації мають розглядати системи, які спільно використовують одні й ті самі мережі.

Пов'язані заходи: AC-4, AC-20, AU-16, CA-6, IA-3, PL-2, PT-7, RA-3, SA-9, SC-7, SI-12.

Посилення заходів:

(1) ВЗАЄМОДІЯ СИСТЕМ- НЕЗАХИЩЕНІ З'ЄДНАННЯ СИСТЕМИ

[Вилучено: Включено до SC-7(25)].

(2) ВЗАЄМОДІЯ СИСТЕМ - ЗАХИЩЕНІ З'ЄДНАННЯ СИСТЕМИ

[Вилучено: Включено до SC-7(26)].

(3) ВЗАЄМОДІЯ СИСТЕМ - НЕСЕКРЕТНІ З'ЄДНАННЯ СИСТЕМИ БЕЗПЕКИ, ЩО НЕ Є НАЦІОНАЛЬНИМИ

[Вилучено: Включено до SC-7(27)].

(4) ВЗАЄМОДІЯ СИСТЕМ - ПІДКЛЮЧЕННЯ ДО ЗАГАЛЬНОДОСТУПНИХ МЕРЕЖ

[Вилучено: Включено до SC-7(28)].

(5) ВЗАЄМОДІЯ СИСТЕМ - ОБМЕЖЕННЯ ЗВ'ЯЗКУ ІЗ ЗОВНІШНІМИ СИСТЕМАМИ

[Вилучено: Включено до SC-7(5)].

(6) ВЗАЄМОДІЯ СИСТЕМ – ПЕРЕДАЧА ДОЗВОЛІВ

Переконатися, що особи або системи, які передають дані між взаємопов'язаними системами, мають необхідні повноваження (тобто дозволи на запис або привілеї), до прийняття таких даних.

Рекомендації з реалізації: Для запобігання неавторизованого доступу особами і системами при передачі інформації до захищених систем, захищена система перевіряє за допомогою незалежних засобів — чи має особа або система, які намагаються передати інформацію такі повноваження (наприклад, маршрутизація та DNS і служби як, автентифіковані ретранслятори SMTP).

Пов'язані заходи: AC-2, AC-3, AC-4.

(7) ВЗАЄМОДІЯ СИСТЕМ – ТРАНЗИТИВНИЙ ОБМІН ІНФОРМАЦІЄЮ

a) Визначити транзитивний (низхідний) обмін інформацією з іншими системами через системи, визначені в CA-3a;

b) Вжити заходів для забезпечення припинення транзитивного (низхідного) обміну інформацією, коли засоби контролю ідентифікованих транзитивних (низхідних) систем не можуть бути перевірені або підтверджені.

Рекомендації з реалізації: Транзитивний або «нисхідний» обмін інформацією — це обмін інформацією між системою або системами, з якими система організації обмінюється інформацією. Для важливих систем, послуг і програм, включаючи активи високої вартості, необхідно ідентифікувати такі обміни інформацією. Прозорість засобів контролю або заходів захисту, що діють у таких нисхідних системах, прямо чи опосередковано пов'язаних з організаційними системами, має важливе значення для розуміння ризиків безпеки та приватності, пов'язаних із таким обміном інформацією. Системи, що належать організації, можуть успадкувати ризики від нисхідних систем через транзитивні зв'язки та обмін інформацією, та стати більш сприйнятливими до загроз, небезпек і несприятливих впливів.

Пов'язані заходи: SC-7.

Посилання: FIPS Publication 199. [OMB A-130], [FIPS 199], [SP 800-47].

## CA-4 СЕРТИФІКАЦІЯ БЕЗПЕКИ

[Вилучено: Включено до CA-2].

## CA-5 ПЛАН УСУНЕННЯ НЕДОЛІКІВ ТА КОНТРОЛЬНІ ПОКАЗНИКИ

Заходи захисту:

a. Розробити для системи план усунення недоліків та контрольні показники з метою документування запланованих коригувальних дій організації для усунення недоліків і зауважень, які виявлені в ході оцінювання заходів захисту, а також для зменшення або усунення відомих вразливостей у системі.

b. Оновлювати чинний план усунення недоліків та контрольні показники з [*Призначення: визначеною організацією частотою*] на основі результатів оцінювання заходів, незалежних аудитів та постійного моніторингу.

Рекомендації з реалізації: Плани усунення недоліків та контрольні показники є необхідними документами в пакетах дозволів.

Пов'язані заходи: CA-2, CA-7, PM-4, PM-9, RA-7, SI-2, SI-12.

Посилення заходів:

(1) ПЛАН УСУНЕННЯ НЕДОЛІКІВ ТА КОНТРОЛЬНІ ПОКАЗНИКИ - АВТОМАТИЗАЦІЯ ПІДТРИМКИ ЗАДЛЯ ТОЧНОСТІ ТА ВЖИВАНОСТІ

Забезпечити точність, актуальність і доступність плану усунення недоліків і основних етапів для системи за допомогою [*Завдання: автоматизовані*

*механізми, визначені організацією*].

Рекомендації з реалізації: Використання автоматизованих інструментів допомагає підтримувати точність, актуальність і доступність плану усунення недоліків і етапів, а також полегшує координацію та обмін інформацією про безпеку та приватність у всій організації. Така координація та обмін інформацією допомагають виявляти слабкі місця або недоліки в системах і забезпечують своєчасне спрямування відповідних ресурсів на найбільш критично вразливі місця системи.

Пов'язані заходи: Немає.

Посилання: [OMB A-130], [SP 800-37].

## CA-6 АКРЕДИТАЦІЯ

Заходи захисту:

a. Призначити старшого керівника, який відповідає за систему;

b. Призначити старшого керівника, відповідального за систему, та будь-які загальні заходи захисту, успадковані системою.

c. Переконатися перед початком функціонування системи, що посадова особа:

   1. акредитує загальні заходи захисту, що успадковані системою;

   2. акредитує систему на функціонування за призначенням.

d. Переконайтеся, що посадова особа, яка акредитує засоби захисту, дозволяє використання цих засобів захисту для успадкування організаційними системами;

e. Оновлювати акредитацію [*Призначення: з визначеною організацією частотою*].

Рекомендації з реалізації: Акредитація — це офіційне рішення керівних органів, які надають дозвіл на експлуатацію систем (включно з управлінням дочірніми системами) та приймають ризик для операцій організації і активів фізичних осіб, інших організацій на основі реалізації узгоджених принципів, після впровадження заходів захисту. Уповноважені посадові особи здійснюють нагляд за системами організації або беруть на себе відповідальність за функції та процеси, підтримувані цими системами. Уповноважені посадові особи несуть відповідальність за ризики безпеки та приватності, пов'язані з функціонуванням та використанням систем. Організації проводять постійну акредитацію систем шляхом постійного моніторингу безпеки. Уповноважені особи видають поточні дозволи системам на основі доказів, отриманих із запроваджених програм постійного моніторингу. Надійні програми постійного моніторингу зменшують потребу в окремих процесах акредитації. Завдяки використанню всебічних процесів постійного моніторингу безпеки важлива інформація, що міститься в пакетах акредитації, включно з планами захисту інформації та персональних даних, звітами про оцінювання безпеки та приватності, а також планами усунення недоліків та контрольними показниками, постійно оновлюються. Це забезпечує уповноваженим посадовим особам, власникам систем наявність інформації про актуальний стан безпеки та приватності систем, органів

управління та робочих середовищ. Щоб зменшити витрати на повторну акредитацію, уповноважені особи максимально використовують результати безперервного моніторингу безпеки як основу для ухвалення рішень про повторну акредитацію.

Пов'язані заходи: CA-2, CA-3, CA-7, PM-9, PM-10, RA-3, SA-10, SI-12.

Посилення заходів:

(1) АКРЕДИТАЦІЯ - СПІЛЬНА АКРЕДИТАЦІЯ — ОДНА Й ТА САМА ОРГАНІЗАЦІЯ

Впровадити спільний процес акредитації для системи, що має кількох уповноважених посадових осіб однієї організації, які здійснюють акредитацію.

Рекомендації з реалізації: Призначення декількох уповноважених осіб однієї організації виконувати спільні функції з акредитації підвищує рівень незалежності в процесі ухвалення рішень. Також реалізується концепція поділу обов'язків. Це посилення є найбільш актуальним для взаємопов'язаних систем, спільних систем і систем з декількома власниками інформації.

Пов'язані заходи: AC-6.

(2) АКРЕДИТАЦІЯ - СПІЛЬНА АКРЕДИТАЦІЯ — РІЗНІ ОРГАНІЗАЦІЇ

Впровадити спільний процес акредитації для системи, що має кількох уповноважених посадових осіб з принаймні однією уповноваженою посадовою особою з організації, яка є зовнішньою організацією, що здійснює акредитацію.

Рекомендації з реалізації: Призначення декількох уповноважених службових осіб, принаймні одна з яких є від зовнішньої організації, виконувати спільні функції підвищує рівень незалежності в процесі ухвалення рішень. Також реалізується концепції поділу обов'язків. Залучення уповноважених осіб із зовнішніх організацій для доповнення функцій посадової особи, яка має дозвіл від організації, що є власником системи або власником приміщення, де розміщується система, може бути необхідним у випадках, коли ці організації мають заінтересовані частки або акції. Це посилення може застосовуватися для взаємопов'язаних систем, спільних систем і систем з декількома власниками інформації.

Пов'язані заходи: AC-6.

Посилання: [OMB A-130], [SP 800-37], [SP 800-137].

## CA-7 БЕЗПЕРЕРВНИЙ МОНІТОРИНГ

Заходи захисту:
Розробити стратегію безперервного моніторингу безпеки та приватності й упровадити програму безперервного моніторингу безпеки та приватності, яка охоплює:

a. встановлення показників безпеки та приватності, які необхідно відстежувати: [*Призначення: визначені організацією метрики*];

b. встановлення [*Призначення: визначена організацією частота*] для моніторингу та [*Призначення: визначена організацією частота*] для безперервного оцінювання

ефективності заходів захисту;

c. поточні оцінювання заходів захисту відповідно до стратегії безперервного моніторингу організації;

d. постійний моніторинг стану безпеки та приватності відповідно до встановлених організацією метрик і відповідно до стратегії безперервного моніторингу організації;

e. зіставлення та аналіз інформації, отриманої в результаті оцінювання та моніторингу безпеки та приватності;

f. дії реагування за результатами аналізу інформації, пов'язаної з безпекою та приватністю;

g. повідомлення про статус безпеки та приватності системи [*Призначення: визначені організацією персонал або ролі*] з [*Призначення: визначеною організацією частотою*].

Рекомендації з реалізації: Програма безперервного моніторингу безпеки сприяє постійній поінформованості про загрози, вразливості, інформаційну безпеку та приватність для підтримки ухвалення рішень організації щодо управління ризиками. Терміни «безперервний» і «постійний» означають, що організації оцінюють і контролюють свої заходи захисту та ризики з частотою, достатньою для підтримки рішень на основі оцінки ризиків. Для різних типів заходів захисту може знадобитися різна частота моніторингу. Результати безперервного моніторингу генерують дії організацій щодо реагування на ризики. Під час моніторингу ефективності кількох заходів захисту, які були згруповані, може знадобитися аналіз першопричини, щоб визначити конкретний захід захисту, який не працює. Програми безперервного моніторингу також дозволяють підтримувати акредитацію систем і контроль у режимі реального часу, враховуючи динамічні умови роботи із зміною потреб, загроз, вразливостей і технологій. Доступ до інформації, що стосується безпеки та приватності, постійно надається у вигляді звітів та інформаційних панелей і дає посадовим особам можливість ухвалювати ефективні та своєчасні рішення щодо управління ризиками, включно з поточними рішеннями про акредитацію.
Автоматизація моніторингу підтримує частіші оновлення обладнання, програмного забезпечення, пакетів акредитації та іншої системної інформації. Ефективність підвищується, коли результати безперервного моніторингу форматуються для надання інформації, яка є конкретною, вимірюваною, дієвою, відповідною та своєчасною. Заходи безперервного моніторингу масштабуються відповідно до категорій безпеки систем. Вимоги до моніторингу, включно з потребою в спеціальному моніторингу, вказані в інших заходах захисту та посилених заходах захисту, таких як AC-2g, AC 2(7), AC-2(12)(a), AC-2(7)( b), AC-2(7)(c), AC-17(1), AT-4a, AU-13, AU-13(1), AU-13(2), CM-3f, CM 6d, CM-11c, IR-5, MA-2b, MA-3a, MA-4a, PE-3d, PE-6, PE-14b, PE-16, PE-20, PM-6, PM-23, PM 31, PS-7e, SA-9c, SR-4, SC-5(3)(b), SC-7a, SC-7(24)(b), SC-18b, SC-43b і SI-4.

Пов'язані заходи: AC-2, AC-6, AC-17, AT-4, AU-6, AU-13, CA-2, CA-5, CA-6, CM-3, CM-4, CM-6, CM-11, IA-5, IR-5, MA-2, MA-3, MA-4, PE-3, PE-6, PE-14, PE-20, PL-2, PM-4, PM-6, PM-9, PM-10, PM-12, PM-14, PM-23, PM-28, PM-31, PS-7, PT-7, RA-3, RA-5, RA-7, RA-10, SA-8, SA-9, SA-11, SC-5, SC-7, SC-18, SC-38, SC-43, SI-3, SI-4, SI-12, SR-6.

Посилення заходів:

(1) БЕЗПЕРЕРВНИЙ МОНІТОРИНГ - НЕЗАЛЕЖНЕ ОЦІНЮВАННЯ

Залучити незалежних експертів або групи з оцінювання, щоб постійно спостерігати за заходами захисту в системі.

Рекомендації з реалізації: Організації можуть максимізувати значення контрольних оцінок під час процесу постійного моніторингу, вимагаючи, щоб оцінювання проводились експертами з відповідним рівнем незалежності. Необхідний рівень незалежності експерта визначається, базуючись на стратегії безперервного моніторингу. Незалежність експерта забезпечує певну неупередженість у процесі моніторингу. Для досягнення такої неупередженості експерти: не повинні мати жодного конфліктного інтересу з організаціями, де проводяться оцінювання; не повинні оцінювати власну роботу; не повинні виконувати функції посадових осіб організацій.

Пов’язані заходи: Немає.

(2) БЕЗПЕРЕРВНИЙ МОНІТОРИНГ - ВИДИ ОЦІНОК

[Вилучено: Включено до CA-2]

(3) БЕЗПЕРЕРВНИЙ МОНІТОРИНГ - АНАЛІЗ ТЕНДЕНЦІЇ

Впровадити аналіз тенденцій, щоб визначити, чи потрібно змінювати реалізацію заходу захисту, частоту постійних моніторингових заходів і види діяльності, що використовуються в процесі безперервного моніторингу, на основі емпіричних даних.

Рекомендації з реалізації: Аналіз тенденцій включає: вивчення останніх відомостей про загрози, що відбулися в межах організації; вивчення показників успішності певних типів атак; вивчення вразливих ситуацій у конкретних технологіях (у тому числі реалізованих за допомогою методів соціальної інженерії та інтелектуального аналізу); вивчення результатів багаторазового оцінювання заходів, ефективності параметрів конфігурації та висновків інспекторів або аудиторів.

Пов’язані заходи: Немає.

(4) БЕЗПЕРЕРВНИЙ МОНІТОРИНГ - МОНІТОРИНГ РИЗИКУ

Забезпечити моніторинг ризиків, що є невід’ємною частиною стратегії постійного моніторингу та включає:

(a) моніторинг ефективності;

(b) моніторинг відповідності;

(c) моніторинг змін.

Рекомендації з реалізації: Моніторинг ризиків базується на встановленій організаційній толерантності до ризику. Моніторинг ефективності визначає постійну ефективність впроваджених заходів реагування на ризики. Моніторинг відповідності перевіряє, чи впроваджено необхідні заходи реагування на ризики. Він також перевіряє дотримання вимог безпеки та приватності. Моніторинг змін визначає зміни в системах організації і робочому середовищі, які можуть вплинути на ризики безпеки та приватності.

Пов'язані заходи: Немає.

(5) БЕЗПЕРЕРВНИЙ МОНІТОРИНГ - УЗГОДЖЕНИЙ АНАЛІЗ

Застосуйте наступні дії, щоб перевірити, що політики встановлені, а запроваджені заходи захисту працюють узгоджено: [*Призначення: дії, визначені організацією*].

Рекомендації з реалізації: Елементи керування безпекою та приватністю часто додаються до системи поступово. Як наслідок, політика вибору та впровадження засобів захисту може бути непослідовною, а засоби захисту можуть не працювати узгоджено чи скоординовано. Як мінімум відсутність узгодженості та координації може означати, що в системі є прогалини в безпеці та приватності. У гіршому випадку це може означати, що деякі елементи заходи захисту, реалізовані в одному місці або одним компонентом, фактично перешкоджають функціонуванню інших заходів захисту (наприклад, шифрування внутрішнього мережевого трафіку може перешкоджати моніторингу). Також, відсутність узгодженого моніторингу всіх реалізованих мережевих протоколів (наприклад, подвійний стек IPv4 і IPv6) може створити ненавмисні вразливості в системі, якими можуть скористатися зловмисники. Підтвердження того, що впроваджені заходи захисту працюють узгоджено, скоординовано та не перешкоджають роботі одне одному, досягається за допомогою тестування, моніторингу та аналізу.

Пов'язані заходи: Немає.

(6) БЕЗПЕРЕРВНИЙ МОНІТОРИНГ - АВТОМАТИЧНА ПІДТРИМКА МОНІТОРИНГУ

Забезпечити точність, актуальність і доступність результатів моніторингу для системи за допомогою [*Завдання: автоматизовані механізми, визначені організацією*]

Рекомендації з реалізації: Використання автоматизованих інструментів для моніторингу допомагає підтримувати точність, актуальність і доступність моніторингової інформації, та, як наслідок, допомагає підвищити рівень постійної обізнаності про безпеку системи та стан конфіденційності для підтримки рішень організації щодо управління ризиками.

Пов'язані заходи: Немає.

Посилання: [OMB A-130], [SP 800-37], [SP 800-39], [SP 800-53A], [SP 800-115],[SP 800-137], [IR 8011-1], [IR 8062].

## CA-8 ТЕСТУВАННЯ НА ПРОНИКНЕННЯ

Заходи захисту:
Проводити тестування на проникнення з [*Призначення: визначеною організацією частотою*] у [*Призначення: визначеній організацією інформаційній системі чи системному компоненті*].

Рекомендації з реалізації: Тестування на проникнення — це спеціалізований тип оцінювання, що проводиться стосовно систем або окремих компонентів системи для виявлення вразливих місць, які можуть бути використані зловмисниками. Тестування на проникнення виходить за рамки автоматизованого сканування вразливості й найефективніше проводиться агентами тестування на проникнення та командами, що мають навички й досвід, які залежать від сфери тестування на проникнення, включно з технічною експертизою в мережі, в операційній системі та/або в безпеці на рівні застосунків. Тестування на проникнення можна використовувати або для перевірки вразливості, або для визначення ступеня стійкості до проникнення в межах визначених обмежень. Такі обмеження містять, наприклад, час, ресурси та навички. При тестуванні на проникнення експерт намагається дублювати дії супротивників при здійсненні нападів та забезпечує глибший аналіз безпеки та приватності. Тестування на проникнення намагається дублювати дії зловмисників і забезпечує більш глибокий аналіз слабких місць або недоліків, пов'язаних із безпекою та конфіденційністю. Тестування на проникнення особливо важливо, коли організації переходять від старих технологій до новіших (наприклад, переходять від мережевих протоколів IPv4 до IPv6). Організації можуть використовувати результати аналізу вразливостей для підтримки тестування на проникнення. Тестування на проникнення може проводитися всередині або ззовні на апаратних, програмних або мікропрограмних компонентах системи та може здійснювати як фізичний, так і технічний контроль. Стандартний метод тестування на проникнення включає попередній аналіз на основі повного знання системи, попереднє визначення потенційних уразливостей на основі попереднього аналізу та тестування, призначеного для визначення можливості використання цих вразливостей. Усі сторони погоджуються з правилами взаємодії перед початком сценаріїв тестування на проникнення. Правила взаємодії для тестів на проникнення схожі з інструментами, методами та процедурами, які, як очікується, використовуватимуть супротивники. Тестування на проникнення може призвести до розкриття інформації, яка захищена законами чи правилами, особам, які проводять тестування. Правила участі, контракти чи інші відповідні механізми можуть бути використані для захисту такої інформацію, а оцінка відповідних ризиків визначає рішення щодо рівня незалежності осіб, які проводять тестування на проникнення.

Пов'язані заходи: RA-5, RA-10, SA-11, SR-5, SR-6.

Посилення заходів:

(1) ТЕСТУВАННЯ НА ПРОНИКНЕННЯ - НЕЗАЛЕЖНА КОМАНДА АБО АГЕНТ НА ПРОНИКНЕННЯ

Залучити незалежного агента або команду для виконання тестування на проникнення системи або системного компонента.

Рекомендації з реалізації: Незалежні агенти або команди тестувальників на проникнення — це особи або групи осіб, які проводять неупереджене тестування на проникнення. Неупередженість передбачає, що ці тестувальники або групи тестувальників не мають будь-якого інтересу щодо розвитку, експлуатації чи управління системою, яка є ціллю тестування на проникнення. Захід безпеки

CA-2 (1) надає додаткову інформацію про незалежні оцінювання, які можна застосувати для тестування на проникнення.

Пов'язані заходи: CA-2.

(2) ТЕСТУВАННЯ НА ПРОНИКНЕННЯ - ЧЕРВОНА КОМАНДА

Використовувати наступні вправи червоної команди, для імітації спроб супротивників скомпрометувати системи організації відповідно до прийнятих правил ведення бойових дій: [*Завдання: визначені організацією вправи червоної команди*].

Рекомендації з реалізації: Червона команда здатна провести більш глибоке тестування на проникнення шляхом вивчення системи безпеки та приватності організації та її здатності застосовувати ефективні засоби захисту від кіберзагроз. Вправи червоної команди імітують спроби зловмисників скомпрометувати місію та бізнес-функції організації та забезпечують комплексну оцінку стану безпеки та приватності систем і організації. Змодельовані атаки також містять атаки на основі технологій і соціальної інженерії. Технологічні атаки включають взаємодію з апаратними, програмними чи апаратно-програмними компонентами та/або процесами. Атаки на основі соціальної інженерії включають взаємодію через електронну пошту, телефон або особисті розмови. Навчання червоної команди є найефективнішими, якщо їх проводять тестувальники на проникнення та команди, які мають знання та досвід поточної тактики, методів, процедур та інструментів боротьби. Хоча тестування на проникнення є в основному лабораторним тестуванням, організації можуть використовувати вправи червоної команди для забезпечення повноти оцінки, яка відображає реальні умови. Результати тестування на проникнення червоною командою можуть бути використані для підвищення рівня безпеки та обізнаності щодо приватності.

Пов'язані заходи: Немає.

(3) ТЕСТУВАННЯ НА ПРОНИКНЕННЯ - МОЖЛИВОСТІ ПЕРЕВІРКИ НА ПРОНИКНЕННЯ

Впровадити процес тестування на проникнення, який охоплює [*Призначення: визначену організацією частоту*] [*Вибір: з попередженням; без попередження*] спроб обійти чи зламати заходи захисту, пов'язані з фізичними точками доступу до об'єкта.

Рекомендації з реалізації: Тестування на проникнення фізичних точок доступу може надати інформацію про критичні вразливості в операційних середовищах систем організації. Така інформація може бути використана для виправлення слабких місць або недоліків у фізичних заходах захисту, необхідних для захисту систем організації.

Пов'язані заходи: CA-2, PE-3.

Посилання: Немає.

## CA-9 ВНУТРІШНІ З'ЄДНАННЯ СИСТЕМИ

Заходи захисту:

a. Авторизувати внутрішні підключення [*Призначення: системні компоненти або класи компонентів, що організація визначила*] до системи;

b. Задокументувати, для кожного внутрішнього з'єднання, характеристики інтерфейсу, вимоги безпеки та приватності, а також характер переданої інформації;

c. Розірвати внутрішні системні підключення після [*Призначення: умови, визначені організацією]*;

d. Переглядати [*Призначення: частота, визначена організацією*] постійну потребу в кожному внутрішньому з'єднанні.

Рекомендації з реалізації: Цей захід безпеки застосовується до зв'язків між організаційними системами та окремими складовими компонентами системи, включаючи компоненти, що використовуються для розробки системи. Ці внутрішньосистемні з'єднання містять, наприклад, з'єднання з мобільними пристроями, ноутбуками, настільними комп'ютерами, робочими станціями, принтерами, факсимільними машинами, сканерами, датчиками та серверами. Замість надання дозволу кожного окремого внутрішнього підключення до системи організації можуть дозволити внутрішні з'єднання для класу компонентів системи із загальними характеристиками та/або конфігураціями. Сюди можна віднести, наприклад, усі цифрові принтери, сканери та копіювальні машини із заданою можливістю обробки, передачі та зберігання або всі смартфони з певною базовою конфігурацією. Тривала потреба у підключенні до внутрішньої системи розглядається з точки зору того, чи забезпечує вона підтримку завдань організації або бізнес-функцій.

Пов'язані заходи: AC-3, AC-4, AC-18, AC-19, CM-2, IA-3, SC-7, SI-12.

Посилення заходів:

(1) ВНУТРІШНІ СИСТЕМНІ З'ЄДНАННЯ - ВІДПОВІДНІСТЬ ПЕРЕВІРКИ

Виконати перевірку безпеки та приватності компонентів складової системи до встановлення внутрішнього з'єднання.

Рекомендації з реалізації: Перевірки відповідності можуть містити, наприклад, перевірку відповідної базової конфігурації.

Пов'язані заходи: CM-6.

Посилання: [SP 800-124], [IR 8023].

## 10.5 Клас заходів захисту СМ — УПРАВЛІННЯ КОНФІГУРАЦІЄЮ

### СМ-1 ПОЛІТИКА ТА ПРОЦЕДУРИ УПРАВЛІННЯ КОНФІГУРАЦІЄЮ

Заходи захисту:

a. Розробити, задокументувати та поширити серед [Призначення: *визначених організацією персоналу або ролей*]:

1. [*Вибір (один або декілька): Рівень організації; Рівень місії/бізнес-процесу; рівень системи*] політики управління конфігурацією, яка:

(a) містить мету, сферу застосування, ролі, обов'язки, відповідальність керівництва, координацію між організаційними підрозділами та систему контролю відповідності (complaince);

(b) відповідає чинним законам, нормативним документам, наказам, положенням, політикам, стандартам і керівним принципам;

2. процедури, що сприяють реалізації політики управління конфігурацією та пов'язаних з нею заходів управління конфігурацією.

b. Призначити [*Призначення: посадова особа, визначена організацією*] для управління розробкою, документуванням і розповсюдженням політики та процедур керування конфігурацією.

c. Переглядати та оновлювати поточну політику управління конфігурацією:

1. Політика [*Призначення: частота, визначена організацією*] та наступні [*Призначення: події, визначені організацією*];

2. Процедури [*Призначення: частота, визначена організацією*] та наступні [*Призначення: події, визначені організацією*].

Рекомендації з реалізації: Цей захід захисту стосується встановлення політики та процедур для ефективного здійснення заходів і їх посилень у класі СМ. Стратегія управління ризиками є важливим фактором у встановленні політики та процедур. Комплексна політика та процедури допомагають забезпечити безпеку та приватність. За наявності політики, а також планів захисту інформації та персональних даних на рівні організації, конкретні системні політики та процедури можуть бути не потрібні. Політика може бути введена до складу загальної політики безпеки та приватності або може бути представлена кількома політиками (у випадках складної архітектури). Процедури описують, як має реалізуватися політика чи заходи захисту та як вони можуть бути спрямовані на персонал або роль, яка є об'єктом процедури. Процедури можуть бути задокументовані в планах захисту інформації та персональних даних (як один або декілька документів). Події, які можуть спричинити оновлення політики та процедур управління конфігурацією, включають: висновки оцінювання чи аудиту, інциденти чи порушення безпеки, зміни у відповідних законах, розпорядженнях, директивах, постановах, політиках, стандартах і вказівках, але не обмежуються ними. Просте повторне встановлення засобів контролю не є організаційною політикою чи процедурою.

Пов'язані заходи: PM-9, PS-8, SA-8, SI-12.

Посилення заходів: Немає.

Посилання: [OMB A-130], [SP 800-12], [SP 800-30], [SP 800-39], [SP 800-100].

## CM-2 БАЗОВА КОНФІГУРАЦІЯ

Заходи захисту:

a. Розробити, задокументувати та підтримувати за допомогою заходів конфігурації поточні базові налаштування системи.

b. Переглядати та оновлювати базові налаштування системи:

   1. з [*Призначення: визначеною організацією частотою*];

   2. за потреби внаслідок [*Призначення: визначених організацією обставин*];

   3. коли встановлені нові або оновлені компоненти системи.

Рекомендації з реалізації: Базові конфігурації для систем і компонентів системи включають підключення, експлуатацію та комунікаційні аспекти систем. Базові конфігурації — це задокументовані та узгоджені набори специфікацій для систем або елементів конфігурації в цих системах. Базові конфігурації служать основою для майбутніх збірок, випусків або змін у системах і включають впровадження контролю безпеки та приватності, операційні процедури, інформацію про компоненти системи, топологію мережі та логічне розміщення компонентів в архітектурі системи. Базові конфігурації систем мають відображати поточну архітектуру підприємства та (за потреби) можуть бути змінені з часом.

Пов'язані заходи: AC-19, AU-6, CA-9, CM-1, CM-3, CM-5, CM-6, CM-8, CM-9, CP-9, CP-10, CP-12, MA-2, PL-8, PM-5, SA-8, SA-10, SA-15, SC-18.

Посилення заходів:

(1) БАЗОВА КОНФІГУРАЦІЯ - ПЕРЕГЛЯД ТА ОНОВЛЕННЯ

[Вилучено: Включено до CM-2].

(2) БАЗОВА КОНФІГУРАЦІЯ - АВТОМАТИЗАЦІЯ ПІДТРИМКИ ЗАДЛЯ ТОЧНОСТІ ТА АКТУАЛЬНОСТІ

Підтримувати актуальність, повноту, точність і доступність базової конфігурації системи за допомогою [*Призначення: автоматизовані механізми, визначені організацією*].

Рекомендації з реалізації: Автоматизовані механізми, що допомагають організаціям підтримувати послідовну базову конфігурацію, можуть охоплювати: апаратні та програмні засоби інвентаризації, засоби управління конфігурацією та засоби управління мережею. Такі інструменти можуть бути використані як загальні елементи управління на системному рівні, або на рівні операційної системи чи компонентів (наприклад, на робочих станціях, серверах, ноутбуках, мережевих компонентах або мобільних пристроях). Інструменти можна використовувати для відстеження номерів версій в операційних системах, застосунках, типах встановленого програмного забезпечення тощо. Це посилення заходу може бути забезпечене вимогами заходу безпеки CM-8 (2) для

організацій, які поєднують інвентаризацію компонентів системи і базову конфігурацію.

Пов'язані заходи: CM-7, IA-3, RA-5.

(3) БАЗОВА КОНФІГУРАЦІЯ - ЗБЕРІГАННЯ ПОПЕРЕДНІХ ВЕРСІЙ КОНФІГУРАЦІЙ

Зберігати [*Призначення: кількість, визначена організацією*] попередніх версій базових конфігурацій системи для підтримки відкату.

Рекомендації з реалізації: Зберігання попередніх версій базових конфігурацій для підтримки відкату включає апаратне і програмне забезпечення, мікропрограми, файли конфігурації, записи конфігурації та відповідну документацію.

Пов'язані заходи: Немає.

(4) БАЗОВА КОНФІГУРАЦІЯ - НЕАВТОРИЗОВАНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

[Вилучено: Включено до CM-7(4)].

(5) БАЗОВА КОНФІГУРАЦІЯ - АВТОРИЗОВАНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

[Вилучено: Включено до CM-7(5)].

(6) БАЗОВА КОНФІГУРАЦІЯ - РОЗРОБКА ТА СЕРЕДОВИЩЕ ТЕСТУВАННЯ

Підтримувати базову конфігурацію для розробки системи та тестових середовищ, які керуються окремо від робочої базової конфігурації.

Рекомендації з реалізації: Створення окремих конфігурацій для розробки системи та тестування допомагають захистити системи від незапланованих/непередбачуваних подій, пов'язаних з розробкою та тестуванням. Окремі конфігурації дозволяють застосовувати управління конфігурацією, яке є найвідповіднішим для кожного типу. Наприклад, управління робочими конфігураціями зазвичай вимагає більшої стабільності, тоді як управління конфігураціями розробки або тестування вимагає більшої гнучкості. Конфігурації в тестовому середовищі відображають конфігурації в середовищі функціонування, наскільки це можливо, так щоб результати тестування відображали запропоновані зміни у операційних системах. Це посилення заходу вимагає створення окремих конфігурацій, але не обов'язково окремих фізичних середовищ.

Пов'язані заходи: CM-4, SC-3, SC-7.

(7) БАЗОВА КОНФІГУРАЦІЯ - КОНФІГУРАЦІЯ СИСТЕМ ТА КОМПОНЕНТІВ ДЛЯ СФЕР З ВИСОКИМ РИЗИКОМ

(a) Видавати [*Призначення: визначених організацією систем або компонентів систем*] з [*Призначенням: визначеними організацією конфігураціями*] особам, що перебувають у місцях, які організація вважає місцями зі значним ризиком;

(b) Застосувати [*Призначення: визначені організацією запобіжні заходи безпеки*] до компонентів, коли особи повертаються з поїздки.

Рекомендації з реалізації: Якщо відомо, що системи чи компоненти системи функціонуватимуть у зонах підвищеного ризику, додаткові заходи можуть бути впроваджені для протидії підвищеним загрозам. Наприклад, додаткові заходи можуть бути запроваджені для портативних комп'ютерів, якими користуються особи, що виїжджають і повертаються з відряджень. Спеціальні налаштування портативних комп'ютерів включають очищені жорсткі диски, обмеження програм та більш жорсткі параметри конфігурації. Засоби захисту, які застосовуються до мобільних пристроїв після повернення з відряджень, включають перевірку мобільного пристрою на наявність ознак фізичного втручання, очищення та повторного створення образів дисків. Захист інформації, яка зберігається на мобільних пристроях, розглядається у класі MP (Захист носіїв інформації).

Пов'язані заходи: MP-4, MP-5.

Посилання: [SP 800-124], [SP 800-128].

## CM-3 УПРАВЛІННЯ ЗМІНАМИ КОНФІГУРАЦІЇ

Заходи захисту:

a. Визначити типи змін у системі, які контролюються конфігурацією.

b. Переглядати запропоновані зміни в конфігурації, контрольовані системою, і схвалити або відхилити ці зміни з явним урахуванням аналізу наслідків безпеки.

c. Документувати рішення зі зміни конфігурації системи.

d. Впровадити схвалені зміни конфігурації в систему.

e. Зберігати записи змін конфігурації системі впродовж [*Призначення: певного періоду часу, визначеного організацією*].

f. Здійснювати моніторинг і аналіз дій, пов'язаних зі змінами конфігурації системи.

g. Координувати та впроваджувати нагляд за діяльністю з управління змінами конфігурації за допомогою [*Призначення: елементу управління змінами конфігурації, визначеного організацією*], який викликається [*Вибір (один або кілька): [Призначення: з визначеною організацією частотою*]; [*Призначення: визначені організацією умови зміни конфігурації*]].

Рекомендації з реалізації: Управління змінами конфігурації систем передбачає розробку, обґрунтування, реалізацію, тестування, перегляд і впровадження змін у системах, включно з оновленням і модифікацією системи. Управління змінами конфігурації охоплює зміни базових конфігурацій для компонентів і елементів систем; зміни в налаштуваннях конфігурації для продуктів; позапланові зміни; зміни, що необхідні для нівелювання нагальних загроз. Типові процеси управління змінами конфігурації в системах містять у собі плани керування конфігурацією або консультативні ради щодо змін, які переглядають і затверджують запропоновані зміни в системах. Аудит змін охоплює діяльність до та після внесення змін до систем і дії аудиту, що необхідні для впровадження таких змін (також див. SA-10).

Пов’язані заходи: CA-7, CM-2, CM-4, CM-5, CM-6, CM-9, CM-11, IA-3, MA-2, PE-16, PT-6, RA-8, SA-8, SA-10, SC-28, SC-34, SC-37, SI-2, SI-3, SI-4, SI-7, SI-10, SR-11.

Посилення заходів:

(1) УПРАВЛІННЯ ЗМІНАМИ КОНФІГУРАЦІЇ - АВТОМАТИЗОВАНЕ ДОКУМЕНТУВАННЯ, ПОВІДОМЛЕННЯ ТА ЗАБОРОНА ВНЕСЕННЯ ЗМІН

Впровадити автоматизовані механізми для:

(a) документування запропонованих змін у системі;

(b) повідомлення [*Призначення: визначених організацією органів влади, що проводять авторизацію*] про запропоновані зміни в системі та схвалення запитів змін;

(c) виділення запропонованих змін у системі, які не були схвалені або відхилені за [*Призначенням: визначений організацією період часу*];

(d) заборони внесення змін до системи, до отримання відповідного погодження;

(e) документування всіх змін у системі;

(f) повідомлення [*Призначення: визначеному організацією персоналу*], коли завершено погоджені зміни в системі.

Рекомендації з реалізації: Немає.

Пов’язані заходи: Немає.

(2) УПРАВЛІННЯ ЗМІНАМИ КОНФІГУРАЦІЇ - ТЕСТУВАННЯ, ВАЛІДАЦІЯ ТА ДОКУМЕНТУВАННЯ ЗМІН

Тестувати, перевіряти та документувати зміни в системі до повної їх реалізації.

Рекомендації з реалізації: Зміни в системах охоплюють модифікації апаратних, програмних засобів або компонентів мікропрограмного забезпечення та налаштування конфігурації, що визначені в CM-6. Тестування має бути організовано таким чином, щоб воно не порушувало роботу системи. Уповноважені особи або відповідальні підрозділи, які проводять тестування, мають розуміти політику й процедури безпеки та приватності, а також ризики для здоров’я, безпеки навколишнього середовища, що пов’язані з конкретними засобами чи процесами. Можуть бути ситуації, у яких перед початком процедури тестування операційна система має бути переведена в особливий «off-line» режим (тобто бути знятою з експлуатації). У таких випадках час проведення тестування має бути запланований заздалегідь. Якщо проведення тестування неможливе (наприклад, якщо неможливо припинення роботи системи), мають бути застосовані компенсаційні заходи захисту.

Пов’язані заходи: Немає.

(3) УПРАВЛІННЯ ЗМІНАМИ КОНФІГУРАЦІЇ - АВТОМАТИЗОВАНА РЕАЛІЗАЦІЯ ЗМІН

Внести зміни в поточний базову план системи та розгорнути оновлений базовий

план на встановленій базі за допомогою [*Призначення: автоматизовані механізми, визначені організацією*].

Рекомендації з реалізації: Автоматизовані інструменти можуть підвищити точність, узгодженість і доступність базової інформації про конфігурацію. Автоматизація також може забезпечити збирання та кореляцію даних, механізми оповіщення та інформаційні панелі для підтримки прийняття рішень на основі оцінки ризиків в організації.

Пов'язані заходи: Немає.

(4) УПРАВЛІННЯ ЗМІНАМИ КОНФІГУРАЦІЇ - ПРЕДСТАВНИК БЕЗПЕКИ

Вимагати від [*Призначення: визначеного організацією представника з інформаційної безпеки*] бути членом [*Призначення: визначеного організацією елементу керування зміною конфігурацій*].

Рекомендації з реалізації: До представників інформаційної безпеки належать посадові особи служби захисту інформації, офіцери системної та нформаційної безпеки та керівники організації. Такі посадові особи повинні відповідати високим вимогам щодо досвіду у сфері захисту інформації, оскільки зміни в конфігурації системи можуть мати непередбачувані побічні ефекти, які вимагатимуть негайних реакцій. Виявлення таких змін на ранній стадії процесу може допомогти уникнути ненавмисних негативних наслідків, які зрештою можуть вплинути на стан безпеки та приватності систем. Захід захисту для керування змінами конфігурації, згаданий у другому параметрі, відображає керування змінами, визначеними організаціями в CM-3g.

Пов'язані заходи: Немає.

(5) УПРАВЛІННЯ ЗМІНАМИ КОНФІГУРАЦІЇ - АВТОМАТИЧНЕ РЕАГУВАННЯ БЕЗПЕКИ

Реалізувати автоматичне [*Призначення: визначене організацією реагування безпеки*], якщо базова конфігурація системи змінюється несанкціонованим чином.

Рекомендації з реалізації: Можливі реакції безпеки можуть містити: зупинку роботи системи, зупинку вибраних функцій, надсилання сповіщень або повідомлень уповноваженим посадовим особам у разі, коли відбувається несанкціонована зміна елемента конфігурації.

Пов'язані заходи: Немає.

(6) УПРАВЛІННЯ ЗМІНАМИ КОНФІГУРАЦІЇ - УПРАВЛІННЯ ЗАСОБАМИ КРИПТОГРАФІЧНОГО ЗАХИСТУ

Забезпечити, щоб криптографічні механізми, які використовуються для забезпечення відповідних заходів захисту перебували під управлінням конфігурацією [*Призначення: визначених організацією заходів безпеки*].

Рекомендації з реалізації: Незалежно від криптографічних засобів, які використовуються, повинні бути забезпечені процеси й процедури для управління ними. Наприклад, якщо пристрої використовують сертифікати для ідентифікації та автентифікації, має бути реалізовано процес для регулювання

терміну дії цих сертифікатів.

Пов’язані заходи: SC-12.

Посилання: Немає.

(7) УПРАВЛІННЯ ЗМІНАМИ КОНФІГУРАЦІЇ - ПЕРЕГЛЯД ЗМІН У СИСТЕМІ

Перегляньте зміни в системі [*Призначення: частота, визначена організацією*] або коли [*Призначення: обставини, визначені організацією*], щоб визначити, чи відбулися неавторизовані зміни.

Рекомендації з реалізації: Ознаки, які вимагають перегляду змін у системі, і конкретні обставини, що виправдовують такі перегляди, можуть бути отримані в результаті діяльності, яку здійснюють організації під час процесу зміни конфігурації або процесу постійного моніторингу.

Пов’язані заходи: AU-6, AU-7, CM-3.

(8) УПРАВЛІННЯ ЗМІНАМИ КОНФІГУРАЦІЇ - ЗАПОБІГАННЯ ЧИ ОБМЕЖЕННЯ ЗМІН КОНФІГУРАЦІЇ

Запобігати або обмежити зміни конфігурації системи за таких обставин: [*Призначення: обставини, визначені організацією*].

Рекомендації з реалізації: Зміни конфігурації системи можуть негативно вплинути на важливі функції безпеки та конфіденційності системи. Обмеження на зміни можна застосовувати за допомогою автоматизованих механізмів.

Пов’язані заходи: Немає.

Посилання: [SP 800-124], [SP 800-128], [IR 8062].

## CM-4 АНАЛІЗ ВПЛИВУ НА БЕЗПЕКУ ТА ПРИВАТНІСТЬ

Заходи захисту:
Аналізувати зміни в системі, щоб визначити потенційну загрозу безпеці та приватності перед реалізацією змін.

Рекомендації з реалізації: Аналіз впливу має проводитися відповідальними за безпеку посадовими особами. Особи, які проводять такий аналіз, мають володіти необхідними навичками для проведення технічної експертизи для аналізу змін у системах та пов’язаних із цим наслідків щодо безпеки чи приватності. Аналіз впливу на безпеку та приватність охоплює: перегляд планів захисту, політик і процедур безпеки та приватності для розуміння вимог безпеки та приватності; перегляд проєктної документації системи для реалізації заходів, які можуть впливати на елементи управління; визначення того, яким чином можливі зміни в системі створюють нові ризики для приватності та здатність впроваджених засобів захисту для зменшення цих ризиків.

Пов’язані заходи: CA-7, CM-3, CM-8, CM-9, MA-2, RA-3, RA-5, RA-8, SA-5, SA-10, SI-2.

Посилення заходів:

(1) АНАЛІЗ ВПЛИВУ НА БЕЗПЕКУ ТА ПРИВАТНІСТЬ - ВІДОКРЕМЛЕНІ ВИПРОБУВАЛЬНІ СЕРЕДОВИЩА

Проаналізувати зміни в системі в окремому тестовому середовищі до впровадження змін в операційному середовищі, шукаючи вплив на безпеку та приватність через недоліки, слабкості, несумісність або навмисне спричинення шкоди.

Рекомендації з реалізації: Окреме випробувальне середовище в цьому контексті означає середовище, фізично або логічно ізольоване та відмінне від середовища функціонування системи. Розмежування має бути достатнім для того, щоб діяльність у випробувальному середовищі не впливала на діяльність у робочому середовищі, а інформація в робочому середовищі не передавалася до випробувального середовища. Відокремлення середовища можна досягти фізичними або логічними засобами. Якщо фізично окремі випробувальні середовища не можуть використовуватися, мають бути визначені механізми для здійснення логічного поділу.

Пов'язані заходи: SA-11, SC-7.

(2) АНАЛІЗ ВПЛИВУ НА БЕЗПЕКУ ТА ПРИВАТНІСТЬ - ВЕРИФІКАЦІЯ ФУНКЦІЙ БЕЗПЕКИ ТА ПРИВАТНОСТІ

Після змін у системі переконайтеся, що відповідні заходи захисту реалізовано правильно і вони функціонують належним чином та дають бажаний результат щодо дотримання вимог безпеки та приватності для системи.

Рекомендації з реалізації: Реалізація в цьому контексті стосується встановлення зміненого коду в операційній системі, що може вплинути на заходи безпеки або конфіденційності.

Пов'язані заходи: SA-11, SC-3, SI-6.

Посилання: [SP 800-128].

## CM-5 ОБМЕЖЕННЯ ДОСТУПУ ДО ЗМІНИ

Заходи захисту:
Визначити, задокументувати, затвердити та забезпечити застосування фізичних і логічних обмежень доступу, пов'язаних зі змінами в системі.

Рекомендації з реалізації: Будь-які зміни апаратних, та/або програмних компонентів систем можуть потенційно впливати на загальну безпеку систем. Тому лише кваліфіковані уповноважені особи можуть мати доступ до систем з метою ініціювання змін, включно з оновленням і модифікацією. Обмеження доступу до змін також стосується бібліотек програмного забезпечення. Обмеження доступу включають фізичний і логічний контроль доступу (див. AC-3 та PE-3), автоматизацію робочого процесу, абстрактні рівні (тобто зміни, впроваджені в зовнішні інтерфейси, а не безпосередньо в системі), а також тимчасові зміни (тобто зміни відбуваються лише протягом визначеного часу).

Пов’язані заходи: AC-3, AC-5, AC-6, CM-9, PE-3, SC-28, SC-34, SC-37, SI-2, SI-10.

Посилення заходів:

(1) ОБМЕЖЕННЯ ДОСТУПУ ДО ЗМІНИ - АУДИТ І ЗДІЙСНЕННЯ АВТОМАТИЧНОГО ДОСТУПУ

(a) Застосовувати обмеження доступу за допомогою [*Призначення: автоматизовані механізми, визначені організацією*];

(b) автоматично генерувати записи аудиту для виконаних дій.

Рекомендації з реалізації: Має бути проведена реєстрація записів доступу до системи, пов’язаних із застосуванням змін конфігурації, для забезпечення здійснення контролю змін конфігурації та підтримки фактичних дій у випадках, якщо виявлені будь-які несанкціоновані зміни.

Пов’язані заходи: AU-2, AU-6, AU-7, AU-12, CM-6, CM-11, SI-12.

(2) ОБМЕЖЕННЯ ДОСТУПУ ДО ЗМІНИ - ПЕРЕГЛЯД ЗМІН У СИСТЕМІ

[Вилучено: перенесено до CM-3(7)].

(3) ОБМЕЖЕННЯ ДОСТУПУ ДО ЗМІНИ - ПІДПИСАНІ КОМПОНЕНТИ

[Вилучено: перенесено до CM-14].

(4) ОБМЕЖЕННЯ ДОСТУПУ ДО ЗМІНИ - ПОДВІЙНА АВТОРИЗАЦІЯ

Здійснювати подвійну авторизацію для внесення змін до [*Призначення: компонентів системи та інформації на рівні системи, визначених організацією*].

Рекомендації з реалізації: Подвійна авторизація має здійснюватися для гарантування того, що будь-які зміни у вибраних компонентах не можуть відбутися, якщо двоє кваліфікованих осіб, які мають достатньо навичок і досвіду для визначення, чи запропоновані зміни є коректними, не затвердять їх.

Пов’язані заходи: AC-2, AC-5, CM-3.

(5) ОБМЕЖЕННЯ ДОСТУПУ ДО ЗМІНИ - ОБМЕЖЕННЯ ПОВНОВАЖЕНЬ ДЛЯ ВИРОБНИЦТВА ТА ЕКСПЛУАТАЦІЇ

(a) обмежити повноваження для зміни компонентів системи та інформації, пов’язаної із системою, у виробничому або операційному середовищі;

(b) переглядати та переоцінювати повноваження [*Призначення: визначеною організацією з частотою*].

Рекомендації з реалізації: У багатьох організаціях системи мають різні призначення, підтримують багато завдань, функцій і процесів. Обмеження привілеїв щодо зміни компонентів системи стосовно операційних систем необхідно, оскільки зміни в компоненті системи можуть мати вплив на функції та процеси. Складні відносини між системами та процесами в деяких випадках можуть бути невідомі розробникам.

Пов’язані заходи: AC-2.

(6) ОБМЕЖЕННЯ ДОСТУПУ ДО ЗМІНИ - ОБМЕЖЕННЯ ПОВНОВАЖЕНЬ ДЛЯ БІБЛІОТЕК

Обмежити повноваження для зміни програмного забезпечення, яке перебуває в бібліотеках програмного забезпечення.

Рекомендації з реалізації: Бібліотеки програмного забезпечення містять привілейовані програми.

Пов'язані заходи: AC-2.

(7) ОБМЕЖЕННЯ ДОСТУПУ ДО ЗМІНИ - АВТОМАТИЧНЕ ВПРОВАДЖЕННЯ ЗАХОДІВ ЗАХИСТУ

[Вилучено: включено до SI-7].

Посилання: FIPS Publications 140-2, 186-4

## CM-6 НАЛАШТУВАННЯ КОНФІГУРАЦІЇ

Заходи захисту:

a. Встановити та задокументувати параметри конфігурації компонентів, які застосовуються в системі, які відображають найбільш обмежений режим, що відповідає експлуатаційним вимогам, використовуючи [*Призначення: визначені організацією загальні безпечні конфігурації*].

b. Реалізувати конфігураційні установки.

c. Визначити, задокументувати та затвердити будь-які відхилення від встановлених конфігураційних параметрів конфігурації для [*Призначення: визначених організацією компонентів системи*] на основі [*Призначення: визначених організацією експлуатаційних вимог*].

d. Відстежувати та керувати змінами конфігураційних параметрів відповідно до організаційної політики та процедур.

Рекомендації з реалізації: Параметри конфігурації — це параметри, які можна змінити в апаратних та/або програмних компонентах системи та які впливають на захищеність або функціональність системи. Продукти інформаційних технологій, для яких мають бути визначені параметри конфігурації, пов'язані з безпекою, охоплюють персональні комп'ютери, сервери, робочі станції, пристрої вводу/виводу, мережеві пристрої, операційні системи та програми. Параметри безпеки — це ті параметри, які впливають на стан безпеки систем, включно з параметрами, необхідними для задоволення інших вимог заходів безпеки. Параметри безпеки містять параметри реєстру; налаштування дозволів акаунтів, файлу, каталогу; налаштування функцій, портів, протоколів та віддалених з'єднань. Організації встановлюють налаштування конфігурації для всієї організації і згодом отримують конкретні параметри конфігурації для систем. Встановлені параметри стають частиною базової конфігурації системи.
Загальні безпечні конфігурації (також їх називають контрольними списками конфігурації безпеки, керівництвом з техніки безпеки, посібниками з технічної реалізації безпеки) забезпечують визнані, стандартизовані та встановлені орієнтири, які передбачають безпечні налаштування конфігурації для конкретних платформ/продуктів інформаційних технологій та інструкції з налаштування. Загальні

безпечні конфігурації можуть бути розроблені різними організаціями, зокрема розробниками продуктів інформаційних технологій, виробниками, постачальниками, консорціумами, науковцями, представниками промисловості, зовнішніми агенціями та іншими організаціями в державному та приватному секторах.
Реалізація конкретної безпечної конфігурації може бути доручена на рівні організації чи на більш високому рівні із залученням регуляторного агентства. Загальні безпечні конфігурації містять базову конфігурацію, яка впливає на реалізацію CM-6 та інших заходів безпеки, таких як AC-19 та CM-7. Протокол автоматизації контенту безпеки (SCAP) та визначені стандарти в протоколі забезпечують ефективний метод унікальної ідентифікації, відстеження та керування налаштуваннями конфігурації.

Пов'язані заходи: AC-3, AC-19, AU-2, AU-6, CA-9, CM-2, CM-3, CM-5, CM-7, CM-11, CP-7, CP-9, CP-10, IA-3, IA-5, PL-8, PL-9, RA-5, SA-4, SA-5, SA-9, SC-18, SC-28, SC-43, SI-2, SI-4, SI-6.

Посилення заходів:

(1) НАЛАШТУВАННЯ КОНФІГУРАЦІЇ - АВТОМАТИЗОВАНЕ УПРАВЛІННЯ, ЗАСТОСУВАННЯ ТА ВЕРИФІКАЦІЯ

Керувати, застосовувати та перевіряти налаштування конфігурації для [*Призначення: системні компоненти, визначені організацією*] за допомогою [*Призначення: визначені організацією автоматизовані механізми*].

Рекомендації з реалізації: Автоматизовані інструменти (наприклад, інструменти підвищення безпеки, інструменти базової конфігурації) можуть підвищити точність, узгодженість і доступність інформації про налаштування конфігурації. Автоматизація також може забезпечити агрегацію та кореляцію даних, механізми попередження та інформаційні панелі для підтримки прийняття рішень на основі оцінки ризиків в організації.

Пов'язані заходи: CA-7.

(2) НАЛАШТУВАННЯ КОНФІГУРАЦІЇ - РЕАГУВАННЯ НА НЕСАНКЦІОНОВАНІ ЗМІНИ

Виконайте такі дії у відповідь на неавторизовані зміни в [*Призначення: параметри конфігурації, визначені організацією*]: [*Призначення: дії, визначені організацією*].

Рекомендації з реалізації: Реагування на несанкціоновані зміни в налаштуваннях конфігурації можуть охоплювати оповіщення персоналу, відновлення встановлених налаштувань конфігурації або, у крайньому разі, зупинку функціонування системи.

Пов'язані заходи: IR-4, IR-6, SI-7.

(3) НАЛАШТУВАННЯ КОНФІГУРАЦІЇ - ВИЯВЛЕННЯ НЕАВТОРИЗОВАНИХ ЗМІН

[Вилучено: Включено до SI-7]

(4) НАЛАШТУВАННЯ КОНФІГУРАЦІЇ - ДЕМОНСТРАЦІЯ ВІДПОВІДНОСТІ

[Вилучено: Включено до CM-4]

Посилання: [SP 800-70], [SP 800-126], [SP 800-128], [USGCB], [NCPR], [DOD STIG].

## CM-7 МІНІМАЛЬНО НЕОБХІДНА ФУНКЦІОНАЛЬНІСТЬ

Заходи захисту:

a. Налаштуйте систему для забезпечення лише [*Призначення: основні функції, визначені організацією для місії*];

b. Заборонити або обмежити використання таких функцій, портів, протоколів, програмного забезпечення та/або служб: [*Призначення: визначені організацією заборонені або обмежені функції, системні порти, протоколи, програмне забезпечення та/або служби*].

Рекомендації з реалізації: Системи можуть надавати широкий спектр функцій і послуг. Деякі функції та послуги, що зазвичай надаються за замовчуванням, можуть не знадобитися для підтримки основних місій організації, функцій або операцій. Крім того, іноді зручно надавати кілька послуг з одного компонента системи, але це збільшує ризик обмеження послуг, що надаються цим компонентом. Там, де це можливо, слід обмежувати функціональність однією функцією на компонент. Організації переглядають функції та послуги, що надаються системами або компонентами для визначення тих функцій і послуг, які не є першочерговими. Має розглядатися можливість відключення фізичних і логічних портів та протоколів, які є надлишковими або рідко використовуються для запобігання несанкціонованому підключенню пристроїв та передачі інформації. Для виявлення та запобігання використанню заборонених функцій, протоколів, портів і послуг можуть бути застосовані засоби мережевого сканування, системи виявлення та запобігання вторгненням і технології захисту кінцевих точок, такі як брандмауери та системи виявлення вторгнень.

Пов'язані заходи: AC-3, AC-4, CM-2, CM-5, CM-6, CM-11, RA-5, SA-4, SA-5, SA-8, SA-9, SA-15,SC-2, SC-7, SC-37. SI-4.

Посилення заходів:

(1) МІНІМАЛЬНО НЕОБХІДНА ФУНКЦІОНАЛЬНІСТЬ - ПЕРІОДИЧНИЙ ПЕРЕГЛЯД

(a) Проводити перегляд системи [*Призначення: з визначеною організацією частотою*] для виявлення непотрібних та/або незахищених функцій, портів, протоколів і послуг;

(b) Вимкнути [*Призначення: визначені організацією функції, порти, протоколи та послуги в системі, які вважаються непотрібними та/або незахищеними*].

Рекомендації з реалізації: Перевірка функцій, портів, протоколів та служб, які можна вимкнути. Такі перевірки особливо важливі здійснювати під час переходу від старих технологій до нових (наприклад, перехід від IPv4 до IPv6). Ці технологічні переходи можуть вимагати впровадження старих і нових технологій одночасно протягом перехідного періоду та повернення до мінімально необхідних функцій, портів, протоколів і послуг за першої нагоди. Оцінювання безпеки функції, порту, протоколу та/або послуги може бути

зроблене в порівнянні з іншими. Наприклад, протоколи Bluetooth, FTP та однорангові мережі є менш безпечними.

Пов'язані заходи: AC-18

(2) МІНІМАЛЬНО НЕОБХІДНА ФУНКЦІОНАЛЬНІСТЬ - ЗАБОРОНА ВИКОНАННЯ ПРОГРАМИ

Заборонити виконання програми відповідно до [*Вибір (один або кілька):* [*Призначення: визначеної організацією політики, правил поведінки та/або угод про доступ щодо використання програмного забезпечення та обмежень*]; *правил, що встановлюють терміни та умови використання програмного забезпечення*].

Рекомендації з реалізації: Це посилення заходу стосується організаційної політики, правил поведінки та/або угод про доступ, які обмежують використання програмного забезпечення, а також умов, встановлених розробником або виробником, включаючи ліцензування програмного забезпечення та авторські права. Обмеження охоплюють, наприклад, обмеження ролей, які можуть використовувати програми; заборону автоматичного виконання; запровадження чорного та білого списків або обмеження кількості екземплярів програми, які виконуються одночасно.

Пов'язані заходи: CM-8, PL-4, PL-9, PM-5, PS-6.

(3) МІНІМАЛЬНО НЕОБХІДНА ФУНКЦІОНАЛЬНІСТЬ - ВІДПОВІДНІСТЬ РЕЄСТРАЦІЇ

Забезпечити відповідність [*Призначення: визначеним організацією вимогам до реєстрації для функцій, портів, протоколів і послуг*].

Рекомендації з реалізації: Процес реєстрації необхідний для можливості управління, відстеження й контролю за системами, функціями, портами, протоколами та послугами.

Пов'язані заходи: Немає.

(4) МІНІМАЛЬНО НЕОБХІДНА ФУНКЦІОНАЛЬНІСТЬ - НЕАВТОРИЗОВАНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ — ЧОРНИЙ СПИСОК

(a) Визначити [*Призначення: визначені організацією програмне забезпечення, що не має дозволу виконуватися в системі*].

(b) Впровадити політику «дозволу всього, за винятком деяких» для заборони виконання неавторизованих програм у системі

(c) Переглядати та оновлювати список неавторизованих програм [*Призначення: з визначеною організацією частотою*].

Рекомендації з реалізації: Неавторизоване програмне забезпечення може бути обмежено певними версіями або з певного джерела. Концепція заборони виконання неавторизованого програмного забезпечення також може бути застосована до дій користувачів, портів і протоколів системи, IP-адрес/діапазонів, веб-сайтів і MAC-адрес.

Пов’язані заходи: CM-6, CM-8, CM-10, PL-9, PM-5.

(5) МІНІМАЛЬНО НЕОБХІДНА ФУНКЦІОНАЛЬНІСТЬ - АВТОРИЗОВАНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ — БІЛИЙ СПИСОК

(a) Визначити [*Призначення: визначені організацією програмне забезпечення, яке авторизовано виконується в системі*]

(b) Впровадити політику «заборони всього, за винятком деяких», щоб дозволити виконання авторизованих програм у системі.

(c) Переглядати та оновлювати список авторизованих програм [*Призначення: з визначеною організацією частотою*].

Рекомендації з реалізації: Процес, який використовується для визначення конкретних програм або цілих категорій програм, дозволених до виконання в системах організації, зазвичай називають білим списком. Для формування всебічного білого списку та підвищення рівня захисту від атак, програми можуть відстежуватися на різних рівнях деталізації. Можуть бути визначені наступні рівні деталізації програм: програми, інтерфейси програмування, модулі, застосунки, скрипти, системні процеси, системні послуги, дії ядра, регістри, драйвери та бібліотеки динамічних посилань. Концепція білого списку також може бути застосована до дій користувачів, портів, IP-адрес і адреси контролю доступу (MAC). Цілісність програм з білого списку може бути перевірена за допомогою криптографічних контрольних сум, цифрових підписів або геш-функцій. Перевірка програмного забезпечення може відбуватися як перед виконанням, так і при запуску системи. Ідентифікація авторизованих URL-адрес для вебсайтів розглядається в CA-3(5) і SC-7.

Пов’язані заходи: CM-2, CM-6, CM-8, CM-10, PL-9, PM-5, SA-10, SC-34, SI-7.

(6) МІНІМАЛЬНО НЕОБХІДНА ФУНКЦІОНАЛЬНІСТЬ - ЗАМКНУТІ СЕРЕДОВИЩА З ОБМЕЖЕНИМИ ПРИВІЛЕЯМИ

Вимагайте, щоб визначене програмне забезпечення, встановлене користувачем, виконувалося в обмеженому середовищі фізичної або віртуальної машини з обмеженими привілеями: [*Призначення: програмне забезпечення, встановлене користувачем, визначене організацією*]

Рекомендації з реалізації: Організації виявляють програмне забезпечення, яке має невідоме походження або потенційний вміст шкідливого коду. Для цього типу програмного забезпечення користувачі встановлюються в обмеженому робочому середовищі, щоб обмежити або стримати пошкодження від шкідливого коду, який може бути виконаний.

Пов’язані заходи: CM-11, SC-44.

(7) МІНІМАЛЬНО НЕОБХІДНА ФУНКЦІОНАЛЬНІСТЬ - ВИКОНУВАНИЙ КОД У ЗАХИЩЕНОМУ СЕРЕДОВИЩІ

Дозволити виконання двійкового або машинно-виконуваного коду лише в обмеженому фізичному або віртуальному машинному середовищі та за явного дозволу [*Призначення: персонал або ролі, визначені організацією*], якщо такий код:

a) Отримано з джерел з обмеженою гарантією або без неї; та/або
b) Без надання вихідного коду.

Рекомендації з реалізації: Виконання коду в захищених середовищах стосується всіх джерел двійкового або машинного виконуваного коду, включаючи комерційне програмне забезпечення та мікропрограми та програмне забезпечення з відкритим кодом.

Пов'язані заходи: CM-10, SC-44.

(8) МІНІМАЛЬНО НЕОБХІДНА ФУНКЦІОНАЛЬНІСТЬ - БІНАРНИЙ АБО МАШИННИЙ ВИКОНУВАНИЙ КОД

a) Заборонити використання двійкового або машинно-виконуваного коду з джерел з обмеженою гарантією або без неї або без надання вихідного коду; і
b) Дозволяти винятки лише для обов'язкових місій або оперативних вимог і за погодженням з уповноваженою посадовою особою.

Рекомендації з реалізації: Двійковий або машинний виконуваний код застосовується до всіх джерел двійкового або машинного виконуваного коду, включаючи комерційне програмне забезпечення, вбудоване програмне забезпечення та програмне забезпечення з відкритим кодом. Організації оцінюють програмні продукти без вихідного коду або з джерел з обмеженою гарантією, або без неї щодо потенційного впливу на безпеку. Оцінюється те, що програмні продукти без наданого вихідного коду складно перевірити, відлагодити або розширити. Крім того, може не бути власників, які б проводили таке відлагодження за дорученням організацій. Якщо використовується програмне забезпечення з відкритим вихідним кодом, оцінюється також те, що гарантія відсутня, а програмне забезпечення може містити бекдори або зловмисне програмне забезпечення, може не бути підтримки від виробника.

Пов'язані заходи: SA-5, SA-22.

(9) МІНІМАЛЬНО НЕОБХІДНА ФУНКЦІОНАЛЬНІСТЬ - ЗАБОРОНА ВИКОРИСТАННЯ НЕАВТОРИЗОВАНОГО ОБЛАДНАННЯ

a. Визначити [*Призначення: апаратні компоненти, визначені організацією, авторизовані для використання в системі*];
b. Заборонити використання або підключення неавторизованих апаратних компонентів;
c. Перегляд та оновлення списку авторизованих апаратних компонентів [*Призначення: частота, визначена організацією*].

Рекомендації з реалізації: Апаратні компоненти забезпечують основу для систем організації і платформу для виконання авторизованих програм. Управління інвентаризацією апаратних компонентів і контроль того, які апаратні компоненти дозволено встановлювати або підключати до систем організації, є важливими для забезпечення належної безпеки.

Пов'язані заходи: Немає.

Посилання: [FIPS 140-3], [FIPS 180-4], [FIPS 186-4], [FIPS 202], [SP 800-167].

## CM-8 ІНВЕНТАРИЗАЦІЯ КОМПОНЕНТІВ СИСТЕМИ

Заходи захисту:

a. Розробити та задокументувати процес інвентаризації компонентів системи, який:

   1. точно описує поточну систему;

   2. охоплює всі компоненти в межах акредитації системи;

   3. не включає повторний облік компонентів або компонентів, будь-якої іншої системи;

   4. визначає рівень деталізації, який є необхідним для відстеження та звітування;

   5. включає інформацію для досягнення підзвітності компонентів системи: [*Призначення: визначена організацією інформація, необхідна для досягнення ефективної підзвітності компонентів системи*].

b. Переглядати та оновлювати опис компонентів системи з [*Призначення: визначеною організацією частотою*].

Рекомендації з реалізації: Компоненти системи — це окремі елементи (продукти) інформаційних технологій, які являють собою блоки системи й містять апаратне, програмне забезпечення та віртуальні машини. Може бути ухвалено рішення щодо впровадження «централізованого» підходу, при якому система розглядається як єдиний блок, що містить усі організаційні компоненти. У таких ситуаціях організації мають забезпечити наявність всієї інформації, достатньої для належної реалізації та звітності всіх компонентів. Інформація, що необхідна для ефективної звітності компонентів системи, містить, наприклад: технічні характеристики; інформацію про ліцензії на програмне забезпечення; власників програмних компонентів; номери версій; а для мережевих компонентів або пристроїв — назви машин і мережеві адреси. Специфікація інвентаризації містить, наприклад: інформацію про виробника; тип пристрою; модель; серійний номер; фізичне розташування компоненту.
Запобігання повторному обліку компонентів системи усуває недолік, який виникає, коли власник компонента та зв'язок системи невідомі, особливо у великих або складних системах. Для ефективного запобігання повторного обліку компонентів системи необхідно використовувати унікальний ідентифікатор для кожного такого компонента. Для того, щоб здійснити інвентаризацію програмного забезпечення, централізовано кероване програмне забезпечення, доступ до якого здійснюється через інші системи, розглядається як компонент системи, у якій воно встановлено та в якій здійснюється його управління. Програмне забезпечення, встановлене в кількох системах, управління яким здійснюється на системному рівні, враховується для кожної окремої системи та може з'являтися в централізованому інвентаризаційному обліку більше одного разу, такий облік потребує системної прив'язки для кожного такого екземпляра програмного забезпечення в централізованому інвентаризаційному обліку. Системи сканування, які реалізують кілька мережевих протоколів (наприклад, IPv4 та IPv6), можуть призвести до виявлення повторюваних компонентів в різних адресних просторах. Впровадження CM-8(7) може допомогти усунути дублюючий облік компонентів.

Пов'язані заходи: CM-2, CM-7, CM-9, CM-10, CM-11, CM-13, CP-2, CP-9, MA-6,

PE-20, PM-5, SA-4, SA-5, SI-2, SR-4.

Посилення заходів:

(1) ІНВЕНТАРИЗАЦІЯ КОМПОНЕНТІВ СИСТЕМИ - ОНОВЛЕННЯ ПІД ЧАС ВСТАНОВЛЕННЯ ТА ВИДАЛЕННЯ

Оновлювати інвентарний опис компонентів системи як складової частини процесу інсталяції, видалення та оновлення компонентів системи.

Рекомендації з реалізації: Організації можуть підвищити точність, повноту та узгодженість інвентаризації компонентів системи, якщо централізований інвентаризаційний облік оновлюватимуть під час встановлення чи видалення компонентів ситеми або під час загальних оновлень системи. Якщо такий облік не оновлюється в ці ключові моменти, існує ймовірність того, що інформація не буде належним чином зібрана та задокументована. Оновлення системи включають апаратні, програмні та мікропрограмні компоненти.

Пов’язані заходи: PM-16.

(2) ІНВЕНТАРИЗАЦІЯ КОМПОНЕНТІВ СИСТЕМИ - АВТОМАТИЗОВАНА ПІДТРИМКА

Підтримувати актуальність, повноту, точність і доступність інвентаризації компонентів системи за допомогою [*Завдання: автоматизовані механізми, визначені організацією*].

Рекомендації з реалізації: Опис компонентів системи має бути вичерпним наскільки це можливо. Наприклад, віртуальні машини важко віслідковувати, оскільки їх не видно в мережі, коли вони не використовуються. У таких випадках організації мають вести максимально актуальний, повний і точний облік компонентів системи. Вимоги цього посилення заходу можуть бути реалізовані впровадженням CM-2 (2) для організацій, які вирішили поєднувати процедури інвентаризації компонентів системи та базову конфігурацію.

Пов’язані заходи: Немає.

(3) ІНВЕНТАРИЗАЦІЯ КОМПОНЕНТІВ СИСТЕМИ - АВТОМАТИЗОВАНЕ ВИЯВЛЕННЯ НЕАВТОРИЗОВАНИХ КОМПОНЕНТІВ

(a) Виявляти наявність несанкціонованого обладнання, програмного забезпечення та мікропрограмних компонентів у системі за допомогою [*Призначення: автоматизовані механізми, визначені організацією*] [*Призначення: частота, визначена організацією*];

(b) При виявленні неавторизованих компонентів виконувати такі дії: [*Вибір (один або кілька): відключення доступу до мережі такими компонентами; ізолювати компоненти; повідомити [Призначення: визначені організацією персонал або посади*]].

Рекомендації з реалізації: Це посилення заходу додатково застосовується до моніторингу несанкціонованих віддалених з’єднань і мобільних пристроїв. Моніторинг неавторизованих компонентів системи може здійснюватися на постійній основі чи періодично. Автоматизовані механізми можуть бути

реалізовані в системах або окремих пристроях. При придбанні та впровадженні автоматизованих механізмів організації розглядають, чи залежать такі механізми від здатності компонента системи підтримувати агента або запитувача, щоб бути виявленим, оскільки деякі типи компонентів не мають або не можуть підтримувати агентів (наприклад, пристрої IoT, датчики). Ізоляція може бути досягнута, наприклад, розміщенням неавторизованих компонентів в окремих доменах чи підмережах або способом переміщення на карантин таких компонентів. Такий тип ізоляції компонентів зазвичай називають «пісочницею».

Пов'язані заходи: AC-19, CA-7, RA-5, SC-3, SC-39, SC-44, SI-3, SI-4, SI-7.

(4) ІНВЕНТАРИЗАЦІЯ КОМПОНЕНТІВ СИСТЕМИ - ІНФОРМАЦІЯ ПРО ПІДЗВІТНІСТЬ

Увести в інвентаризаційну інформацію компоненту системи засіб для ідентифікації за [*Вибір (один або більше): ім'ям; позицією; роллю*] осіб, відповідальних і підзвітних за управління цими компонентами.

Рекомендації з реалізації: Ідентифікація осіб, які несуть відповідальність за адміністрування компонентів системи, допомагає забезпечити правильне управління призначеними компонентами, а також дозволяє організаціям зв'язатися з цими особами, якщо потрібні певні дії (наприклад, якщо компонент визначається як джерело порушення, або компонент потрібно відкликати, замінити або перенести).

Пов'язані заходи: AC-3.

(5) ІНВЕНТАРИЗАЦІЯ КОМПОНЕНТІВ СИСТЕМИ - ВИКЛЮЧЕННЯ ДУБЛЮВАННЯ КОМПОНЕНТІВ ОБЛІКУ

[Вилучено: перенесено до CM-8].

(6) ІНВЕНТАРИЗАЦІЯ КОМПОНЕНТІВ СИСТЕМИ - ПЕРЕВІРЕНІ НАЛАШТУВАННЯ ТА ЗАТВЕРДЖЕНІ ВІДХИЛЕННЯ

Включити перевірені налаштування компонентів і будь-які затверджені відхилення до поточних розгорнутих конфігурацій в інвентаризаційний облік компонентів системи.

Рекомендації з реалізації: Це посилення управління охоплює налаштування конфігурацій, встановлені організаціями, на конкретних компонентах, які були оцінені для визначення відповідності необхідним параметрам конфігурації; а також будь-які затверджені відхилення від встановлених параметрів конфігурації.

Пов'язані заходи: Немає.

(7) ІНВЕНТАРИЗАЦІЯ КОМПОНЕНТІВ СИСТЕМИ - ЦЕНТРАЛІЗОВАНЕ СХОВИЩЕ

Впровадити централізоване сховище для інвентаризаційного обліку компонентів системи.

Рекомендації з реалізації: Може бути ухвалено рішення щодо впровадження «централізованого» підходу, при якому система розглядається як єдиний блок,

що охоплює всі організаційні компоненти. Централізоване сховище для інвентаризаційного обліку компонентів системи надає можливості для ефективності обліку активів обладнання та програмного забезпечення. Таке сховище за потреби може також допомогти швидко визначити місцезнаходження компонентів системи та відповідальних осіб, які стали учасниками інциденту безпеки. У таких ситуаціях організації мають забезпечити наявність всієї інформації, достатньої для належної реалізації та звітності всіх компонентів.

Пов'язані заходи: Немає.

(8) ІНВЕНТАРИЗАЦІЯ КОМПОНЕНТІВ СИСТЕМИ - АВТОМАТИЗОВАНЕ ВІДСТЕЖЕННЯ МІСЦЯ РОЗТАШУВАННЯ

Відстежувати компоненти системи за географічним розташуванням за допомогою [*Призначення: автоматизовані механізми, визначені організацією*].

Рекомендації з реалізації: Використання автоматизованих механізмів для відстеження розташування компонентів системи може підвищити точність визначення місцезнаходження компонентів. Така спроможність може допомогти організаціям швидко визначити місцезнаходження компонентів системи та відповідальних осіб, які стали учасниками інциденту безпеки. Використання механізмів відстеження можна узгоджувати з консультантами з питань приватності, якщо є наслідки, які впливають на приватність особи.

Пов'язані заходи: Немає.

(9) ІНВЕНТАРИЗАЦІЯ КОМПОНЕНТІВ СИСТЕМИ - ПРИЗНАЧЕННЯ КОМПОНЕНТІВ СИСТЕМАМ

(a) Призначити визначені компоненти системі;

(b) Отримати підтвердження від [*Призначення: персонал або ролі, визначені організацією*] про виконання призначення.

Рекомендації з реалізації: Компоненти, які не призначені системі, можуть бути некерованими, не мати необхідного захисту та стати вразливістю для системи.

Пов'язані заходи: Немає.

Посилання: [OMB A-130], [SP 800-57-1], [SP 800-57-2], [SP 800-57-3], [SP 800-128], [IR 8011-2], [IR 8011-3].

## CM-9 ПЛАН УПРАВЛІННЯ КОНФІГУРАЦІЄЮ

Заходи захисту:
Розробити, задокументувати та реалізувати план управління конфігурацією системи, який:

a. описує ролі, відповідальність, процеси та процедури управління конфігурацією;

b. встановлює процес ідентифікації елементів конфігурації протягом всього життєвого циклу розробки системи та для управління конфігурацією елементів;

c. визначає елементи конфігурації для системи та розміщує елементи конфігурації під

управлінням конфігурації;

d. розглядає та затверджує [*Призначення: визначеним організацією персоналом або ролями*];

e. захищає план управління конфігурацією від несанкціонованого розкриття та модифікації.

Рекомендації з реалізації: План управління конфігурацією має відповідати вимогам політики керування конфігурацією, проте одночасно адаптуватися до конкретної системи. План управління конфігурацією визначає процеси та процедури, як управління конфігурацією використовується для підтримки життєвого циклу розвитку системи. План управління конфігурацією зазвичай розробляється на етапі розробки системи. У плані має бути описано, як оновлювати параметри конфігурації, як проводити інвентаризацію компонентів системи, як контролювати середовища розробки, тестування та експлуатації, а також, як розробляти, випускати та оновлювати ключові документи. Організації можуть використовувати шаблони для забезпечення послідовної та своєчасної розробки та реалізації планів управління конфігурацією. Такі шаблони можуть представляти головний план управління конфігурацією для організації з підмножинами планів, реалізованими в системі на конкретних компонентах. Процеси затвердження керування конфігураціями включають призначення ключових зацікавлених сторін, відповідальних за перегляд і затвердження запропонованих змін до систем, а також персоналу, який проводить аналіз впливу на безпеку та приватність перед впровадженням змін у системи. Елементи конфігурації — це компоненти системи (тобто апаратне, програмне забезпечення та документація), за допомогою яких відбувається управління конфігурацією. Протягом життєвого циклу системи нові елементи конфігурації можуть бути ідентифіковані, а деякі наявні елементи конфігурації можуть більше не потребувати управління.

Пов’язані заходи: CM-2, CM-3, CM-4, CM-5, CM-8, PL-2, RA-8, SA-10, SI-12.
Посилення заходів:

(1) ПЛАН УПРАВЛІННЯ КОНФІГУРАЦІЄЮ - ВСТАНОВЛЕННЯ ВІДПОВІДАЛЬНОСТІ

Встановити відповідальність за реалізацію процесу управління конфігурацією персоналу, який безпосередньо не бере участь у розробці системи.

Рекомендації з реалізації: За відсутності спеціалізованих команд управління конфігурацією, призначених в організації, до процесу управління конфігурацією можуть залучати персонал, який безпосередньо не бере участь у розробці або інтеграції системи. Такий розподіл обов’язків гарантує, що організація встановлює та підтримує достатній ступінь незалежності між процесами розробки й інтеграції системи та процесами управління конфігурацією для полегшення контролю якості та більш ефективного нагляду.

Пов’язані заходи: Немає.

Посилання: [SP 800-128].

**CM-10ОБМЕЖЕННЯ ВИКОРИСТАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ**

Заходи захисту:

a. Використовувати програмне забезпечення та супутні документи відповідно до договірних угод та законів про авторські права.

b. Відстежувати використання програмного забезпечення та пов'язаної документації, захищеної ліцензіями, для контролю копіювання та розповсюдження.

c. Контролювати та документувати використання технології однорангового обміну файлами, щоб гарантувати, що ця можливість не використовується для несанкціонованого розповсюдження, відображення, виконання або відтворення програмного забезпечення, захищеного авторським правом.

Рекомендації з реалізації: Відстеження ліцензій на програмне забезпечення може здійснюватися вручну або автоматизованими методами залежно від потреб організації. Прикладами угод є ліцензійні угоди на програмне забезпечення та угоди про нерозголошення.

Пов'язані заходи: AC-17, AU-6, CM-7, CM-8, PM-30, SC-7.
Посилення заходів:

(1) ОБМЕЖЕННЯ ВИКОРИСТАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ - ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ З ВІДКРИТИМ ВИХІДНИМ КОДОМ

Встановити такі обмеження на використання програмного забезпечення з відкритим вихідним кодом: [*Призначення: визначені організацією обмеження*].

Рекомендації з реалізації: Програмне забезпечення з відкритим кодом є доступним у формі вихідного коду. Певні права на програмне забезпечення, які зарезервовані для власників авторських прав, забезпечуються ліцензійними угодами (це дозволяє вивчати, змінювати та вдосконалювати програмне забезпечення). З погляду безпеки, головна перевага програмного забезпечення з відкритим кодом полягає в тому, що воно надає організаціям можливість досліджувати вихідний код. У деяких випадках існує онлайн-спільнота, пов'язана з програмним забезпеченням, яка постійно перевіряє, тестує, оновлює та звітує про проблеми, виявлені в програмному забезпеченні. Однак усунення вразливостей у програмному забезпеченні з відкритим кодом може бути проблематичним. Також, є питання щодо ліцензування програмного забезпеченням з відкритим кодом, включно з обмеженням щодо використання похідного програмного забезпечення. Крім того, програмне забезпечення з відкритим кодом, доступне лише у двійковій формі, може збільшити рівень ризику його икористання.

Пов'язані заходи: SI-7.

Посилання: Немає.

## CM-11ВСТАНОВЛЕНЕ КОРИСТУВАЧЕМ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

Заходи захисту:

a. Встановити [*Призначення: визначені організацією правила (політики)*], що регулюють встановлення програмного забезпечення користувачами.

b. Застосувати правила (політики) встановлення програмного забезпечення за допомогою таких методів: [*Призначення: визначені організацією методи*].

c. Відстежувати відповідність правилам (політики) з [*Призначення: визначеною організацією частотою*].

Рекомендації з реалізації: Користувачі, які мають відповідні привілеї, можуть встановлювати програмне забезпечення в системах організації. Для підтримки контролю над типами встановленого програмного забезпечення організації визначають дозволені та заборонені дії щодо встановлення програмного забезпечення. Дозволене програмне забезпечення може містити, наприклад, оновлення до наявного програмного забезпечення та завантаження програм із затверджених організацією «магазинів застосунків». До забороненого програмного забезпечення може належати, наприклад, програмне забезпечення з невідомим чи підозрілим походженням або програмне забезпечення, яке організації вважають потенційно шкідливим. Політики щодо встановленого користувачем програмного забезпечення можуть бути розроблені безпосередньо організацією або зовнішніми експертами. Методи застосування політики можуть включати організаційні та автоматизовані методи.

Пов'язані заходи: AC-3, AU-6, CM-2, CM-3, CM-5, CM-6, CM-7, CM-8, PL-4, SI-4, |SI-7.

Посилення заходів:

(1) ВСТАНОВЛЕНЕ КОРИСТУВАЧЕМ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ - ПОПЕРЕДЖЕННЯ ПРО НЕСАНКЦІОНОВАНУ ІНСТАЛЯЦІЮ

[Вилучено: Включено до CM-8(3)].

(2) ВСТАНОВЛЕНЕ КОРИСТУВАЧЕМ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ - ВСТАНОВЛЕННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ З ПРИВІЛЕЙОВАНИМ СТАТУСОМ

Дозволити користувачам встановлювати програмне забезпечення лише за наявності привілейованого статусу.

Рекомендації з реалізації: Привілейований статус може мати, наприклад, адміністратор системи.

Пов'язані заходи: AC-5, AC-6.

(3) ВСТАНОВЛЕНЕ КОРИСТУВАЧЕМ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ - АВТОМАТИЧНЕ ВИКОНАННЯ І МОНІТОРИНГ

Застосування та моніторинг відповідності політикам встановлення програмного забезпечення за допомогою [*Призначення: автоматизовані механізми, визначені організацією*]

Рекомендації з реалізації: Організації забезпечують дотримання та контролюють відповідність політикам встановлення програмного забезпечення за допомогою автоматизованих механізмів для більш швидкого виявлення та реагування на несанкціоноване встановлення програмного забезпечення, яке може бути показником внутрішньої чи зовнішньої ворожої атаки.

Пов’язані заходи: Немає.

Посилання: Немає.

## CM-12РОЗТАШУВАННЯ ІНФОРМАЦІЇ

Заходи захисту:

a. Визначити місце розташування [*Призначення: інформації, визначеної організацією*] та конкретних компонентів системи, на яких зберігається інформація.

b. Визначити та задокументувати користувачів, які мають доступ до системи та компонентів системи, де зберігається інформація.

c. Задокументувати зміни в розташуванні (наприклад, системи або компонентів системи), де перебуває інформація.

Рекомендації з реалізації: Цей захід захисту формулює необхідність розуміння того, де інформація обробляється та зберігається, і здебільшого застосовується до критичної інформації. Під розташуванням інформації розуміється місце, де конкретні типи інформації перебувають у компонентах системи, і порядок її обробки. Це потрібно для розуміння інформаційних потоків задля забезпечення належного захисту та управління політикою безпеки інформації та компонентів системи. Категорія безпеки інформації також є чинником при визначенні заходів захисту, необхідних для захисту відповідної інформації та системного компонента, де зберігається така інформація (див. FIPS 199). Розташування інформаційних і компонентів системи також є фактором, який впливає на архітектуру та проектування системи (див. SA-4, SA-8, SA-17)

Пов’язані заходи: AC-3, AC-4, AC-6, AC-23, CM-8, PM-5, RA-2, SC-4, SA-8, SA-17, SC-4, SC-16, SC-28, SI-4, SI-7.

Посилення заходів:

(1) РОЗТАШУВАННЯ ІНФОРМАЦІЇ - АВТОМАТИЗОВАНІ ІНСТРУМЕНТИ ПІДТРИМКИ РОЗТАШУВАННЯ ІНФОРМАЦІЇ

Використовувати автоматизовані інструменти для ідентифікації [*Призначення: визначеної організацією інформації за типом інформації*] на [*Призначення: визначених організацією компонентах системи*] для впровадження належних заходів захисту щодо інформації про організацію і персональних даних.

Рекомендації з реалізації: Використання автоматизованих інструментів допомагає підвищити ефективність реалізованої в системі можливості визначення місця розташування інформації. Автоматизація також допомагає керувати даними, отриманими під час діяльності з визначення інформації, і обмінюватися такою інформацією в межах організації. Вихідні дані автоматизованих інструментів визначення місцезнаходження інформації можуть бути використані для керівництва та інформування про архітектуру системи та проектні рішення.

Пов’язані заходи: Немає.

Посилання: FIPS Publication 199, [SP 800-60-1], [SP 800-60-2].

## CM-13ВІДОБРАЖЕННЯ ДІЙ ДАНИХ

Заходи захисту:

Розробіть і задокументуйте карту дій даних системи

Рекомендації з реалізації: Дії з даними – це системні операції, які обробляють особисту інформацію. Обробка такої інформації охоплює повний життєвий цикл інформації, який включає збір, генерацію, перетворення, використання, розкриття, збереження та видалення. Карта дій із даними системи включає окремі дії з даними, елементи персональної інформації, яка обробляється під час дій із даними, системні компоненти, залучені до дій із даними, і власників або операторів компонентів системи. Розуміння того, яка ідентифікаційна інформація обробляється (наприклад, конфіденційність ідентифікаційної інформації), як обробляється персональна інформація (наприклад, чи дані дані доступні людині чи обробляються в іншій частині системи), і ким (наприклад, особи можуть мати різні уявлення про конфіденційність залежно від суб'єкта, який обробляє особисту інформацію), надає низку контекстуальних факторів, важливих для оцінки ступеня ризику конфіденційності, створеного системою. Карти даних можна проілюструвати різними способами, а рівень деталізації може відрізнятися залежно від місії та бізнес-потреб організації. Карта даних може бути накладанням будь-якого артефакту проектування системи, який використовує організація. Розробка цієї карти може вимагати координації між програмами конфіденційності та безпеки щодо охоплених дій із даними та компонентів, визначених як частина системи.

Пов'язані заходи: AC-3, CM-4, CM-12, PM-5, PM-27, PT-2, PT-3, RA-3, RA-8.

## CM-14ПІДПИСАНІ КОМПОНЕНТИ

Заходи захисту: Запобігання інсталяції [*Призначення: програмне забезпечення та мікропрограмні компоненти, визначені організацією*] без перевірки того, що компонент має цифровий підпис за допомогою сертифіката, визнаного та схваленого організацією.

Рекомендації з реалізації: Компоненти програмного забезпечення та мікропрограми, заборонені для встановлення, якщо вони не підписані визнаними та схваленими сертифікатами, включають оновлення версій програмного забезпечення та мікропрограми, виправлення, пакети оновлень, драйвери пристроїв і базові оновлення системи введення/виведення. Організації можуть ідентифікувати застосоване програмне забезпечення та мікропрограмні компоненти за типом, конкретними елементами або комбінацією обох. Цифрові підписи та організаційна перевірка таких підписів є методом автентифікації коду.

Пов'язані заходи: CM-7, SC-12, SC-13, SI-7.

Посилання: [IR 8062].

## 10.6 Клас заходів захисту CP — ПЛАНУВАННЯ БЕЗПЕРЕРВНОЇ РОБОТИ

### CP-1 ПОЛІТИКА ТА ПРОЦЕДУРИ ПЛАНУВАННЯ БЕЗПЕРЕРВНОЇ РОБОТИ

Заходи захисту:

a. Розробити, задокументувати та поширити серед [*Призначення: визначених організацією персоналу або посад*]:

   1. [*Вибір (один або декілька): Рівень організації; Рівень місії/бізнес-процесу; рівень системи*] політику планування безперервної роботи на випадок надзвичайної ситуації, яка:

      (a) містить мету, сферу застосування, ролі, обов'язки, відповідальність керівництва, координацію між організаційними підрозділами та систему контролю відповідності (complaince);

      (b) відповідає чинним законам, виконавчим розпорядженням, директивам, положенням, політиці, стандартам і керівним принципам.

   2. процедури, що сприяють реалізації політики планування безперервної роботи та пов'язаних з ними заходів, на випадок надзвичайної ситуації.

b. Призначити [*Призначення: визначену організацією посадову особу вищого керівництва*] для управління, документування і розповсюдження політики та процедур планування безперервної роботи на випадок надзвичайних ситуацій.

c. Переглядати та оновлювати:

   1. поточну політику планування безперервної роботи з [*Призначення: визначеною організацією частотою*];

   2. поточні процедури планування безперервної роботи з [*Призначення: визначеною організацією частотою*].

d. Забезпечити, щоб процедури планування безперервної роботи реалізовували політику та заходи планування безперервної роботи.

e. Розробити, задокументувати та здійснити коригувальні заходи щодо виправлення становища в разі порушень політики планування безперервної роботи.

Рекомендації з реалізації: Цей захід захисту стосується встановлення політики та процедур для ефективного здійснення заходів та їх посилень у класі CP. Стратегія управління ризиками є важливим фактором у встановленні політики та процедур. Комплексна політика та процедури допомагають забезпечити безпеку та приватність. За наявності політики, а також планів захисту інформації та персональних даних на рівні організації, конкретні системні політики та процедури можуть бути не потрібні. Політика може бути внесена до складу загальної політики безпеки та приватності або може бути представлена кількома політиками (у випадках складної архітектури). Процедури описують, як має реалізуватися політика чи заходи захисту та як вони можуть бути спрямовані на персонал або роль, яка є об'єктом процедури. Процедури можуть бути задокументовані в планах захисту інформації та персональних даних (як

один або декілька документів). Події, які можуть спричинити оновлення політики та процедур планування безпеки на випадок надзвичайних ситуацій, включають: висновки аудиту, інциденти чи порушення безпеки, зміни в законах, розпорядженнях, директивах, постановах чи стандартах. Просте повторне встановлення засобів захисту не є організаційною політикою чи процедурою.

Пов'язані заходи: PM-9, PS-8, SI-12.
Посилення заходів: Немає.
Посилання: Немає.

## CP-2 ПЛАН ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ

Заходи захисту:

a. Розробити план забезпечення безперервної роботи та відновлення функціонування системи на випадок надзвичайної ситуації, який:

   1. визначає основні завдання, функції та пов'язані з ними вимоги щодо безперервної роботи;

   2. забезпечує цілі, пріоритети та відповідні показники відновлення функціонування;

   3. визначає ролі, обов'язки та відповідальних осіб з контактною інформацією;

   4. спрямований на підтримку основних завдань і функції, попри системні збої, компрометації або помилки;

   5. спрямований на повне відновлення функціонування системи без погіршення запланованих і реалізованих заходів захисту інформації та персональних даних;

   6. вирішує питання обміну інформацією про надзвичайні ситуації;

   7. переглядається та затверджується [*Призначення: персонал або ролі, визначені організацією*];

b. Поширити копії плану забезпечення безперервної роботи та відновлення функціонування серед [*Призначення: визначеного організацією ключового персоналу з непередбачених обставин (ідентифікується за ім'ям та/або за ролями) та елементів організації*].

c. Координувати діяльність з планування безперервної роботи із заходами по усуненню інцидентів.

d. Переглядати план забезпечення безперервної роботи та відновлення функціонування системи з [*Призначення: визначеною організацією частотою*].

e. Оновлювати план забезпечення безперервної роботи та відновлення функціонування з урахуванням змін в організації, системі або середовищі експлуатації, а також проблем, що виникають при реалізації, виконанні або тестуванні плану забезпечення безперервної роботи та відновлення функціонування.

f. Повідомляти про зміни в плані забезпечення безперервної роботи та відновлення функціонування [*Призначення: визначений організацією ключовий персонал з відновлення функціонування (ідентифікується за ім'ям та/або за ролями) та елементів організації*].

g. Включати уроки, отримані під час тестування плану забезпечення безперервної роботи та відновлення функціонування у навчання та тестування для випадків надзвичайних ситуацій.

h. Забезпечити захист плану забезпечення безперервної роботи та відновлення функціонування від несанкціонованого доступу або змін.

Рекомендації з реалізації: Планування системи забезпечення безперервної роботи та відновлення функціонування є частиною загальної організаційної програми для досягнення цілей місії. Планування системи забезпечення безперервної роботи та відновлення функціонування стосується відновлення системи та впровадження альтернативних процесів, коли системи скомпрометовані. Ефективність планування системи забезпечення безперервної роботи та відновлення функціонування досягається шляхом врахування такого планування протягом усього життєвого циклу системи. Планування системи забезпечення безперервної роботи та відновлення функціонування щодо розробки апаратного та програмного забезпечення може бути ефективним засобом досягнення стійкості системи. Планування системи забезпечення безперервної роботи та відновлення функціонування має відображати ступінь відновлення, необхідний для систем організації, оскільки не всі системи потребують повного відновлення для досягнення бажаного рівня безперервності операцій. Цілі відновлення системи мають відповідати чинному законодавству. Окрім доступності, забезпечення безперервної роботи та відновлення функціонування стосуються інших подій, пов'язаних з безпекою, які призводять до зниження ефективності роботи, наприклад, зловмисних атак, що загрожують приватності та цілісності системи. Дії, що мають розглядатися в планах, охоплюють, наприклад, впорядковану деградацію, вимкнення системи, відкат до ручного режиму, альтернативні інформаційні потоки та роботу в режимах, зарезервованих для того, коли системи піддаються атаці. Погоджуючи планування системи забезпечення безперервної роботи та відновлення функціонування з діяльністю з обробки інцидентів, організації можуть забезпечити проведення необхідних заходів з планування та активізацію в разі інциденту безпеки. Організації розглядають, чи конфліктує безперервність операцій під час інциденту з можливістю автоматичного вимкнення системи, як зазначено в IR-4(5). Планування реагування на інциденти є частиною планування на випадок непередбачених ситуацій для організацій і розглядається в сімействі IR (Incident Response).

Пов'язані заходи: CP-3, CP-4, CP-6, CP-7, CP-8, CP-9, CP-10, CP-11, CP-13, IR-4, IR-6, IR-8, IR-9, MA-6, MP-2, MP-4, MP-5, PL-2, PM-8, PM-11, SA-15, SA-20, SC-7, SC-23, SI-12.

Посилення заходів:

(1) ПЛАН ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ - КООРДИНАЦІЯ З ПОВ'ЯЗАНИМИ ПЛАНАМИ

Координувати розробку плану забезпечення безперервної роботи та відновлення функціонування зі структурними підрозділами, які відповідають за розробку та реалізацію пов'язаних планів.

Рекомендації з реалізації: Планування забезпечення безперервної роботи та відновлення функціонування містить: планування безперервності, планування відновлення після стихійних лих, планування безперервності операцій, планування відновлення критичної інфраструктури, планування реагування на кіберінциденти тощо.

Пов'язані заходи: Немає.

(2) ПЛАН ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ - ПЛАНУВАННЯ РЕСУРСІВ

Здійснити планування ресурсів з метою забезпечення необхідного потенціалу для обробки інформації, телекомунікацій та підтримки навколишнього середовища під час відновлення функціонування системи.

Рекомендації з реалізації: Планування ресурсів необхідне, оскільки різні види загроз можуть призвести до зменшення доступних послуг з обробки, призначених для підтримки завдань і функцій організації. Організація повинна передбачити операції, що деградують під час функціонування системи в позаштатному режимі. Необхідно врахувати, що заходи, пов'язані із захистом робочого середовища, повинні бути впроваджені при функціонуванні системи в позаштатному режимі. При плануванні ресурсів слід враховувати результати аналізу ризиків, категоризації системи (рівень впливу) та організаційній толерантності до ризику.

Пов'язані заходи: PE-11, PE-12, PE-13, PE-14, PE-18, SC-5.

(3) ПЛАН ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ - ВІДНОВЛЕННЯ КРИТИЧНИХ ФУНКЦІЙ

План відновлення [*Вибір: усі; істотні*] місія та бізнес-функції протягом [*Призначення: визначений організацією період часу*] активації плану на випадок надзвичайних ситуацій.

Рекомендації з реалізації: Організації можуть вирішити, чи проводити заходи з планування забезпечення безперервної роботи та відновлення функціонування як частину планування безперервності. Організації віддають пріоритет відновленню місії та основних функцій. Період часу для відновлення місії та основних функцій може залежати від серйозності та масштабу збоїв у системі та її допоміжній інфраструктурі.

Пов'язані заходи: Немає.

(4) ПЛАН ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ - ВІДНОВЛЕННЯ ВСІХ ФУНКЦІЙ

[Відкликано: включено до CP-2(3)].

(5) ПЛАН ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ - БЕЗПЕРЕРВНІСТЬ ВИКОНАННЯ КРИТИЧНИХ ФУНКЦІЙ

Планувати безперервність виконання критичних функцій [*Вибір: усі; основні*] з мінімальною втратою або без втрати безперервності роботи та підтримувати безперервну роботу до повного відновлення системи в місцях первинної

обробки та/або зберігання.

Рекомендації з реалізації: Організації можуть вирішити, чи проводити заходи з планування забезпечення безперервної роботи та відновлення функціювання як частину планування безперервності. Місця первинної обробки та/або зберігання, визначені організаціями як частина планування забезпечення безперервної роботи та відновлення функціонування, можуть змінюватися залежно від обставин, пов'язаних з надзвичайними ситуаціями.

Пов'язані заходи: Немає.

(6) ПЛАН ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ - МІСЦЯ АЛЬТЕРНАТИВНОЇ ОБРОБКИ ТА ЗБЕРІГАННЯ

Планувати перенесення виконання критичних функцій [*Вибір: усі; основні*] в альтернативні місця обробки та/або зберігання з мінімальною втратою або без втрати безперервності роботи та підтримувати безперервність роботи під час відновлення системи на первинних майданчиках обробки та/або зберігання.

Рекомендації з реалізації: Організації можуть вирішити, чи проводити заходи з планування забезпечення безперервної роботи та відновлення функціювання як частину планування безперервності для альтернативних місць обробки та зберігання. Місця первинної обробки та/або зберігання, визначені організаціями як частина планування забезпечення безперервної роботи та відновлення функціонування, можуть змінюватися залежно від обставин, пов'язаних з надзвичайними ситуаціями.

Пов'язані заходи: Немає.

(7) ПЛАН ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ - КООРДИНАЦІЯ З ПРОВАЙДЕРАМИ ЗОВНІШНІХ ПОСЛУГ

Узгодити план забезпечення безперервної роботи та відновлення функціонування з планами забезпечення безперервної роботи та відновлення функціювання зовнішніх постачальників послуг, з метою забезпечення виконання вимог на випадок надзвичайних ситуацій.

Рекомендації з реалізації: Коли здатність організації успішно виконувати свої основні завдання та функції залежить від зовнішніх постачальників послуг, розробка актуального та всебічного плану забезпечення безперервної роботи та відновлення функціонування може стати більш складним завданням. У цій ситуації організації координують діяльність з планування забезпечення безперервної роботи та відновлення функціонування із зовнішніми організаціями таким чином, щоб окремі плани відображали загальні потреби організації в позаштатних ситуаціях.

Пов'язані заходи: SA-9.

(8) ПЛАН ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ - ВИЗНАЧЕННЯ КРИТИЧНИХ АКТИВІВ

Визначити критичні активи системи, що підтримують критичні функції [*Вибір: усі; основні*].

Рекомендації з реалізації: Організації можуть вирішити, чи проводити заходи з планування забезпечення безперервної роботи та відновлення функціонування як частину аналізу критичної діяльності організації або планування безперервності (враховуючи результати аналізу впливу на організацію). Організації мають визначити критичні активи системи щодо яких потрібно застосовувати додаткові гарантії та контрзаходи (за винятком тих гарантій та контрзаходів, що виконуються звичайно) для забезпечення безперервного виконання завдань/функцій у позаштатних ситуаціях. Наявність переліку критично важливих інформаційних ресурсів також полегшує визначення пріоритетності ресурсів організації. Критичні активи системи охоплюють як технічні, так і операційні аспекти. До технічних аспектів належать: послуги інформаційних технологій, компоненти системи, продукти інформаційних технологій та механізми. До операційних аспектів належать: процедури (операції, що виконуються вручну) та персонал (особи, які забезпечують технічні гарантії та/або виконують ручні процедури). Плани захисту програм організації можуть допомогти у визначенні критичних активів. Якщо критичні активи є резидентами або підтримуються зовнішніми постачальниками послуг, організації розглядають впровадження CP-2(7) як покращення контролю.

Пов'язані заходи: CM-8, RA-9.

Посилання:

## CP-3 НАВЧАННЯ ІЗ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ

Заходи захисту:

a. Проведіть навчання користувачів системи на випадок надзвичайних ситуацій відповідно до призначених ролей і обов'язків:

   1. протягом [*Призначення: визначеного організацією періоду часу*] взяти на себе відповідну роль та відповідальність з відновлення функціонування;

   2. у разі внесення змін у систему;

   3. надалі з [*Призначення: визначеною організацією частотою*].

b. Переглядати та оновлювати зміст тренінгів на випадок надзвичайних ситуацій [*Призначення: частота, визначена організацією*] та дотримання [*Призначення: події, визначені організацією*].

Рекомендації з реалізації: Навчання із забезпечення безперервної роботи повинне бути пов'язане з обов'язками конкретних ролей та/або організаційного персоналу. Наприклад, звичайним користувачам можливо лише знати, коли й де потрібно звітувати про виконання службових обов'язків під час функціонування системи в позаштатному режимі. Для адміністраторів системи може знадобитися додаткове навчання щодо налаштування систем на місцях альтернативної обробки та зберігання інформації. Менеджери/старші керівники мають отримувати більш глибоку підготовку щодо того, як виконувати важливі функції у визначених місцях поза межами звичних компонентів та як встановити зв'язок з іншими установами з метою координації заходів, пов'язаних з надзвичайними ситуаціями.
Навчання ролям або обов'язкам на випадок надзвичайних ситуацій відображає конкретні вимоги в плані для відновлення безперервної роботи системи. Події, які

можуть спричинити оновлення вмісту навчання на випадок надзвичайних ситуацій, включають, але не обмежуються тестуванням плану на випадок надзвичайних ситуацій або фактичних надзвичайних випадків (засвоєних уроків), висновків з оцінювання чи аудиту, інцидентів чи порушень безпеки або змін в законах, розпорядженнях, директивах, правилах, політиках, стандартах, тощо. На розсуд організації, участь у випробуванні плану дій у надзвичайних ситуаціях або навчаннях, включаючи заняття з вивчення уроків після випробування чи вправ, може задовольнити вимоги до підготовки плану дій у надзвичайних ситуаціях.

Пов'язані заходи: AT-2, AT-3, AT-4, CP-2, CP-4, CP-8, IR-2, IR-4, IR-9.

Посилення заходів:

(1) НАВЧАННЯ ІЗ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ - ЗІМІТОВАНІ ПОДІЇ

Впровадити моделювання подій у навчанні, щоб забезпечити ефективне реагування персоналу на надзвичайні ситуації.

Рекомендації з реалізації: Використання змодельованих подій створює середовище, у якому персонал може відчувати реальні загрози, зокрема кібератаки, які відключають вебсайти, атаки програм-вимагачів, які шифрують організаційні дані на серверах, урагани, які пошкоджують або руйнують організаційні об'єкти, або апаратні чи програмні збої.

Пов'язані заходи: Немає.

(2) НАВЧАННЯ ІЗ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ - АВТОМАТИЗОВАНІ НАВЧАЛЬНІ СЕРЕДОВИЩА

Впровадити автоматизовані механізми, щоб забезпечити більш досконале та реалістичне середовище навчання.

Рекомендації з реалізації: Операційні механізми стосуються процесів, які були створені для досягнення організаційної мети або роботи системи, яка підтримує конкретну організаційну місію або бізнес-ціль. Фактична місія та бізнес-процеси, системи та/або засоби можуть бути використані для генерації змодельованих подій і підвищення реалістичності змодельованих подій під час навчання на випадок надзвичайних ситуацій.

Пов'язані заходи: Немає.

Посилання: [SP 800-50].

## CP-4 ТЕСТУВАННЯ ПЛАНУ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ

Заходи захисту:

a. Протестувати план забезпечення безперервної роботи та відновлення функціонування системи з [*Призначення: визначеною організацією частотою*], використовуючи [*Призначення: тести, що визначила організація*], з метою визначення ефективності плану та організаційної готовності виконати план.

b. Переглядати результати тестування плану.

c. За необхідності ініціювати коригувальні дії.

Рекомендації з реалізації: Методи тестування плану забезпечення безперервної роботи та відновлення функціонування для визначення ефективності планів та виявлення потенційних недоліків у них містять: анкетування, моделювання ситуацій та комплексні вправи. Організації проводять тестування на основі вимог безперервності в планах на випадок позаштатних ситуацій і охоплюють визначення впливу на організаційні операції, активи та осіб, що виникають внаслідок дій у позаштатних ситуаціях. Корегувальні дії мають бути гнучкими з погляду обсягів і строків.

Пов'язані заходи: AT-3, CP-2, CP-3, CP-8, CP-9, IR-3, IR-4, PL-2, PM-14, SR-2.

Посилення заходів:

(1) ТЕСТУВАННЯ ПЛАНУ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ - КООРДИНАЦІЯ З ПОВ'ЯЗАНИМИ ПЛАНАМИ

Координувати тестування плану забезпечення безперервної роботи та відновлення функціонування з організаційними підрозділами, що відповідають за реалізацію пов'язаних планів.

Рекомендації з реалізації: Плани, які пов'язані з планом забезпечення безперервної роботи та відновлення функціонування, містять, наприклад, плани безперервності, плани відновлення після аварій, плани безперервності операцій, плани критичної інфраструктури, плани реагування на кіберінциденти. Це посилення заходу не вимагає від організацій створювати організаційні елементи для обробки пов'язаних планів або узгоджувати такі елементи з конкретними планами. Однак це необхідно, якщо такі організаційні елементи відповідають за пов'язані плани. У такому разі організації повинні координувати ці елементи.

Пов'язані заходи: IR-8, PM-8.

(2) ТЕСТУВАННЯ ПЛАНУ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ - АЛЬТЕРНАТИВНА ПЛАТФОРМА ТЕСТУВАННЯ

Організація тестує план забезпечення безперервної роботи та відновлення функціонування на альтернативній платформі тестування:

(a) ознайомлює персонал з об'єктом та наявними ресурсами;

(b) оцінює можливості альтернативної платформи тестування для підтримки безперервної роботи.

Рекомендації з реалізації: Умови функціонування на альтернативній платформі можуть значно відрізнятися від умов на основній платформі. Можливість відвідати альтернативну платформу і відчути фактичні можливості, доступні на ній, може надати важливу інформацію про потенційні вразливості, які можуть вплинути на важливу місію організації та бізнес-функції, а також уточнити план забезпечення безперервної роботи та відновлення функціонування для усунення вразливостей, виявлених під час тестування.

Пов'язані заходи: CP-7.

(3) ТЕСТУВАННЯ ПЛАНУ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ - АВТОМАТИЧНЕ ТЕСТУВАННЯ

Перевіряйте план забезпечення безперервної роботи та відновлення функціонування за допомогою [*Призначення: автоматизовані механізми, визначені організацією*].

Рекомендації з реалізації: Автоматизовані механізми сприяють більш ретельному та ефективному тестуванню планів забезпечення безперервної роботи та відновлення функціонування. Це відбувається шляхом забезпечення більш повного висвітлення проблем у позаштатних ситуаціях; шляхом вибору більш реалістичних тестових сценаріїв і середовищ.

Пов'язані заходи: Немає.

(4) ТЕСТУВАННЯ ПЛАНУ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ - ПОВНЕ ВІДНОВЛЕННЯ

Ввести повне відновлення та повернення системи до відомого стану як частину тестування плану забезпечення безперервної роботи та відновлення функціонування.

Рекомендації з реалізації: Немає.

Пов'язані заходи: CP-10, SC-24.

(5) ТЕСТУВАННЯ ПЛАНУ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ - САМОВИКЛИК

Застосовуйте [*Призначення: визначені організацією механізми*] до [*Призначення: визначену організацією систему чи компонент системи*], щоб порушити роботу системи чи компонента системи та негативно вплинути на них.

Рекомендації з реалізації: Часто найкращим методом оцінки стійкості системи є порушення її роботи певним чином. Механізми, що використовуються організацією, можуть порушувати функції системи або системні служби багатьма способами, включаючи припинення або відключення критичних компонентів системи, зміну конфігурації компонентів системи, погіршення критичної функціональності (наприклад, обмеження пропускної здатності мережі) або зміну привілеїв. Автоматизовані, постійні та змодельовані кібератаки та збої в обслуговуванні можуть виявити несподівані функціональні залежності та допомогти організації визначити її здатність забезпечити стійкість перед обличчям фактичної кібератаки.

Пов'язані заходи: Немає.

Посилання: [FIPS 199], [SP 800-34], [SP 800-84], [SP 800-160-2].

## CP-5 ОНОВЛЕННЯ ПЛАНУ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ

[Вилучено: Включено до CP-2].

## CP-6 АЛЬТЕРНАТИВНЕ МІСЦЕ ЗБЕРІГАННЯ

Заходи захисту:

a. Створити альтернативне місце зберігання, включно з необхідними угодами, що дозволяють зберігати та видавати інформацію резервного копіювання системи.

b. Переконатися, що в альтернативному місці зберігання впроваджені заходи захисту, аналогічні заходам захисту основної локації.

Рекомендації з реалізації: Альтернативні місця зберігання — це місця, які географічно відокремлені від основних місць зберігання. Географічно розподілені архітектури, які підтримують вимоги щодо надзвичайних ситуацій, можуть вважатися альтернативними місцями зберігання. Пункти, на які поширюються угоди про альтернативні місця зберігання, включають екологічні умови в альтернативних місцях, правила доступу до систем і засобів, фізичні вимоги та вимоги щодо захисту навколишнього середовища, а також координацію доставки та отримання резервних носіїв. Альтернативні місця зберігання мають бути затверджені в планах забезпечення безперервної роботи та відновлення функціонування, щоб організації могли виконувати основні функції та завдання, незважаючи на збої в системах організації.

Пов’язані заходи: CP-2, CP-7, CP-8, CP-9, CP-10, MP-4, MP-5, PE-3, SC-36, SI-13.

Посилення заходів:

(1) АЛЬТЕРНАТИВНЕ МІСЦЕ ЗБЕРІГАННЯ - ВІДДІЛЕННЯ ВІД ПЕРВИННОГО СХОВИЩА

Визначити альтернативне місце зберігання, яке відокремлене від основного місця зберігання, щоб зменшити сприйнятливість до тих самих загроз.

Рекомендації з реалізації: Загрози, які впливають на альтернативні місця зберігання, мають бути визначені при проведенні оцінювання ризику (наприклад, стихійні лиха, структурні збої, атаки та помилки). За результатами оцінювання загроз організації визначають, що вважається достатнім ступенем поділу між основними та альтернативними місцями зберігання.

Пов’язані заходи: RA-3.

(2) АЛЬТЕРНАТИВНЕ МІСЦЕ ЗБЕРІГАННЯ - ЧАС ВІДНОВЛЕННЯ ТА ВСТАНОВЛЕННЯ ЦІЛЕЙ ВІДНОВЛЕННЯ

Налаштувати альтернативне місце зберігання для полегшення операцій відновлення відповідно до часу відновлення та встановлених цілей відновлення.

Рекомендації з реалізації: Немає.

Пов’язані заходи: Немає.

(3) АЛЬТЕРНАТИВНЕ МІСЦЕ ЗБЕРІГАННЯ - ДОСТУПНІСТЬ

Визначити потенційні проблеми доступності для альтернативного місця зберігання в разі збоїв або стихійних лих по всьому регіоні та в загальних рисах окреслити дії щодо пом’якшення наслідків.

Рекомендації з реалізації: Порушення в усіх регіонах стосуються тих типів перебоїв, які є широкими в географічному масштабі. Дії щодо пом'якшення наслідків охоплюють, наприклад, дублювання резервної інформації в інших альтернативних місцях зберігання, або забезпечення фізичного доступу для отримання резервної інформації, якщо електронний доступ до альтернативного місця зберігання порушений.

Пов'язані заходи: RA-3.

Посилання: [SP 800-34].

## CP-7 АЛЬТЕРНАТИВНИЙ МАЙДАНЧИК РОБОТИ

Заходи захисту:

a. Створити альтернативний майданчик для роботи, включно з необхідними угодами, які дозволяють передачу та відновлення [*Призначення: визначених організацією операцій системи*] для основних завдань і функцій у рамках [*Призначення: визначеного організацією періоду часу, відповідно термінам відновлення та встановленим цілям відновлення*], коли можливості основного майданчика недоступні.

b. Забезпечити на альтернативному майданчику доступними для роботи інформацію, обладнання та прилади, необхідні для передачі та відновлення роботи або укласти контракти протягом встановленого організацією періоду часу для передачі та відновлення роботи.

c. Впровадити на альтернативному майданчику роботи заходи захисту, еквівалентні тим, що впровадженні на основному майданчику.

Рекомендації з реалізації: Альтернативний майданчик роботи — це майданчик, який географічно відокремлений від основного майданчика роботи. Альтернативний майданчик роботи забезпечує можливість роботи, якщо основний майданчик роботи не доступний. Географічно розподілені будівлі також можуть розглядатися як альтернативні майданчики роботи. Альтернативні майданчики роботи мають бути затверджені в планах забезпечення безперервної роботи та відновлення функціонування, щоб організації могли виконувати основні функції та завдння, незважаючи на збої в системах. Можливість альтернативної обробки може бути реалізована за допомогою фізичного майданчика або за допомогою постачальника хмарних послуг або іншої внутрішньої чи зовнішньої служби обробки. Географічно розподілені архітектури, які підтримують вимоги на випадок непередбачених ситуацій, також можуть розглядатися як альтернативні майданчики обробки. Контроль, який охоплюється угодами про альтернативні майданчики обробки, включає умови навколишнього середовища на альтернативних майданчиках, правила доступу, фізичні вимоги та вимоги щодо захисту навколишнього середовища, а також координацію передачі та призначення персоналу.

Пов'язані заходи: CP-2, CP-6, CP-8, CP-9, CP-10, MA-6, PE-3, PE-11, PE-12, PE-17, SC-36, SI-13.

Посилення заходів:

(1) АЛЬТЕРНАТИВНИЙ МАЙДАНЧИК ДЛЯ РОБОТИ - ВІДДІЛЕННЯ ВІД ОСНОВНОГО МАЙДАНЧИКА

Визначити альтернативний майданчик для роботи, який відокремлений від основного майданчика, з метою зменшення вразливості до тих самих загроз.

Рекомендації з реалізації: Загрози, які впливають на альтернативні майданчики роботи, мають бути визначені при проведенні оцінювання ризику (наприклад, стихійні лиха, структурні збої, атаки та помилки). За результатами оцінювання загроз організації визначають, що вважається достатнім ступенем поділу між основними та альтернативними майданчиками роботи.

Пов'язані заходи: RA-3.

(2) АЛЬТЕРНАТИВНИЙ МАЙДАНЧИК ДЛЯ РОБОТИ - ДОСТУПНІСТЬ

Визначити потенційні проблеми доступності для альтернативного майданчика для роботи в разі збоїв або катастрофи по всьому регіону та окреслити чіткі заходи щодо пом'якшення наслідків.

Рекомендації з реалізації: Порушення в усіх регіонах стосуються тих типів перебоїв, які є суттєвими, незалежно від географічного розташування (такі висновки мають бути зроблені за результатами оцінювання ризиків).

Пов'язані заходи: RA-3.

(3) АЛЬТЕРНАТИВНИЙ МАЙДАНЧИК ДЛЯ РОБОТИ - ПРІОРИТЕТ ОБСЛУГОВУВАННЯ

Розробити угоди про альтернативний майданчик для роботи, які містять положення щодо пріоритету обслуговування відповідно до вимог стосовно організаційної доступності (включно з вимогами щодо часу відновлення).

Рекомендації з реалізації: Угоди з пріоритетним обслуговуванням — це угоди з постачальниками послуг, які забезпечують, щоб організації отримували пріоритетне обслуговування (відповідно до вимог щодо їх доступності та наявності інформаційних ресурсів) на альтернативному майданчику роботи.

Пов'язані заходи: Немає.

(4) АЛЬТЕРНАТИВНИЙ МАЙДАНЧИК ДЛЯ РОБОТИ - ПІДГОТОВКА ДЛЯ ВИКОРИСТАННЯ

Підготувати альтернативний майданчик для роботи таким чином, щоб майданчик був готовий до використання як оперативний майданчик, що підтримує виконання основних завдань і функцій.

Рекомендації з реалізації: Підготовка майданчика охоплює, наприклад, налаштування конфігурації для компонентів системи на альтернативному майданчику роботи (що відповідає вимогам щодо таких самих налаштувань на основному майданчику).

Пов'язані заходи: CM-2, CM-6, CP-4.

(5) АЛЬТЕРНАТИВНИЙ МАЙДАНЧИК ДЛЯ РОБОТИ - ЕКВІВАЛЕНТНІ ЗАХОДИ БЕЗПЕКИ ІНФОРМАЦІЇ

[Вилучено: Включено до CP-7].

(6) АЛЬТЕРНАТИВНИЙ МАЙДАНЧИК ДЛЯ РОБОТИ - НЕЗДАТНІСТЬ ПОВЕРНУТИСЯ НА ОСНОВНИЙ МАЙДАНЧИК

Розробити план та підготуватися до обставин, що виключають повернення на основний майданчик для роботи.

Рекомендації з реалізації: Можуть виникнути ситуації, які перешкоджають поверненню організації на основний майданчик обробки, наприклад, якщо стихійне лихо (наприклад, повінь або ураган) завдало шкоди або зруйнувло об'єкт, і було встановлено, що відновлення в тому ж місці є недоцільним.

Пов'язані заходи: Немає.

Посилання: [SP 800-34].

## CP-8 КОМУНІКАЦІЙНІ ПОСЛУГИ

Заходи захисту:
Впровадити альтернативні комунікаційні послуги, включно з необхідними угодами, що дозволять відновити [*Призначення: визначені організацією системні операції*] для основних завдань і функцій у [*Призначення: визначений організацією період часу*], коли основні можливості зв'язку недоступні на основному місці локації або розташовані на альтернативному майданчику для роботи чи зберігання.

Рекомендації з реалізації: Цей захід захисту застосовується до комунікаційних послуг (даних і голосових повідомлень) для основних та альтернативних майданчиків роботи та зберігання. Альтернативні комунікаційні послуги необхідні для забезпечення безперервності виконання функцій і завдань. До них належать, наприклад, додаткові організаційні або комерційні наземні чи супутникові лінії зв'язку. Під час укладення угод з надання альтернативних комунікаційних послуг організації враховують такі фактори, як доступність та якість обслуговування.

Пов'язані заходи: CP-2, CP-6, CP-7, CP-11, SC-7.

Посилення заходів:

(1) КОМУНІКАЦІЙНІ ПОСЛУГИ - ПРІОРИТЕТ ПОСТАЧАННЯ ПОСЛУГ

(a) Розробити основні та альтернативні угоди про надання комунікаційних послуг, які містять пріоритетні положення про надання послуг відповідно до вимог організаційної доступності (включно з вимогами щодо часу відновлення).

(b) Надсилати запит про пріоритети комунікаційних послуг для всіх комунікаційних послуг, що використовуються для забезпечення безперервності роботи, якщо основні та/або альтернативні комунікаційні послуги надаються загальним оператором.

Рекомендації з реалізації: Організації мають аналізувати потенційний вплив на діяльність у ситуаціях, якщо постачальники комунікаційних послуг обслуговують також інші організації, які мають право на пріоритетне обслуговування від постачальників. Пріоритет комунікаційних послуг (TSP) — це програма Федеральної комісії зі зв'язку (FCC), яка наказує постачальникам комунікаційних послуг (наприклад, компаніям дротового та бездротового

зв’язку) надавати пільговий режим користувачам, зареєстрованим у програмі, коли їм потрібно додати нові лінії або мати свої. FCC встановлює правила та політику для програми TSP, а Департамент внутрішньої безпеки керує програмою TSP. Програма TSP завжди діє і не залежить від великої катастрофи чи нападу. Для участі в програмі TSP потрібне федеральне спонсорство.

Пов’язані заходи: Немає.

(2) КОМУНІКАЦІЙНІ ПОСЛУГИ - ЄДИНІ ТОЧКИ ВІДМОВИ

Отримати альтернативні комунікаційні послуги з метою зменшення ймовірності спільного використання єдиної точки відмови з основними комунікаційними послугами.

Рекомендації з реалізації: За певних обставин постачальники комунікаційних послуг або послуги можуть використовувати ті самі фізичні лінії, що збільшує вразливість єдиної точки відмови. Важливо забезпечити прозорість постачальника щодо фактичної фізичної можливості передачі комунікаційних послуг.

Пов’язані заходи: Немає.

(3) КОМУНІКАЦІЙНІ ПОСЛУГИ - ВІДДІЛЕННЯ ОСНОВНИХ ТА АЛЬТЕРНАТИВНИХ ПРОВАЙДЕРІВ

Отримувати альтернативні комунікаційні послуги від постачальників, які відокремлені від основних постачальників послуг, щоб зменшити сприйнятливості до тих самих загроз.

Рекомендації з реалізації: До загроз, які впливають на комунікаційні послуги, належать: стихійні лиха, збої, кібератаки, фізичні атаки та помилки з бездіяльності. Такі загрози мають бути проаналізовані в ході проведення оцінювання ризиків. Загальна сприйнятливість може бути зменшена, наприклад, шляхом мінімізації спільної інфраструктури між провайдерами комунікаційних послуг або залученням географічно розподілених провайдерів. Організації можуть розглядати можливість використання одного постачальника послуг у ситуаціях, коли постачальник послуг може надавати альтернативні комунікаційні послуги, що відповідають вимогам розподілення, розглянутим при оцінюванні ризику.

Пов’язані заходи: Немає.

(4) КОМУНІКАЦІЙНІ ПОСЛУГИ - ПЛАН ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ПОСТАЧАЛЬНИКА КОМУНІКАЦІЙНИХ ПОСЛУГ

(a) вимагати, щоб постачальники основних та альтернативних комунікаційних послуг мали плани забезпечення безперервної роботи;

(b) переглядати плани забезпечення безперервної роботи постачальників комунікаційних послуг для забезпечення відповідності планам забезпечення безперервної роботи організації;

(c) отримати свідчення про тестування планів забезпечення безперервної роботи та навчання постачальників комунікаційних послуг [*Призначення: з визначеною організацією частотою*].

Рекомендації з реалізації: У ході перегляду планів забезпечення безперервної роботи постачальників комунікаційних послуг необхідно враховувати властивості таких планів (у деяких ситуаціях короткого огляду плану забезпечення безперервної роботи постачальників комунікаційних послуг може бути достатньо). Якщо постачальники комунікаційних послуг беруть участь у поточних навчаннях щодо забезпечення безперервної роботи в координації з державними та/або місцевими органами влади, то організації можуть зараховувати такі навчання як гарантії щодо надійності та кваліфікованості такого постачальника.

Пов'язані заходи: CP-3, CP-4.

(5) КОМУНІКАЦІЙНІ ПОСЛУГИ - ТЕСТУВАННЯ АЛЬТЕРНАТИВНИХ КОМУНІКАЦІЙНИХ ПОСЛУГ

Тестувати надання альтернативних комунікаційних послуг [*Призначення: з визначеною організацією частотою*].

Рекомендації з реалізації: Тестування альтернативних комунікаційних послуг організовується за договором з постачальниками послуг. Тестування може відбуватися паралельно зі звичайними операціями, для гарантування того, що немає погіршення задач чи функцій організації.

Пов'язані заходи: CP-3.

Посилання: [SP 800-34].

## CP-9 РЕЗЕРВНЕ КОПІЮВАННЯ

Заходи захисту:

a. Проводити резервне копіювання інформації користувачів, що міститься [*Призначення: системні компоненти, визначені організацією*] [*Призначення: з визначеною організацією частотою, відповідно до часу відновлення та встановлених цілей відновлення*].

b. Проводити резервне копіювання системної інформації на системному рівні, що міститься в системі [*Призначення: з визначеною організацією частотою, відповідно до завдань відновлення і встановлених цілей відновлення*].

c. Проводити резервне копіювання системної документації, включно з документацією, пов'язаною із забезпеченням безпеки та приватності [*Призначення: з визначеною організацією частотою, відповідно до часу відновлення та встановлених цілей відновлення*].

d. Забезпечити захист конфіденційності, цілісності та доступності резервних копій інформації в місцях їх зберігання.

Рекомендації з реалізації: Системна інформація охоплює: інформацію про стан системи, програмне забезпечення, операційну систему, прикладне програмне забезпечення, ліцензії тощо. Інформація користувачів охоплює будь-яку інформацію, крім системної інформації. Механізми, які можуть застосовуватися для захисту цілісності резервних копій, містять, наприклад, цифрові підписи та криптографічні геші. Захист резервної інформації під час транзиту забезпечується MP-5 і SC-8.

Положення щодо резервного копіювання відображаються в планах забезпечення безперервної роботи та відновлення функціонування, а також інші вимоги щодо резервного копіювання інформації. На організації можуть поширюватися закони, виконавчі накази, директиви, нормативні акти чи політики з вимогами щодо певних категорій інформації (наприклад, інформація про особисте здоров'я). Персонал організації консультується з представником з питань конфіденційності та юрисконсультантом щодо таких вимог.

Пов'язані заходи: CP-2, CP-6, CP-10, MP-4, MP-5, SC-8, SC-12, SC-13, SI-4, SI-13.

Посилення заходів:

(1) РЕЗЕРВНЕ КОПІЮВАННЯ - ВИПРОБУВАННЯ НА НАДІЙНІСТЬ ТА ЦІЛІСНІСТЬ

Тестувати носії резервних копій інформації [*Призначення: з визначеною організацією частотою*] для перевірки надійності носіїв та цілісності інформації.

Рекомендації з реалізації: Необхідно бути впевненим у тому, що інформацію з резервної копії можна отримати. Надійність стосується систем і компонентів системи, де зберігається резервна інформація, операцій, які використовуються для отримання інформації, і цілісності інформації, що вилучається. Для кожного з аспектів надійності можна використовувати незалежні та спеціалізовані тести. Наприклад, дешифрування та передача випадкової вибірки файлів резервних копій з альтернативного сховища або майданчика резервного копіювання та порівняння інформації з тією самою інформацією в первинному місці обробки може забезпечити таку гарантію.

Пов'язані заходи: CP-4.

(2) РЕЗЕРВНЕ КОПІЮВАННЯ - ТЕСТУВАННЯ ВІДНОВЛЕННЯ З ВИКОРИСТАННЯМ ЗРАЗКІВ

Використовувати зразок резервної копії інформації при відновленні вибраних функцій системи як частину тестування плану забезпечення безперервної роботи та відновлення функціонування.

Рекомендації з реалізації: Необхідна впевненість, що функції системи можна відновити належним чином і що вони зможуть підтримувати встановлені функції. Щоб переконатися, що вибрані функції системи ретельно відпрацьовуються під час тестування плану забезпечення безперервної роботи, витягується зразок резервної інформації, щоб визначити, чи функції працюють належним чином. Організації можуть визначати розмір вибірки для функцій і резервної інформації на основі необхідного рівня впевненості.

Пов'язані заходи: CP-4.

(3) РЕЗЕРВНЕ КОПІЮВАННЯ - ВІДОКРЕМЛЕНЕ СХОВИЩЕ КРИТИЧНОЇ ІНФОРМАЦІЇ

Зберігати резервні копії [*Призначення: визначеного організацією критичного системного програмного забезпечення та іншої інформації, пов'язаної з безпекою*] в окремому сховищі або у вогнестійкому контейнері, які не пов'язані

із системою.

Рекомендації з реалізації: Відокремлене зберігання критичної інформації стосується всієї важливої інформації, незалежно від типу носія для зберігання резервних копій. До критичного системного програмного забезпечення належать операційні системи, проміжне програмне забезпечення, системи керування криптографічними ключами та системи виявлення вторгнень. Інформація, пов'язана з безпекою, включає інвентаризацію системного обладнання, програмного забезпечення та мікропрограмних компонентів. Відокремлені сховища мають бути територіально розділеними з організаційними системами. Організації можуть забезпечте окреме зберігання шляхом впровадження автоматизованих процесів резервного копіювання в альтернативних місцях зберігання (наприклад, центри обробки даних). Адміністрація загального обслуговування (GSA) встановлює стандарти та специфікації для контейнерів із захищеністю та вогнестійкістю.

Пов'язані заходи: CM-2, CM-6, CM-8.

(4) РЕЗЕРВНЕ КОПІЮВАННЯ - ЗАХИСТ ВІД НЕАВТОРИЗОВАНИХ МОДИФІКАЦІЙ

[Вилучено: Включено до CP-9].

(5) РЕЗЕРВНЕ КОПІЮВАННЯ - ПЕРЕДАЧА НА АЛЬТЕРНАТИВНЕ СХОВИЩЕ ЗБЕРІГАННЯ

Перенести резервні копії інформації системи на альтернативне сховище [*Призначення: у визначений організацією період часу та швидкість передачі, відповідні часу відновлення та встановленим цілям відновлення*].

Рекомендації з реалізації: Резервні копії системи можуть бути передані на альтернативні сховища в електронному вигляді або на фізичному носії інформації.

Пов'язані заходи: CP-7, MP-3, MP-4, MP-5.

(6) РЕЗЕРВНЕ КОПІЮВАННЯ - НАДЛИШКОВА ВТОРИННА СИСТЕМА

Виконати резервне копіювання системи, підтримуючи надлишкову вторинну систему, яка не пов'язана з первинною системою та яку можна активувати без втрати інформації або порушення роботи.

Рекомендації з реалізації: Резервного копіювання системи можна досягти шляхом підтримки резервної вторинної системи, яка відображає первинну систему, включаючи реплікацію інформації. Якщо існує такий тип резервування та існує достатнє територіальне відокремлення між двома системами, вторинна система також може служити альтернативним місцем обробки.

Пов'язані заходи: CP-7.

(7) РЕЗЕРВНЕ КОПІЮВАННЯ - ПОДВІЙНА АВТОРИЗАЦІЯ

Використовувати подвійну авторизацію для видалення або знищення [*Призначення: визначених організацією резервних копій інформації*].

Рекомендації з реалізації: Подвійна авторизація забезпечує, щоб видалення резервних копій було можливе лише в тому разі, якщо двоє уповноважених осіб схвалили таке рішення (базуючись на тому, що воно відображає організаційну політику щодо резервного копіювання). Особи, які видаляють або знищують резервну копію інформації, володіють навичками або досвідом, щоб визначити, чи запропоноване видалення або знищення інформації відображає політику та процедури організації. Щоб зменшити ризик змови, організації розглядають можливість передачі подвійних повноважень різним особам.

Пов'язані заходи: AC-3, AC-5, MP-2.

(8) РЕЗЕРВНЕ КОПІЮВАННЯ - КРИПТОГРАФІЧНИЙ ЗАХИСТ

Впровадити криптографічні механізми для запобігання несанкціонованому розкриттю та змінам [*Призначення: визначених організацією резервних копій інформації*].

Рекомендації з реалізації: Вибір криптографічних механізмів ґрунтується на необхідності захисту конфіденційності та цілісності резервної інформації. Надійність механізму має відповідати категорії безпеки та/або класифікації інформації. Це посилення заходу застосовується до резервної інформації системи в основних та альтернативних сховищах. Якщо організація впровадила механізми криптографічного захисту, додатково мають бути забезпечені надійні механізми управління криптографічними ключами.

Пов'язані заходи: SC-12, SC-13, SC-28.

Посилання: FIPS Publications 140-2, 186-4, [SP 800-34], [SP 800-130], [SP 800-152].

## CP-10 ВІДНОВЛЕННЯ ТА ВІДТВОРЕННЯ СИСТЕМИ

Заходи захисту:

Забезпечити відновлення та відтворення системи до відомого стану після збою, компрометації або помилок у межах [*Призначення: визначеного організацією періоду часу, відповідного часу відновлення та встановлених цілей відновлення*].

Рекомендації з реалізації: Відновлення — це виконання плану дій щодо забезпечення безперервної роботи та відновлення функціонування систем. Відтворення відбувається після відновлення і містить заходи щодо повернення систем до повноцінного функціонування. Операції з відновлення та відтворення відображають пріоритети діяльності, час і цілі відновлення та відтворення показників, що відповідають вимогам плану забезпечення безперервної роботи та відновлення функціонування. Відтворення передбачає деактивацію будь-яких тимчасових можливостей системи, які, можливо, були необхідні для відновлення. Відтворення також охоплює оцінювання повністю відновлених можливостей системи, відновлення безперервної моніторингової діяльності та заходів з підготовки систем до подальших можливих збоїв, порушень або компрометації. Процедури відновлення та відтворення можуть містити як ручні, так і автоматизовані механізми. Організації встановлюють час відновлення та цілі відновлення як частини планування на випадок надзвичайних ситуацій.

Пов'язані заходи: CP-2, CP-4, CP-6, CP-7, CP-9, IR-4, SA-8, SC-24, SI-13.

Посилення заходів:

(1) ВІДНОВЛЕННЯ ТА ВІДТВОРЕННЯ СИСТЕМИ - ТЕСТУВАННЯ ПЛАНУ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОЇ РОБОТИ ТА ВІДНОВЛЕННЯ ФУНКЦІОНУВАННЯ

[Вилучено: Включено до CP-4].

(2) ВІДНОВЛЕННЯ ТА ВІДТВОРЕННЯ СИСТЕМИ - ВІДНОВЛЕННЯ ТРАНЗАКЦІЙ

Реалізувати відновлення транзакцій для систем, що базуються на транзакціях.

Рекомендації з реалізації: До систем, що базуються на транзакціях, належать системи управління базами даних і системи оброблення транзакцій. Механізми відновлення транзакцій можуть містити ведення журналу транзакцій з можливістю відкату.

Пов'язані заходи: Немає.

(3) ВІДНОВЛЕННЯ ТА ВІДТВОРЕННЯ СИСТЕМИ - КОМПЕНСАЦІЙНІ ЗАХОДИ ЗАХИСТУ

[Вилучено: Переадресовано через процедури адаптації].

(4) ВІДНОВЛЕННЯ ТА ВІДТВОРЕННЯ СИСТЕМИ - ВІДНОВЛЕННЯ В МЕЖАХ ЧАСОВОГО ПЕРІОДУ

Забезпечити можливість відновлення компонентів системи в межах [*Призначення: визначеного організацією періоду відновлення*] з інформації управління конфігурацією та захищеною цілісністю, яка описує відомий робочий стан компонентів.

Рекомендації з реалізації: Відновлення компонентів системи охоплює, наприклад, повернення компонентів до відомих, операційних станів.

Пов'язані заходи: CM-2, CM-6.

(5) ВІДНОВЛЕННЯ ТА ВІДТВОРЕННЯ СИСТЕМИ - ЗДАТНІСТЬ ВІДМОВОСТІЙКОСТІ

[Вилучено: Включено до SI-13].

(6) ВІДНОВЛЕННЯ ТА ВІДТВОРЕННЯ СИСТЕМИ - ЗАХИСТ КОМПОНЕНТУ

Забезпечити захист компонентів системи, які використовуються для резервного копіювання та відновлення.

Рекомендації з реалізації: Захист компонентів резервного копіювання та відновлення системи (апаратне та програмне забезпечення) передбачає використання як фізичних, так і технічних засобів. До програмного забезпечення для резервного копіювання та відновлення належать, наприклад, таблиці маршрутизаторів, компілятори й інше системне програмне забезпечення, що стосується безпеки.

Пов'язані заходи: AC-3, AC-6, MP-2, MP-4, PE-3, PE-6.

Посилання: [SP 800-34].

## CP-11 АЛЬТЕРНАТИВНІ ПРОТОКОЛИ ЗВ'ЯЗКУ

Заходи захисту:

Забезпечити можливість застосування [*Призначення: визначені організацією альтернативні протоколи зв'язку*] для підтримки збереження безперервності функціонування.

Рекомендації з реалізації: Плани забезпечення безперервної роботи та відновлення функціонування та навчання/тестування, що пов'язані з цими планами, мають забезпечувати можливість застосування альтернативного протоколу зв'язку як частину встановлення стійкості систем організації. Переключення протоколів зв'язку може впливати на програми та операційні аспекти систем. Організація має проводити оцінювання потенційних побічних ефектів впровадження таких альтернативних протоколів зв'язку.

Пов'язані заходи: CP-2, CP-8, CP-13.

Посилення заходів: Немає.

Посилання: Немає.

## CP-12 БЕЗПЕЧНИЙ РЕЖИМ

Заходи захисту:

Коли виявлено [*Призначення: визначені організацією умови*], організація вводить безпечний режим роботи з [*Призначення: визначеними організацією обмеженнями в безпечному режимі роботи*].

Рекомендації з реалізації: Для систем, що підтримують критичні функції та завдання (наприклад, військові операції та системи озброєння, цивільні космічні операції, операції на АЕС та операції з контролю повітряного простору), організації можуть визначити певні умови, за яких ці системи повертаються до попередньо визначеного безпечного режиму роботи. Безпечний режим роботи, який можна активувати автоматично або вручну, обмежує діяльність (тобто, системи можуть функціонувати лише при дотриманні цих умов). До таких обмежень можуть належати, наприклад, виконання лише певних функцій, які можна виконувати з обмеженою потужністю або зі зменшеною пропускною здатністю.

Пов'язані заходи: CM-2, SA-8, SC-24, SI-13, SI-17.

Посилення заходів: Немає.

Посилання: Немає.

## CP-13 АЛЬТЕРНАТИВНІ МЕХАНІЗМИ БЕЗПЕКИ

Заходи захисту:

Використовуйте [*Призначення: визначені організацією альтернативні або додаткові механізми безпеки*] для реалізації [*Призначення: визначених організацією функцій безпеки*], коли основні засоби реалізації функцій безпеки недоступні або скомпрометовані.

Рекомендації з реалізації: Для забезпечення цілей і завдань організації, а також

безперервності діяльності організації можуть впроваджуватися альтернативні або додаткові механізми безпеки. Ці механізми можуть бути менш ефективними, ніж основні механізми. Однак, маючи можливість легко використовувати ці альтернативні або додаткові механізми, організація підвищує гарантії безперервності. Зважаючи на вартість і рівень зусиль, необхідних для надання таких альтернативних механізмів безпеки, цей захід безпеки зазвичай застосовується лише в критичних системах чи компонентах системи. Наприклад, організація може видати одноразові блокноти старшому керівництву, посадовцям і системним адміністраторам, якщо зламано багатофакторні маркери — стандартний засіб для досягнення безпечної автентифікації.

Пов’язані заходи: CP-2 CP-11, SI-13.

Посилення заходів: Немає.

Посилання: Немає.

## 10.7 Клас заходів захисту ІА — ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ

### ІА-1 ПОЛІТИКА ТА ПРОЦЕДУРИ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ

Заходи захисту:

a. Розробити, задокументувати та поширити [*Призначення: серед визначеного організацією персоналу або посадових осіб*]:

   1. 1. [*Вибір (один або декілька): Рівень організації; Рівень місії/бізнес-процесу; рівень системи*] політики ідентифікації та автентифікації, яка:

      (a) містить мету, сферу застосування, ролі, обов'язки, відповідальність керівництва, координацію між організаційними підрозділами та систему контролю відповідності (complaince);

      (b) відповідає чинному законодавству, виконавчим розпорядженням, директивам, положенням, політиці, стандартам і керівним принципам;

   2. процедури, що спрямовані на реалізацію політики ідентифікації та автентифікації і пов'язаних з ними заходів ідентифікації та перевірки автентичності.

b. Призначити [*Призначення: визначену організацією посадову особу*] для управління політикою та процедурами ідентифікації та автентифікації.

c. Переглянути та оновити поточну політику ідентифікації та автентифікації:

   1. політика [*Призначення: з визначеною організацією частотою]* і наступні [*Призначення: події, визначені організацією*];

   2. процедури [*Призначення: з визначеною організацією частотою*] і наступні [*Призначення: події, визначені організацією*].

Рекомендації з реалізації: Цей захід захисту стосується встановлення політики та процедур для ефективного здійснення заходів та їх посилень у класі ІА. Стратегія управління ризиками є важливим фактором у встановленні політики та процедур. Комплексна політика та процедури допомагають забезпечити безпеку та приватність. За наявності політики, а також планів захисту інформації та персональних даних на рівні організації, конкретні системні політики та процедури можуть бути не потрібні. Політика може бути внесена до складу загальної політики безпеки та приватності або може бути представлена кількома політиками (у випадках складної архітектури). Процедури описують, як має реалізуватися політика чи заходи захисту, та можуть бути спрямовані на персонал або роль, яка є об'єктом процедури. Процедури можуть бути задокументовані в планах захисту інформації та персональних даних (як один або декілька документів). Події, які можуть спричинити оновлення політики та процедур ідентифікації та автентифікації, включають висновки оцінювання або аудиту, інциденти чи порушення безпеки або зміни у чинних законах, розпорядженнях, директивах, постановах, стандартах і вказівках. Просте повторне встановлення засобів захисту не є організаційною політикою чи процедурою.

Пов'язані заходи: AC-1, PM-9, PS-8, SI-12.

Посилення заходів: Немає.

Посилання: [OMB A-130], [FIPS 201-2], [SP 800-12], [SP 800-30], [SP 800-39], [SP 800-63-3], [SP 800-73-4], [SP 800-76-2], [SP 800-78-4], [SP 800-100], [IR 7874].

## IA-2 ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ)

Заходи захисту:
Унікально ідентифікувати та автентифікувати користувачів або процеси, що діють від імені користувачів.

Рекомендації з реалізації: Організації можуть задовольнити вимоги щодо ідентифікації та автентифікації, дотримуючись вимог [HSPD 12]. До користувачів організації належать працівники або особи, які за своїм статусом прирівнюються до них, включно з, наприклад, підрядниками та зовнішніми дослідниками. Цей захід безпеки застосовується до всіх доступів: тих, які явно визначені в AC-14 і які регулюються використанням групових автентифікаторів без індивідуальної автентифікації. Організації можуть вимагати унікальної ідентифікації осіб у групових облікових записах для детальної підзвітності індивідуальної діяльності. Для автентифікації можуть використовувати паролі, фізичні автентифікатори, біометричні дані або їх комбінацію (для організації багатофакторної автентифікації). Доступ до систем організації може бути локальним або мережевим. Локальний доступ — це будь-який доступ до систем організації, коли він здійснюється через прямі з'єднання без використання мереж. Мережевий доступ — це доступ до систем організації з використанням мережевих з'єднань. Віддалений доступ — це тип мережевого доступу, який передбачає використання зовнішніх мереж. До внутрішніх мереж належать локальні мережі. Використання зашифрованих віртуальних приватних мереж для мережевих з'єднань між контрольованими організацією кінцевими точками та неорганізованими кінцевими точками може трактуватися як внутрішні мережі. Вимоги до ідентифікації та автентифікації для користувачів, які не належать до організації, описані в IA-8.

Пов'язані заходи: AC-2, AC-3, AC-4, AC-14, AC-17, AC-18, AU-1, AU-6, IA-4, IA-5, IA-8, MA-4, MA-5, PE-2, PL-4, SA-4, SA-8.

Посилення заходів:

(1) ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ) - БАГАТОФАКТОРНА АВТЕНТИФІКАЦІЯ ПРИВІЛЕЙОВАНИХ ОБЛІКОВИХ ЗАПИСІВ

Реалізувати багатофакторну автентифікацію для доступу до привілейованих облікових записів.

Рекомендації з реалізації: Багатофакторна автентифікація передбачає використання двох або більше різних факторів для успішного проходження процедури автентифікації. Фактори визначаються на декількох рівнях: щось, що відомо користувачу (наприклад, пароль або особистий ідентифікаційний номер (PIN)); щось, що є в користувача (наприклад, фізичний автентифікатор); щось, чим володіє користувач (наприклад, біометричні дані). До фізичних автентифікаторів належать, наприклад, апаратні автентифікатори, смарткарти, затвердженні чинним законодавством електронні посвідчення особистості (електронні паспорти). Крім автентифікації користувачів на системному рівні

(тобто при вході), організації можуть також використовувати механізми автентифікації на рівні застосунків для забезпечення підвищеної безпеки. Незалежно від типу доступу (локального, мережевого або віддаленого) привілейовані облікові записи мають завжди проходити процедуру багатофакторної автентифікації. Організації можуть вживати додаткові заходи безпеки (наприклад, більш жорсткі механізми автентифікації) для конкретних типів доступу.

Пов'язані заходи: AC-5, AC-6.

(2) ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ) - БАГАТОФАКТОРНА АВТЕНТИФІКАЦІЯ НЕПРИВІЛЕЙОВАНИХ ОБЛІКОВИХ ЗАПИСІВ

Реалізувати багатофакторну автентифікацію для доступу до непривілейованих облікових записів.

Рекомендації з реалізації: Багатофакторна автентифікація передбачає використання двох або більше різних факторів для успішного проходження процедури автентифікації. Фактори визначаються на декількох рівнях: щось, що відомо користувачу (наприклад, пароль або особистий ідентифікаційний номер (PIN)); щось, що є в користувача (наприклад, фізичний автентифікатор); щось, чим володіє користувач (наприклад, біометричні дані). До фізичних автентифікаторів належать, наприклад, апаратні автентифікатори, смарткарти, затвердженні чинним законодавством електроні посвідчення особистості (електронні паспорти). Крім автентифікації користувачів на системному рівні (тобто при вході), організації можуть також використовувати механізми автентифікації на рівні застосунків для забезпечення підвищеної безпеки. Незалежно від типу доступу (локального, мережевого або віддаленого) привілейовані облікові записи мають завжди проходити процедуру багатофакторної автентифікації. Організації можуть вживати додаткові заходи безпеки (наприклад, більш жорсткі механізми автентифікації) для конкретних типів доступу.

Пов'язані заходи: AC-5.

(3) ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ) - ЛОКАЛЬНИЙ ДОСТУП ДО ПРИВІЛЕЙОВАНИХ ОБЛІКОВИХ ЗАПИСІВ

[Вилучено: Включено до IA-2(1)].

(4) ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ) - ЛОКАЛЬНИЙ ДОСТУП ДО НЕПРИВІЛЕЙОВАНИХ ОБЛІКОВИХ ЗАПИСІВ

[Вилучено: Включено до IA-2(2)].

(5) ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ) - ІНДИВІДУАЛЬНА АВТЕНТИФІКАЦІЯ З ГРУПОВОЮ АВТЕНТИФІКАЦІЄЮ

Якщо використовуються спільні облікові записи або автентифікатори, вимагайте від користувачів індивідуальної автентифікації перед наданням доступу до спільних облікових записів або ресурсів.

Рекомендації з реалізації: Проходження процедури індивідуальної

автентифікації перед процедурою автентифікації групи допомагає зменшити ризики, які пов'язані з використанням спільних облікових записів або автентифікаторів.

Пов'язані заходи: Немає.

(6) ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ) - МЕРЕЖЕВИЙ ДОСТУП ДО ПРИВІЛЕЙОВАНИХ ОБЛІКОВИХ ЗАПИСІВ — ОКРЕМИЙ ПРИСТРІЙ

Реалізація багатофакторної автентифікації для [*Вибір (один або кілька): локальний; мережевий; віддалений*] доступ до [*Вибір (один або кілька): привілейовані облікові записи; непривілейовані облікові записи*] такі, що:

a) Один із факторів забезпечується пристроєм, окремим від системи, який отримує доступ;

b) Пристрій відповідає [*Призначення: визначені організацією вимоги до міцності механізму*].

Рекомендації з реалізації: Метою багатофакторної автентифікації для окремого пристрою, який використовує користувач, є зменшення ймовірності компрометації автентифікаторів або облікових даних, що зберігаються в системі. Зловмисники можуть отримати доступ до таких автентифікаторів або облікових даних і згодом видати себе за авторизованих користувачів. Реалізація одного з факторів на окремому пристрої (наприклад, апаратний токен) забезпечує більшу міцність механізму та підвищений рівень надійності в процесі автентифікації.

Пов'язані заходи: AC-6.

(7) ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ) - МЕРЕЖЕВИЙ ДОСТУП ДО НЕПРИВІЛЕЙОВАНИХ ОБЛІКОВИХ ЗАПИСІВ — ОКРЕМИЙ ПРИСТРІЙ

[Вилучено: Включено до IA-2(6)].

(8) ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ) - ДОСТУП ДО ОБЛІКОВИХ ЗАПИСІВ — СТІЙКІСТЬ ДО ВІДТВОРЕННЯ

Реалізувати стійкі до відтворення механізми автентифікації для доступу до [*Вибір (один або кілька): привілейованих облікових записів; непривілейованих облікових записів*]

Рекомендації з реалізації: Процеси автентифікації мають бути стійким до атак відтворення. Для забезпечення таких властивостей механізми автентифікації можуть використовувати, наприклад, протоколи з одноразовими автентифікаторами синхронними за часом чи криптографічні автентифікатори.

Пов'язані заходи: Немає.

(9) ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ) - ДОСТУП ДО НЕПРИВІЛЕЙОВАНИХ ОБЛІКОВИХ ЗАПИСІВ — СТІЙКІСТЬ ДО ВІДТВОРЕННЯ

[Вилучено: Включено до IA-2(8)].

(10) ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ) - ЄДИНА ТОЧКА ВХОДУ

Впровадити можливість єдиного входу для [*Призначення: облікових записів і послуг системи, визначених організацією*].

Рекомендації з реалізації: Система єдиного входу дозволяє користувачам входити один раз і отримувати доступ до кількох ресурсів системи. Організації мають аналізувати ефективність єдиного входу, беручи до уваги ризики, які пов'язані з відсутністю повторної автентифікації при зверненні до іншого ресурсу. Система єдиного входу може сприяти підвищенню рівня безпеки системи у випадках, коли завдяки її використанню можливо забезпечити процедуру багатофакторної автентифікації при доступі до компонентів, власні можливості яких не дозволяють реалізувати такі механізми автентифікації (наприклад, це може стосуватися застарілих програмних компонентів).

Пов'язані заходи: Немає.

(11) ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ) - ВІДДАЛЕНИЙ ДОСТУП — ОКРЕМИЙ ПРИСТРІЙ

[Вилучено: Включено до IA-2(6)].

(12) ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ) - ПРИЙНЯТТЯ ПОВНОВАЖЕНЬ ДЛЯ ВЕРИФІКАЦІЇ ОСОБИСТОЇ ІНФОРМАЦІЇ (PIV CREDENTIALS)

Прийняти та електронним шляхом підтвердити повноваження облікових даних особистої ідентифікації.

Рекомендації з реалізації: Це посилення заходу застосовується у випадках, коли організації впроваджують логічні системи контролю доступу та фізичні системи контролю доступу. Верифікатори особистої інформації (PIV) — це облікові дані, що видані уповноваженими органами. Облікові дані, сумісні з PIV, — це облікові дані, видані федеральними агентствами, які відповідають публікації FIPS 201 і допоміжним керівним документам. Адекватність та надійність емітентів карток PIV авторизовано за допомогою [SP 800-79-2]. Прийняття облікових даних, сумісних із PIV, включає похідні облікові дані PIV, використання яких розглядається в [SP 800-166]. Картка спільного доступу DOD (CAC) є прикладом облікових даних PIV.

Пов'язані заходи: Немає.

(13) ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІВ ОРГАНІЗАЦІЇ) - АВТЕНТИФІКАЦІЯ ПО ЗОВНІШНЬОМУ КАНАЛУ

Застосовуйте такі механізми зовнішньої автентифікації в [*Призначення: умови, визначені організацією*]: [*Призначення: визначена організацією зовнішня автентифікація*].

Рекомендації з реалізації: Зовнішня автентифікація передбачає використання двох окремих шляхів зв'язку для ідентифікації та автентифікації користувачів або пристроїв в інформаційній системі. Перший шлях (внутрішній)

використовується для ідентифікації та автентифікації користувачів або пристроїв і, як правило, це шлях, по якому проходить інформація. Другий шлях (зовнішній) використовується для незалежної перевірки автентифікації та/або запитаної дії. Наприклад, користувач проходить автентифікацію за допомогою ноутбука на віддаленому сервері, до якого користувач бажає отримати доступ, і запитує певну дію сервера через цей шлях зв'язку. Згодом сервер зв'язується з користувачем через мобільний телефон користувача, щоб переконатися, що запитана дія походить від користувача. Користувач може підтвердити заплановану дію особі по телефону або надати код автентифікації. Зовнішня автентифікація може використовуватися для пом'якшення фактичних або ймовірних атак «людина посередині». Умови або критерії для активації включають підозрілу діяльність, нові індикатори загрози, підвищений рівень загрози або рівень впливу чи класифікації інформації в запитуваних транзакціях.

Пов'язані заходи: IA-10, IA-11, SC-37.

Посилання: FIPS Publications 140-2, 201, 202, [SP 800-63-3], [SP 800-73-4], [SP 800-76-2], [SP 800-78-4], [SP 800-79-2], [SP 800-156], [SP 800-166], [IR 7539], [IR 7676], [IR 7817], [IR 7849], [IR 7870], [IR 7874], [IR 7966].

## IA-3 ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ ПРИСТРОЇВ

Заходи захисту:
Унікально ідентифікувати та автентифікувати [*Призначення: визначені організацією типи пристроїв*] перед установкою [*Вибір (один або кілька): локального, дистанційного, мережного*] підключення.

Рекомендації з реалізації: Пристрої, що потребують унікальної взаємної ідентифікації, визначаються за типом або власне пристроєм (чи комбінацією обох параметрів). До визначених організацією типів пристроїв можуть належати пристрої, які не є власністю організації. Для ідентифікації та автентифікації пристроїв у локальних мережах можуть використовуватися: MAC-адреси, адреси в протоколі TCP/IP, дані автентифікації зі стандарту IEEE 802.1x, TLS, RADIUS серверу тощо. Організації мають визначати необхідність таких механізмів автентифікації на основі категорій безпеки систем. Через проблеми здійснення цього заходу безпеки в широкому масштабі організації можуть обмежувати його застосування визначеною кількістю (і типом) пристроїв на основі потреб організації.

Пов'язані заходи: AC-17, AC-18, AC-19, AU-6, CA-3, CA-9, IA-4, IA-5, IA-9, IA-11, SI-4.

Посилення заходів:

(1) ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ ПРИСТРОЇВ - КРИПТОГРАФІЧНА ДВОБІЧНА АВТЕНТИФІКАЦІЯ

Автентифікувати [*Призначення: певні пристрої, визначені організацією та/або типи пристроїв*] перед встановленням [*Вибір (один або кілька): локального; віддаленого; мережевого*] підключення за допомогою двобічної автентифікації, яка заснована на криптографічних механізмах.

Рекомендації з реалізації: Локальне з'єднання — це будь-яке з'єднання з пристроєм, що відбувається без використання мережі. Мережеве з'єднання — це

будь-яке з'єднання з пристроєм, що відбувається через мережу. Віддалене з'єднання — це будь-яке з'єднання з пристроєм, що відбувається через зовнішню мережу. Двонаправлена автентифікація забезпечує надійніший захист для перевірки ідентичності інших пристроїв для підключень, які становлять більший ризик.

Пов'язані заходи: SC-8, SC-12, SC-13.

(2) ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ ПРИСТРОЇВ - КРИПТОГРАФІЧНА ДВОБІЧНА МЕРЕЖА АВТЕНТИФІКАЦІЇ

[Виключено: включено до IA-3(1)].

(3) ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ ПРИСТРОЇВ - ДИНАМІЧНИЙ РОЗПОДІЛ АДРЕСИ

(a) У разі динамічного розподілу адреси визначити вимоги щодо оренди динамічного розміщення адреси та тривалості такої оренди, призначених для пристроїв відповідно до [*Призначення: інформації про оренду, визначеної організацією, та тривалість такої оренди*];

(b) Провести аудит інформації щодо оренди при призначенні на пристрій.

Рекомендації з реалізації: Протокол динамічної конфігурації хоста (DHCP) є прикладом засобу, за допомогою якого клієнти можуть динамічно отримувати призначення мережевих адрес.

Пов'язані заходи: AU-2.

(4) ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ ПРИСТРОЇВ - АТЕСТАЦІЯ ПРИСТРОЮ

Здійснювати ідентифікацію та автентифікацію пристроїв на основі атестації за допомогою [*Призначення: визначеного організацією процесу управління конфігурацією*].

Рекомендації з реалізації: Атестація пристрою стосується ідентифікації та автентифікації пристрою на основі його конфігурації та відомого робочого стану. Атестацію пристрою можна визначити за допомогою криптографічного гешу пристрою. Якщо атестація пристрою є засобом ідентифікації та автентифікації, то важливо, щоб виправлення та оновлення пристрою оброблялися через процес керування конфігурацією безпечно та не порушувало ідентифікацію та автентифікацію на інших пристроях.

Пов'язані заходи: CM-2, CM-3, CM-6.

Посилання: Немає.

## IA-4 УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ

Заходи захисту:
Управляти системними ідентифікаторами шляхом:

a. отримання дозволу від [*Призначення: визначеного організацією персоналу або ролей*] для призначення ідентифікатора особі, групі, ролі або пристрою;

b. вибору ідентифікатора, який ідентифікує окрему особу, групу, роль або пристрій;

c. призначення ідентифікатора особі, групі, ролі або пристрою;

d. запобігання повторному використанню ідентифікаторів впродовж [*Призначення: визначеного організацією періоду часу*].

Рекомендації з реалізації: Загальні ідентифікатори пристроїв охоплюють, наприклад, MAC-адреси, IP-адреси або унікальні ідентифікатори токенів. Управління індивідуальними ідентифікаторами не застосовується до спільних облікових записів системи. Зазвичай індивідуальні ідентифікатори — це імена користувачів облікових записів системи, призначених цим особам. У таких випадках в управлінні обліковими записами AC-2 використовуються імена облікових записів, надані IA-4. Цей захід безпеки також стосується окремих ідентифікаторів, не пов'язаних із системними обліковими записами. Запобігання повторному використанню ідентифікаторів передбачає запобігання присвоєнню раніше використовуваних ідентифікаторів особи, групи, ролі чи пристрою іншим особам, групам, ролям або пристроям.

Пов'язані заходи: AC-5, IA-2, IA-3, IA-5, IA-8, IA-9, IA-12, MA-4, PE-2, PE-3, PE-4, PL-4, PM-12, PS-3, PS-4, PS-5, SC-37.

Посилення заходів:

(1) УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ - ЗАБОРОНА ВИКОРИСТАННЯ ІДЕНТИФІКАТОРІВ ОБЛІКОВИХ ЗАПИСІВ ТАКИХ САМИХ, ЯК І ПУБЛІЧНІ ІДЕНТИФІКАТОРИ

Заборонити використання ідентифікаторів облікових записів системи, які збігаються із загальнодоступними ідентифікаторами для індивідуальних облікових записів.

Рекомендації з реалізації: Заборона використання ідентифікаторів облікових записів системи, які є такими самими, як і загальнодоступні ідентифікатори (наприклад, ідентифікатори адреси електронної пошти) дозволяє знизити ризик того, що порушник вгадає ідентифікатор користувача в системах. Використання цього заходу безпеки лише знижує ризик вгадування ідентифікатора; це посилення заходу необхідно використовувати разом із (а не замість) відповідними засобами захисту автентифікаторів та атрибутів для захисту облікового запису в цілому.

Пов'язані заходи: AT-2, PT-7.

(2) УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ - АВТОРИЗАЦІЯ СУПЕРВАЙЗЕРА

[Виключено: Включено до IA-12 (1)].

(3) УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ - МНОЖИННІ ФОРМИ СЕРТИФІКАЦІЇ

Виключено: Включено до IA-12(2)].

(4) УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ - ІДЕНТИФІКАЦІЯ СТАТУСУ КОРИСТУВАЧА

Управляти індивідуальними ідентифікаторами, однозначно ідентифікуючи кожного індивідуума як [*Призначення: визначена організацією ознака, що*

*ідентифікує індивідуальний статус*].

Рекомендації з реалізації: До характеристик статусу осіб належать, наприклад, статус підрядника, наявність іноземного громадянства. Ідентифікація статусу осіб за специфічними ознаками надає додаткову інформацію про осіб, з якими спілкується персонал організації. Наприклад, державному службовцю може бути корисно знати, що одна з осіб у електронному повідомленні є підрядником.

Пов'язані заходи: Немає.

(5) УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ - ДИНАМІЧНЕ УПРАВЛІННЯ

Динамічно управляти індивідуальними ідентифікаторами відповідно до [*Призначення: політика динамічних ідентифікаторів, визначена організацією*].

Рекомендації з реалізації: На відміну від традиційних підходів до ідентифікації, які передбачають статичні облікові записи для попередньо зареєстрованих користувачів, розподілені системи можуть надавати ідентифікатори суб'єктам, які раніше не були відомі безпосередньо під час взаємодії. У цих ситуаціях організації передбачають і забезпечують динамічну видачу ідентифікаторів. При цьому важливе значення мають заздалегідь налагоджені довірчі відносини та механізми з відповідними органами для підтвердження ідентичності та пов'язаних даних.

Пов'язані заходи: AC-16.

(6) УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ - КРОС-ОРГАНІЗАЦІЙНЕ УПРАВЛІННЯ

Здійснювати координацію з [*Призначення: визначеними організацією зовнішніми організаціями*] для міжорганізаційного управління ідентифікаторами.

Рекомендації з реалізації: Управління міжорганізаційними ідентифікаторами забезпечує можливість належним чином ідентифікувати осіб, групи, ролі або пристрої під час проведення міжорганізаційних заходів, пов'язаних з обробкою, зберіганням або передачею інформації.

Пов'язані заходи: AU-16, IA-2, IA-5

(7) УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ - ОСОБИСТА РЕЄСТРАЦІЯ

[Виключено: Включено до IA-12(4)].

(8) УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ - ПОПАРНІ ПСЕВДОНІМНІ ІДЕНТИФІКАТОРИ

Створити попарні псевдонімні ідентифікатори.

Рекомендації з реалізації: Парний псевдонімний ідентифікатор — це непрозорий ідентифікатор абонента, який неможливо вгадати, створений постачальником ідентифікаційної інформації для використання окремою повірюючою стороною. Генерування парних псевдонімних ідентифікаторів без ідентифікаційної інформації про користувача перешкоджає відстеженню активності користувачів. Попарні псевдонімні ідентифікатори мають бути унікальними для кожної сторони, за винятком ситуацій, коли сторони мають тісні довірчі відносини, які

підтверджуються операційною потребою у взаємодії, або всі сторони дають згоду на взаємодію таким чином.

Пов'язані заходи: IA-5.

(9) УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ - ОБСЛУГОВУВАННЯ АТРИБУТІВ І ЗАХИСТ

Зберігайте атрибути для кожної унікально ідентифікованої особи, пристрою чи служби в [*Призначення: визначене організацією захищене центральне сховище*].

Рекомендації з реалізації: Для кожного з об'єктів, розглянутих у IA-2, IA-3, IA-8 та IA-9, важливо підтримувати атрибути автентифікації на постійній основі в центральному (захищеному) сховищі.

Пов'язані заходи: Немає.

Посилання: [FIPS 201-2], [SP 800-63-3], [SP 800-73-4], [SP 800-76-2], [SP 800-78-4].

## IA-5 УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ

Заходи захисту:
Управляти системними автентифікаторами шляхом:

a. перевірки, як частини початкового розподілу автентифікатора, особи, групи, ролі або пристрою, який отримує автентифікатор;

b. створення вихідного вмісту автентифікатора для будь-яких автентифікаторів, виданих організацією;

c. забезпечення того, щоб автентифікатори мали достатню стійкість механізму для їх використання за призначенням;

d. створення та реалізація адміністративних процедур для первинного розповсюдження автентифікаторів, для втрачених/скомпрометованих або пошкоджених автентифікаторів, а також для відкликання автентифікаторів;

e. зміни типових автентифікаторів перед першим використанням;

f. зміни/оновлення автентифікаторів у встановлений [*Призначення: визначений організацією період часу за типом автентифікатора*] або коли відбуваються [*Призначення: події, визначені організацією*];

g. захисту вмісту автентифікатора від несанкціонованого розкриття та модифікацій;

h. вимоги до осіб, які використовують пристрої, використовувати спеціальні заходи безпеки для захисту автентифікаторів;

i. вимоги змінювати автентифікатори для облікових записів груп/ролей при зміні членства в цих облікових записах.

Рекомендації з реалізації: До індивідуальних автентифікаторів належать паролі, криптографічні пристрої, біометричні дані, сертифікати, пристрої з одноразовим паролем та ідентифікаційні значки. Початковий вміст автентифікатора — це

фактичний вміст автентифікатора, наприклад, початковий пароль. Вихідний вміст автентифікатора — це фактичний вміст автентифікатора, наприклад, початковий пароль. Вимоги щодо вмісту автентифікатора охоплюють, наприклад, мінімальну довжину пароля. Розробниками можуть надаватися компоненти системи із заводськими обліковими записами автентичності за замовчуванням для забезпечення початкової установки та конфігурації. Автентифікаційні дані за замовчуванням часто добре відомі, легко вгадуються та становлять значний ризик безпеки. Вимога щодо захисту індивідуальних автентифікаторів може бути реалізована через заходи безпеки PL-4 або PS-6 для автентифікаторів, що перебувають у власності фізичних осіб, та заходи безпеки AC-3, AC-6 та SC-28 для автентифікаторів, що зберігаються в системах організації, включно з паролями, які зберігаються в гешованих чи зашифрованих форматах або файлах, що містять зашифровані чи гешовані паролі. Системи підтримують управління автентифікатором за допомогою встановлених організацією налаштувань та обмежень для різних характеристик автентифікатора, включно з, наприклад, мінімальною довжиною пароля, проміжком часу перевірки синхронних одноразових маркерів та кількістю дозволених відхилень на етапі перевірки біометричної автентифікації. Дії, які можуть бути вжиті для захисту індивідуальних автентифікаторів, охоплюють, наприклад, надійне зберігання автентифікатора, заборону розголошення або передачі автентифікатора, а також вимогу негайного повідомлення про загублені, викрадені чи скомпрометовані автентифікатори. Управління автентифікатором охоплює видачу та відкликання автентифікаторів тимчасового доступу (наприклад, необхідного для віддаленого обслуговування). До автентифікаторів пристроїв належать сертифікати та паролі.

Пов’язані заходи: AC-3, AC-6, CM-6, IA-2, IA-4, IA-7, IA-8, IA-9, MA-4, PE-2, PL-4, SC-12, SC-13.

Посилення заходів:

(1) УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - АВТЕНТИФІКАЦІЯ НА ОСНОВІ ПАРОЛЯ

Для автентифікації на основі пароля необхідно:

(a) вести список часто використовуваних, очікуваних або скомпрометованих паролів та оновлювати його [*Призначення: з визначеною організацією частотою*], а також при підозрі, що паролі організацій скомпрометовані прямо чи опосередковано;

(b) перевіряти, коли користувачі створюють або оновлюють паролі, що паролі не перебувають у визначеному організацією списку найчастіше використовуваних, очікуваних або скомпрометованих паролів у IA-5(1)(a);

(c) передавати паролі лише через криптографічно захищені канали;

(d) зберігати паролі за допомогою затвердженого алгоритму гешування, переважно використовуючи ключову геш-функцію;

(e) вимагати негайного вибору нового пароля після відновлення облікового запису;

(f) дозволити користувачеві вибирати довгі паролі та фрази, включно з пробілами та всіма друкованими символами;

(g) використовувати автоматизовані інструменти для допомоги користувачеві у виборі надійних автентифікаторів паролів;

(h) застосовувати наступні правила складу та складності: [*Призначення: правила складу та складності, визначені організацією*].

Рекомендації з реалізації: Це посилення заходу застосовується до паролів незалежно від їхнього використання в однофакторній або багатофакторній автентифікації. Надається перевага використанню довгих паролів. При цьому слід застосовувати закріплені правила генерації паролів (наприклад, мінімальна довжина символів для довгих паролів) за певних обставин можна забезпечити дотримання цієї вимоги в IA-5(1)(h). Якщо пароль втрачений (користувач його забув), має відбуватися відновлення облікового запису. Криптографічно захищені паролі містять односторонні криптографічні геші паролів. Список часто використовуваних, скомпрометованих або очікуваних паролів включає попередньо зламані паролі, слова зі словника та повторювані або послідовні символи. Список містить контекстно-залежні слова, такі як назва служби, ім'я користувача та похідні від них.

Пов'язані заходи: IA-6.

(2) УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - АВТЕНТИФІКАЦІЯ НА ОСНОВІ ВІДКРИТОГО КЛЮЧА

(a) Для автентифікації на основі відкритого ключа:

1) забезпечити авторизований доступ до відповідного закритого ключа;

2) зіставити автентифіковану особу з обліковим записом особи чи групи;

(b) При використанні інфраструктури відкритого ключа (PKI):

1) перевіряти сертифікати шляхом створення та перевірки шляху сертифікації до прийнятої довіреної прив'язки, включно з перевіркою інформації про статус сертифіката;

2) впровадити локальний кеш даних для підтримки виявлення та перевірки шляху.

Рекомендації з реалізації: Асиметрична криптографія може бути надійним механізмом автентифікації осіб і пристроїв. При використанні інфраструктури відкритих ключів (PKI) інформація про стан шляхів сертифікації містить списки відкликаних сертифікатів або відповіді протоколу статусу сертифіката. Для електронних посвідчень особистості (в тому числі PIV карток), у яких зберігається особистий ключ користувача, валідація сертифікатів передбачає побудову та перевірку шляху сертифікації до кореневого сертифіката. Впровадження локального списку відкликаних сертифікатів дозволяє здійснювати перевірку валідності в ситуаціях, коли системи тимчасово відключені від зовнішньої мережі.

Пов'язані заходи: IA-3, SC-17.

(3) УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - ОСОБИСТА АБО ДОВІРЧА АВТЕНТИФІКАЦІЯ ЗОВНІШНЬОЇ СТОРОНИ

[Виключено: Включено до IA-12(4)].

(4) УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - АВТОМАТИЗОВАНА ПІДТРИМКА ДЛЯ ВИЗНАЧЕННЯ МІЦНОСТІ ПАРОЛЯ

[Виключено: Включено до IA-5(1)].

(5) УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - ЗМІНА АВТЕНТИФІКАТОРІВ ДО ДОСТАВКИ

Вимагати, щоб розробники та інсталятори компонентів системи надавали унікальні автентифікатори або змінювали за замовчуванням автентифікатори до доставки та встановлення.

Рекомендації з реалізації: Це посилення заходу розширює вимогу щодо зміни автентифікаторів за замовчуванням після встановлення системи, вимагаючи від розробників видавати унікальні автентифікатори або змінити автентифікатори за замовчуванням для компонентів системи перед їхнім інсталюванням. Однак це, як правило, не стосується розробників комерційних позаштатних продуктів інформаційних технологій. Вимоги до унікальних автентифікаторів можуть бути надані в супровідній документації, що надається організаціям при закупівлі систем або компонентів системи.

Пов’язані заходи: Немає.

(6) УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - ЗАХИСТ АВТЕНТИФІКАТОРІВ

Захищати автентифікатори відповідно з категорією безпеки інформації, до якої надає доступ використання автентифікатора.

Рекомендації з реалізації: Для систем, які обробляють інформацію різних категорій безпеки інформації без надійного фізичного чи логічного розділення між категоріями, автентифікатори, що використовуються для надання доступу до систем, мають захищатися відповідно до найвищої категорії безпеки в системах. Категорії безпеки інформації визначаються як частина процесу категоризації безпеки.

Пов’язані заходи: RA-2.

(7) УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - ВІДСУТНІСТЬ ВБУДОВАНИХ НЕЗАШИФРОВАНИХ СТАТИЧНИХ АВТЕНТИФІКАТОРІВ

Переконатися, що незашифровані статичні автентифікатори не вбудовані в застосунки або сценарії доступу та не збережені на функціональній клавіші.

Рекомендації з реалізації: Окрім програм, інші форми статичного зберігання включають сценарії доступу та функціональні клавіші. Організації проявляють обережність, визначаючи, чи є вбудовані чи збережені автентифікатори в зашифрованій чи незашифрованій формі Якщо автентифікатори можуть використовуватися без явного введення (завдяки вбудованим функціям), то вони вважаються незашифрованими незалежно від того, чи захищена така функція сама по собі.

Пов’язані заходи: Немає.

(8) УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - БАГАТОСИСТЕМНІ ОБЛІКОВІ ЗАПИСИ

Реалізувати [*Призначення: визначені організацією заходи безпеки*] для управління ризиком компрометації через те, що користувачі мають облікові записи в декількох системах.

Рекомендації з реалізації: Якщо особа має облікові записи в декількох системах, є ризик, що компрометація одного облікового запису може призвести до компрометації інших облікових записів (якщо використовуються одні й ті самі автентифікатори для всіх облікових записів). Для зниження такого ризику можливі заходи охоплюють: наявність різних автентифікаторів для різних систем; використання механізму єдиного входу; використання додатково одноразових паролів.Організації також можуть використовувати правила поведінки (див. PL-4) і угоди про доступ (див. PS-6), щоб зменшити ризик кількох облікових записів системи.

Пов'язані заходи: PS-6.

(9) УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - УПРАВЛІННЯ ОБ'ЄДНАННЯМ АВТЕНТИФІКАТОРІВ

Використовувати [*Призначення: визначені організацією зовнішні організації*] для об'єднання автентифікаторів.

Рекомендації з реалізації: Під час проведення міжорганізованих заходів, пов'язаних з обробкою, зберіганням або передачею інформації, має бути забезпечена можливість належної взаємної автентифікації.

Пов'язані заходи: AU-7, AU-16.

(10) УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - ДИНАМІЧНЕ ЗВ'ЯЗУВАННЯ МАНДАТІВ

Динамічно прив'язуйте ідентифікатори та автентифікатори за такими правилами: [*Призначення: правила зв'язування, визначені організацією*].

Рекомендації з реалізації: Перевірка автентичності вимагає певної форми прив'язки між цифровою ідентичністю та автентифікатором, що використовується для її підтвердження. У загальноприйнятих підходах це зв'язування відбувається шляхом попереднього надання ідентичності та автентифікатора системі. Наприклад, прив'язка між іменем користувача (тобто ідентичністю) та паролем (тобто автентифікатором) здійснюється шляхом надання системі ідентичності та автентифікатора як пари. Нові методи автентифікації дозволяють здійснювати зв'язок між ідентичністю та автентифікатором поза системою. Наприклад, за допомогою смарткартки, якщо ідентичність та автентифікатор пов'язані разом на ній. Використовуючи ці облікові дані, системи можуть автентифікувати цифрові ідентичності, які не були попередньо зв'язані самою системою, динамічно надаючи інформацію про цифрову ідентичність після процедури автентифікації. З цієї точки зору заздалегідь налагоджені довірчі відносини з відповідними органами для підтвердження ідентичності мають важливе значення.

Пов'язані заходи: AU-16, IA-5.

(11) УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - АВТЕНТИФІКАЦІЯ НА ОСНОВІ АПАРАТНИХ ТОКЕНІВ

[Вилучено: Включено до IA-2(1) та IA-2(2)].

(12) УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - ЕФЕКТИВНІСТЬ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ

Для біометричної автентифікації використовувати механізми, які задовольняють [*Призначення: визначені організацією вимоги до якості біометрії*].

Рекомендації з реалізації: На відміну від автентифікації на основі паролів, яка забезпечує можливість точно визначити відповідність введених користувачем паролів з тим, що зберігається, біометрична автентифікація не забезпечує таких точних перевірок. Залежно від типу біометричної автентифікації та типу механізму визначення відповідності (порівняння), є певна розбіжність між представленими біометричними даними та збереженими раніше (які служать основою для порівняння). Ефективність узгодження — це швидкість, з якою біометричний алгоритм правильно визначає таку відповідність. Вимоги до ефективності біометричної автентифікації містять, наприклад, коефіцієнт відповідності, який забепечується системою.

Пов’язані заходи: AC-7.

(13) УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - ЗАКІНЧЕННЯ ТЕРМІНУ КЕШУВАННЯ АВТЕНТИФІКАТОРІВ

Заборонити використання кешованих автентифікаторів після [*Призначення: визначеного організацією періоду часу*].

Рекомендації з реалізації: Кешовані автентифікатори використовуються для автентифікації на локальній машині, коли мережа недоступна. Якщо кешована інформація автентифікації застаріла, дійсність інформації автентифікації може бути недостовірною.

Пов’язані заходи: Немає.

(14) УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - УПРАВЛІННЯ ЗМІСТОМ ДОВІРЧИХ СХОВИЩ ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧІВ

Для автентифікації на основі інфраструктури з відкритим ключем використовувати загальноорганізаційну методологію управління вмістом довірених сховищ інфраструктури відкритого ключа, встановлених на всіх платформах, включно з мережами, операційними системами, браузерами та застосунками.

Рекомендації з реалізації: Немає.

Пов’язані заходи: Немає.

(15) УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - ПРОДУКТИ ТА ПОСЛУГИ, ЗАТВЕРДЖЕНІ УПОВНОВАЖЕНИМ ОРГАНОМ

Використовувати лише схвалені та затверджені уповноваженим органом продукти та послуги.

Рекомендації з реалізації: Продукти та послуги, затверджені уповноваженим органом — це продукти та послуги, які були затверджені відповідно до вимог

нормативних документів і законодавства та розміщені в затверджених списках.

Пов'язані заходи: Немає.

(16) УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - ПЕРЕДАЧА ОСОБИСТОЇ АБО ДОВІРЧОЇ АВТЕНТИФІКАЦІЇ ЗОВНІШНЬОЇ СТОРОНИ

Вимагати, щоб передача [*Призначення: визначених організацією видів та/або конкретних автентифікаторів*] проводилась [*Вибір: особисто; довіреною зовнішньою стороною*] до [*Призначення: визначеного організацією, зареєстрованого органу*] здійснювалася з авторизацією [*Призначення: визначеними організацією персоналом або ролями*].

Рекомендації з реалізації: Передача автентифікаторів особисто або довіреною зовнішньою стороною покращує та підвищує надійність процесу автентифікації особи.

Пов'язані заходи: IA-12.

(17) УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - АВТОМАТИЗОВАНІ ЗАСОБИ ВИЯВЛЕННЯ АТАК З ВИКОРИСТАННЯМ БІОМЕТРИЧНИХ АВТЕНТИФІКАТОРІВ

Використовувати механізми виявлення атак із використанням штучно виготовлених артефактів для біометричних автентифікаторів.

Рекомендації з реалізації: Біометричні характеристики не є таємницею. Такі характеристики можна отримати через Інтернет або просто сфотографувавши людину. Відбитки пальців можуть бути скопійовані навіть, якщо людина про це не здогадується. За допомогою захоплення зображення з високою роздільною здатністю можна отримати візерунок райдужної оболонки тощо. Автоматизовані засоби виявлення атак з використанням біометричних автентифікаторів можуть зменшити ризик виникнення цих типів атак та ускладнити створення арефактів для зламу біометричного датчика.

Пов'язані заходи: AC-7.

(18) УПРАВЛІННЯ АВТЕНТИФІКАТОРОМ - МЕНЕДЖЕР ПАРОЛІВ

a) Використовуйте [*Призначення: визначені організацією менеджери паролів*] для створення та керування паролями;

b) Захистіть паролі за допомогою [*Призначення: елементи керування, визначені організацією*].

Рекомендації з реалізації: Для систем, де використовуються статичні паролі, часто важко переконатися, що паролі є достатньо складними та що вони не використовуються в кількох системах. Менеджер паролів є вирішенням цієї проблеми, оскільки він автоматично генерує та зберігає надійні та різні паролі для різних облікових записів. Потенційний ризик використання менеджерів паролів полягає в тому, що зловмисники можуть націлитися на список паролів, згенерованих менеджером паролів. Таким чином, список паролів вимагає захисту, включаючи шифрування паролів (див. IA-5(1)(d)) і збереження цього списку офлайн в токені.

Пов’язані заходи: Немає.

Посилання: [FIPS 140-3], [FIPS 180-4], [FIPS 201-2], [FIPS 202], [SP 800-63-3], [SP 800-73-4], [SP 800-76-2], [SP 800-78-4], [IR 7539], [IR 7817], [IR 7849], [IR 7870], [IR 8040].

## IA-6 ЗВОРОТНИЙ ЗВ’ЯЗОК АВТЕНТИФІКАТОРА

Заходи захисту:
Забезпечити приховану зворотну передачу інформації автентифікації в процесі автентифікації для забезпечення захисту інформації від можливої експлуатації та використання неавторизованими особами.

Рекомендації з реалізації: Зворотній зв’язок не повинен містити інформацію, яка дозволила б стороннім особам скомпрометувати механізми автентифікації. Загроза типу «shoulder surfing» може бути більш імовірною для таких систем або компонентів, як настільні персональні комп’ютери чи ноутбуки з відносно великими моніторами, тоді як для інших, наприклад для мобільних пристроїв з невеликими дисплеями, вона є малоймовірною. Засіб для нівелювання зворотного зв’язку автентифікатора має вибиратися відповідно. До засобів приховування зворотнього зв’язку автентифікатора може належати відображення зірочок при введенні паролю або обмеження часу зворотнього зв’язку перед його приховуванням.

Пов’язані заходи: AC-3.

Посилення заходів: Немає.

Посилання: Немає.

## IA-7 АВТЕНТИФІКАЦІЯ КРИПТОГРАФІЧНОГО МОДУЛЯ

Заходи захисту:
Впровадити механізми автентифікації в криптографічний модуль, який відповідає вимогам чинних законів, виконавчих розпоряджень, директив, політик, правил, стандартів та рекомендацій для такої автентифікації.

Рекомендації з реалізації: Механізми автентифікації в криптографічному модулі можуть використовуватися для автентифікації оператора, який отримує доступ до модуля, і для перевірки того, що оператор має право виконувати конкретні дії.

Пов’язані заходи: AC-3, IA-5, SA-4, SC-12, SC-13.

Посилення заходів: Немає.

Посилання: FIPS Publication 140-3.

## IA-8 ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІ, ЩО НЕ НАЛЕЖАТЬ ДО ОРГАНІЗАЦІЇ)

Заходи захисту:
Унікально ідентифікувати та автентифікувати користувачів, що не належать до організації або процеси (що не належать організації), які діють від імені користувачів.

Рекомендації з реалізації: До користувачів, що не належать до організації, відносяться ті користувачі системи, які явно не зазначені в IA-2. Ці особи мають бути однозначно ідентифіковані й автентифіковані для отримання доступу, виняток становлять тільки випадки, коли потрібен доступ до загальнодоступних, чітко визначених і задокументованих в AC-14 ресурсів. Для ухвалення збалансованого й адекватного рішення щодо необхідності чіткої ідентифікації та автентифікації таких користувачів, організації мають враховувати багато факторів, включно з необхідністю масштабування, доцільністю, безпекою та приватністю.

Пов'язані заходи: AC-2, AC-6, AC-14, AC-17, AC-18, AU-6, IA-2, IA-4, IA-5, IA-10, IA-11, MA-4, RA-3, SA-4, SC-8.

Посилення заходів:

(1) ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІ, ЩО НЕ НАЛЕЖАТЬ ДО ОРГАНІЗАЦІЇ) - ВИЗНАННЯ ПОСВІДЧЕНЬ ІДЕНТИФІКАЦІЙНИХ ДАНИХ ВІД ІНШИХ УСТАНОВ

Приймати та в електронному вигляді перевіряти облікові дані (посвідчення ідентифікаційних даних), видані іншими установами для встановлення особи.

Рекомендації з реалізації: Це посилення заходу стосується як логічних, так і фізичних систем контролю доступу. Посвідчення ідентифікаційних даних особи — це облікові дані, видані уповноваженими установами, які відповідають чинному законодавству. Адекватність та надійність емітентів карт PIV розглядаються та авторизуються за допомогою [ SP 800-79-2 ].

Пов'язані заходи: PE-3.

(2) ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІ, ЩО НЕ НАЛЕЖАТЬ ДО ОРГАНІЗАЦІЇ) - ВИЗНАННЯ ЗОВНІШНІХ ПОСВІДЧЕНЬ ІДЕНТИФІКАЦІЙНИХ ДАНИХ

a) Приймати тільки зовнішні облікові дані (посвідчення ідентифікаційних даних), що відповідають вимогам нормативних документів та стандартів;

b) Документувати та підтримувати список прийнятих зовнішніх автентифікаторів.

Рекомендації з реалізації: Це посилення заходу стосується систем організації, доступних для громадськості (наприклад загальнодоступних вебсайтів). Зовнішні облікові автентифікатори — це ті дані, які видаються зовнішніми структурами. Вимоги щодо зовнішніх облікових даних мають відповідати або перевищувати набір вимог щодо безпеки та приватності, які затверджені в організації (це дозволить сторонам довіряти таким даним).

Пов'язані заходи: Немає.

(3) ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІ, ЩО НЕ НАЛЕЖАТЬ ДО ОРГАНІЗАЦІЇ) - ВИКОРИСТАННЯ ЗАТВЕРДЖЕНИХ ПРОДУКТІВ

[Вилучено: Включено до IA-8(2)]

(4) ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІ, ЩО НЕ НАЛЕЖАТЬ ДО ОРГАНІЗАЦІЇ) - ВИКОРИСТАННЯ ПРОФІЛІВ ВИДАНИХ УПОВНОВАЖЕНИМ ОРГАНОМ

Відповідайте наведеним нижче профілям для керування ідентифікацією.

Для керування ідентифікацією забезпечити відповідність до профілів [*Призначення: визначені організацією профілі керування ідентифікацією*], що видані уповноваженим органом.

Рекомендації з реалізації: Це посилення стосується відкритих стандартів управління цифровими ідентичностями. Для гарантування надійності й актуальності стандартів управління цифровими ідентичностями, вони мають відповідати чинним державним та міжнародним нормативним документам. Профілі таких даних мають бути затверджені уповноваженими органами.

Пов'язані заходи: Немає.

(5) ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІ, ЩО НЕ НАЛЕЖАТЬ ДО ОРГАНІЗАЦІЇ) - ВИЗНАННЯ ПОСВІДЧЕНЬ ОСОБИ (PIV-I)

Приймати та підтверджувати облікові дані або дані PKI, які відповідають [*Призначення: політика, визначена організацією*]

Приймати та підтверджувати в електронному вигляді облікові дані для підтвердження особи, що видаються недержавними органами.

Рекомендації з реалізації: Це посилення застосовується як до логічного контролю доступу, так і до фізичного. Воно стосується недержавних органів, що прагнуть взаємодіяти з державними системами, і яким можна довіряти.
Прийняття облікових даних PIV-I може здійснюватися PIV, PIV-I та іншими комерційними або зовнішніми постачальниками ідентифікаційної інформації. Прийняття та перевірка облікових даних, сумісних із PIV-I, застосовується як до логічних, так і до фізичних систем контролю доступу для недержавних емітентів посвідчень особи, які бажають взаємодіяти з урядовими системами Політика щодо сертифікатів X.509 Федерального центру сертифікації мостів (FBCA) відповідає вимогам PIV-I. Картка PIV-I співмірна з обліковими даними PIV, як визначено в цитованих посиланнях. Облікові дані PIV-I – це облікові дані, видані постачальником послуг PIV-I, чия політика сертифікатів PIV-I відповідає політиці сертифікатів Federal Bridge PIV-I. Постачальник PIV-I проходить перехресну сертифікацію з FBCA (безпосередньо або через інший міст PKI) із політиками, які зіставлено та схвалено як такі, що відповідають вимогам політик PIV-I, визначених у політиці сертифікатів FBCA.

Пов'язані заходи: Немає.

(6) ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (КОРИСТУВАЧІ, ЩО НЕ НАЛЕЖАТЬ ДО ОРГАНІЗАЦІЇ) - РОЗМЕЖУВАННЯ

Застосувати наступні заходи, щоб розмежувати атрибути користувача або зв'язки підтвердження ідентифікатора між окремими особами, постачальниками облікових даних і довіреними сторонами: [*Призначення: заходи, визначені організацією*].

Рекомендації з реалізації: Однакові рішення в управлінні цифровими ідентичностями можуть створювати підвищені ризики приватності (оскільки потенційні зловмисники легко зможуть відстежувати осіб). Використання таблиць відповідності ідентифікаторів або криптографічних методів, для розмежування постачальників облікових даних і довірених сторін один від одного або зробити атрибути ідентифікації менш видимими для сторін, може зменшити ці ризики конфіденційності.

Пов'язані заходи: Немає.

Посилання: [OMB A-130], [FED PKI], [FIPS 201-2], [SP 800-63-3], [SP 800-79-2], [SP 800-116], [IR 8062].

## IA-9 ПОСЛУГИ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ

Заходи захисту:
Ідентифікувати та автентифікувати [*Призначення: визначені організацією системні служби та застосунки*], перш ніж встановлювати зв'язок з пристроями, користувачами або іншими послугами чи застосунками.

Рекомендації з реалізації: До служб, які можуть вимагати ідентифікації та автентифікації, належать, наприклад, вебзастосунки, які використовують цифрові сертифікати, або послуги, які запитують дані з бази даних. Методи ідентифікації та автентифікації для служб/застосунків системи охоплюють, наприклад, підписи інформації або коду, графіки походження та електронні підписи, які вказують на джерела послуг. Рішення щодо дійсності ідентифікації та автентифікації приймаються службами, окремими від тих, які діють на основі цих рішень. Це може статися в системах з розподіленими архітектурами. У таких ситуаціях рішення щодо ідентифікації та автентифікації (замість фактичних ідентифікаторів і даних автентифікації) надаються службам, які повинні діяти відповідно до цих рішень.

Пов'язані заходи: IA-3, IA-4, IA-5, SC -8.

Посилення заходів:

(1) ПОСЛУГИ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ - ОБМІН ІНФОРМАЦІЄЮ

[Виключено: перенесено до IA-9]

(2) ПОСЛУГИ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ - ПЕРЕДАЧА РІШЕНЬ

[Виключено: перенесено до IA-9]

Посилання: Немає.

## IA-10 АДАПТИВНА АВТЕНТИФІКАЦІЯ

Заходи захисту:
Вимагати, щоб особи, які отримують доступ до системи, використовували [*Призначення: визначені організацією додаткові методи або механізми автентифікації*] відповідно до конкретних [*Призначення: визначених організацією обставин або ситуацій*].

Рекомендації з реалізації: Порушники можуть скомпрометувати окремі механізми автентифікації та згодом спробувати видати себе за законних користувачів. Ця ситуація потенційно може статися з будь-якими механізмами автентифікації. Для зниження ймовірності такої загрози організації можуть використовувати конкретні методи чи механізми та реалізовувати протоколи для оцінювання підозрілої поведінки. До такої поведінки може належати доступ до інформації, яку користувач зазвичай не запитував і яка йому не потрібна для виконання службових обов'язків, або спроби отримати доступ до інформації з підозрілих мережевих адрес. У заздалегідь визначених ситуаціях організації можуть вимагати від користувачів надання додаткової інформації для автентифікації. Адаптивна автентифікація не замінює і не використовується замість багатофакторних механізмів, але може розширювати реалізацію цих заходів безпеки.

Пов'язані заходи: IA-2, IA-8.

Посилення заходів: Немає.

Посилання: [SP 800-63-3].

## IA-11 ПОВТОРНА АВТЕНТИФІКАЦІЯ

Заходи захисту:
Вимагати від користувачів повторної автентифікації, при [*Призначення: визначених організацією обставинах або ситуаціях, що вимагають повторної автентифікації*].

Рекомендації з реалізації: Окрім вимог повторної автентифікації у випадках, пов'язаних з блокуванням пристроїв, організації можуть вимагати повторну автентифікацію користувачів у певних ситуаціях, зокрема при зміні автентифікатора або ролі, категорії безпеки системи, при використанні привілейованих облікових записів або після проходження встановленого проміжку часу.

Пов'язані заходи: AC-3, AC-11, IA-2, IA-3, IA-4, IA-8.

Посилення заходів: Немає.

Посилання: Немає.

## IA-12 ПЕРЕВІРКА СПРАВЖНОСТІ (ІДЕНТИЧНОСТІ)

Заходи захисту:

a. Засвідчити особи користувачів, яким потрібні облікові записи для логічного доступу до систем на основі вимог гарантій відповідного рівня, як це зазначено у відповідних стандартах і рекомендаціях.

b. Встановити ідентифікатори користувачів унікальні для особи.

c. Збирати, затверджувати та перевіряти докази (свідчення) ідентичності особи.

Рекомендації з реалізації: Підтвердження ідентичності — це процес збору та

перевірки персональних даних користувача для видачі облікових даних для доступу до системи. Цей захід безпеки призначений для зменшення ймовірності загроз при реєстрації користувачів та створенні їхніх облікових записів. Стандарти та вказівки, що визначають рівні забезпечення ідентифікації для підтвердження особи, включають [SP 800-63-3] і [SP 800-63A]. На організації можуть поширюватися закони, виконавчі накази, директиви, нормативні акти або правила, які стосуються збору ідентифікаційних даних. Персонал організації консультується зі старшим представником агентства з конфіденційності та юрисконсультантом щодо таких вимог.

Пов'язані заходи: AC-5, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-8.

Посилення заходів:

(1) ПЕРЕВІРКА СПРАВЖНОСТІ (ІДЕНТИЧНОСТІ) - АВТОРИЗАЦІЯ СУПЕРВАЙЗЕРА

Вимагати, щоб процес реєстрації для отримання облікового запису для логічного доступу містив авторизацію супервайзера.

Рекомендації з реалізації: Авторизація супервайзера забезпечує додатковий рівень перевірки, щоб переконатися, що ланцюжок керування користувача знає про обліковий запис і що обліковий запис є важливим для виконання завдань і функцій організації, а привілеї користувача відповідають передбачуваним обов'язкам і повноваженням в організації.

Пов'язані заходи: Немає.

(2) ПЕРЕВІРКА СПРАВЖНОСТІ (ІДЕНТИЧНОСТІ) - ПОСВІДЧЕННЯ ОСОБИ

Вимагати пред'явлення до реєстраційного органу документів, що посвідчують особу.

Рекомендації з реалізації: Вимога перевірки доказів ідентичності (документальних та/або біометричних) зменшує ймовірність використання особами чужих персональних даних. Форми доказів мають відповідати конкретній системі та залежати від ролей та привілеїв, пов'язаних з обліковим записом користувача.

Пов'язані заходи: Немає.

(3) ПЕРЕВІРКА СПРАВЖНОСТІ (ІДЕНТИЧНОСТІ) - ПЕРЕВІРКА ТА ВЕРИФІКАЦІЯ ДОКАЗІВ ІДЕНТИЧНОСТІ

Вимагати, щоб надані докази ідентифікації були підтверджені та перевірені за допомогою [*Призначення: визначені організацією методи перевірки та верифікації*].

Рекомендації з реалізації: Перевірка та верифікація посвідчень особи підвищує впевненість у тому, що акаунти, ідентифікатори та автентифікатори видаються істинному користувачеві. Верифікація — це процес підтвердження того, що докази є справжніми та достовірними та що дані, які містяться в доказах, є правильними, актуальними та стосуються реальної особи. Верифікація підтверджує та встановлює зв'язок між заявленою особою та фактичним існуванням користувача, який надає докази. Прийнятні методи перевірки та

верифікації посвідчень ідентичності мають відповідати конкретній системі та залежати від ролей і привілеїв, пов'язаних з обліковим записом користувача.

Пов'язані заходи: Немає.

(4) ПЕРЕВІРКА СПРАВЖНОСТІ (ІДЕНТИЧНОСТІ) - ОЧНА ПЕРЕВІРКА ТА ВЕРИФІКАЦІЯ

Вимагати, щоб підтвердження та перевірка посвідчень особи проводилися особисто в призначеному органі реєстрації.

Рекомендації з реалізації: Особиста верифікація знижує ймовірність видачі шахрайських даних, оскільки це вимагає фізичної присутності осіб, надання фізичних документів, що посвідчують особу, та фактичної взаємодії з органами реєстрації.

Пов'язані заходи: Немає.

(5) ПЕРЕВІРКА СПРАВЖНОСТІ (ІДЕНТИЧНОСТІ) - ПІДТВЕРДЖЕННЯ АДРЕСИ

Вимагати, щоб [*Вибір: реєстраційний код; повідомлення про перевірку*] доставлялися через зовнішній канал для перевірки адреси (фізичної або цифрової) реєстрації користувачів.

Рекомендації з реалізації: Для зменшення ризику того, що порушники маскуватимуться під легітимних користувачів під час процесу перевірки ідентичності, організації можуть використовувати додаткові методи для підвищення впевненості, що особою, пов'язаною з адресою запису, є та сама особа, яка брала участь у реєстрації. Підтвердження може мати форму тимчасового коду або повідомлення про підтвердження. Адреса (фізична або електронна) доставки цих тимчасових даних отримується з облікових записів, а не від користувача. Домашня адреса — приклад фізичної адреси. Адреси електронної пошти та телефонні номери — приклади електронних адрес.

Пов'язані заходи: IA-12.

(6) ПЕРЕВІРКА СПРАВЖНОСТІ (ІДЕНТИЧНОСТІ) - ПРИЙНЯТТЯ ІДЕНТИФІКАЦІЙ, СХВАЛЕНИХ ТРЕТЬОЮ СТОРОНОЮ

Приймати ідентифікатори із зовнішньою перевіркою з [*Призначення: рівень гарантії ідентичності, визначений організацією*].

Рекомендації з реалізації: Для обмеження непотрібного повторного підтвердження особи, особливо користувачів, організації можуть приймати докази, які надані іншими установами та організаціями (за умови, що такі докази відповідають політиці безпеки організації та мають достатній рівень гарантій).

Пов'язані заходи: IA-3, IA-4, IA-5, IA-8.

Посилання: [FIPS 201-2], [SP 800-63-3], [SP 800-63A], [SP 800-79-2].

## 10.8 Клас заходів захисту IR — РЕАГУВАННЯ НА ІНЦИДЕНТИ

### IR-1 ПОЛІТИКА ТА ПРОЦЕДУРИ РЕАГУВАННЯ НА ІНЦИДЕНТИ

Заходи захисту:

a. Розробити, задокументувати та поширити [*Призначення: серед визначеного організацією персоналу або ролей*]:

   1. [*Вибір (один або декілька): Рівень організації; Рівень місії/бізнес-процесу; рівень системи*] політики реагування на інциденти, яка:

      (a) містить мету, сферу застосування, ролі, обов'язки, відповідальність керівництва, координацію між організаційними підрозділами та систему контролю відповідності (complaince);

      (a) відповідає чинному законодавству, виконавчим наказам, директивам, нормам, політикам, стандартам та керівним принципам;

   2. процедури, що забезпечують реалізацію політики реагування на інциденти та пов'язані з нею заходи реагування на інциденти.

b. Призначити [*Призначення: визначену організацією посадову особу вищого керівництва*] для управління, документування і розповсюдження політики та процедур реагування на інциденти.

c. Переглядати та оновлювати поточні:

   1. політику реагування на інциденти [*Призначення: з визначеною організацією частотою*] і наступні [*Призначення: події, визначені організацією*];

   2. процедури реагування на інциденти [*Призначення: з визначеною організацією частотою*] та наступні [*Призначення: події, визначені організацією*].

Рекомендації з реалізації: Цей захід захисту стосується встановлення політики та процедур для ефективного здійснення заходів і їх посилень у класі IR. Стратегія управління ризиками є важливим фактором у встановленні політики та процедур. Комплексна політика та процедури допомагають забезпечити безпеку та приватність. За наявності політики, а також планів захисту інформації та персональних даних на рівні організації, конкретні системні політики та процедури можуть бути не потрібні. Політика може бути внесена до складу загальної політики безпеки та приватності або може бути представлена кількома політиками (у випадках складної архітектури). Процедури описують, як має реалізуватися політика чи заходи захисту та як вони можуть бути спрямовані на персонал або роль, яка є об'єктом процедури. Процедури можуть бути задокументовані в планах захисту інформації та персональних даних (як один або декілька документів). Події, які можуть спричинити оновлення політики та процедур реагування на інциденти, включають висновки оцінки або аудиту, інциденти чи порушення безпеки або зміни в законах, розпорядженнях, директивах, постановах, політиках, стандартах і вказівках. Просте повторне встановлення засобів контролю не є організаційною політикою чи процедурою.

Пов'язані заходи: PM-9, PS-8, SI-12.

Посилення заходів: Немає.

Посилання: [OMB A-130], [SP 800-12], [SP 800-30], [SP 800-39], [SP 800-50], [SP 800-61], [SP 800-83], [SP 800-100].

## IR-2 НАВЧАННЯ З РЕАГУВАННЯ НА ІНЦИДЕНТИ

Заходи захисту:

a. Забезпечити навчання користувачів щодо системи реагування на інциденти, відповідно до призначених ролей та обов'язків:

   1. у рамках [*Призначення: визначеного організацією періоду часу*], впродовж якого авторизована роль або відповідальність за реагування на інциденти;

   2. у разі внесення змін у систему;

   3. з визначеною [*Призначення: визначена організацією частота*] у подальшому.

b. Переглядайте та оновлюйте навчальний контент із реагування на інциденти [*Призначення: частота, визначена організацією*] та наступні [*Призначення: події, визначені організацією*].

Рекомендації з реалізації: Для забезпечення відповідного змісту та рівня деталізації, навчання реагування на інцидент має бути пов'язане з ролями й обов'язками персоналу організації. Наприклад, користувачам необхідно знати, як розпізнати інцидент і кому повідомити про нього; системним адміністраторам може знадобитися додаткова підготовка з питань реагування на інцидент; посадові особи, на яких покладені обов'язки безпосереднього реагування на інцидент, можуть пройти додаткову підготовку з криміналістики, звітності, відновлення та відтворення системи. Навчання має охоплювати реагування на інциденти, спровоковані як внутрішніми, так і зовнішніми джерелами. Навчання з реагування на інциденти для користувачів може бути надано як частина AT-2 або AT-3 . Події, які можуть спричинити оновлення навчального вмісту з реагування на інциденти, включають, але не обмежуються тестуванням плану реагування на інциденти або реагування на фактичний інцидент (засвоєні уроки), висновками оцінювання чи аудиту або змін у чинних законах, розпорядженнях, директивах, правилах, політиках, стандартах та рекомендаціях.

Пов'язані заходи: AT-2, AT-3, AT-4, CP-3, IR-3, IR-4, IR-8, IR-9.

Посилення заходів:

(1) НАВЧАННЯ З РЕАГУВАННЯ НА ІНЦИДЕНТИ - МОДЕЛЮВАННЯ ПОДІЙ

Впровадити в процес навчання моделювання події реагування на інциденти для забезпечення ефективного реагування персоналу в кризових ситуаціях.

Рекомендації з реалізації: Організації встановлюють вимоги щодо реагування на інциденти в планах реагування на інциденти. Включення змодельованих подій у навчання з реагування на інциденти допомагає переконатися, що персонал розуміє свої обов'язки та дії, які слід застосовувати в кризових ситуаціях.

Пов’язані заходи: Немає.

(2) НАВЧАННЯ З РЕАГУВАННЯ НА ІНЦИДЕНТИ - АВТОМАТИЗОВАНІ НАВЧАЛЬНІ СЕРЕДОВИЩА

Забезпечте навчальне середовище реагування на інциденти, використовуючи [*Призначення: автоматизовані механізми, визначені організацією*].

Рекомендації з реалізації: Автоматизовані механізми можуть забезпечити більш реалістичне середовище навчання реагування на інциденти, наприклад шляхом надання більш повного висвітлення питань реагування на інциденти, вибору більш реалістичних сценаріїв навчання, середовища та можливостей реагування.

Пов’язані заходи: Немає.

Посилання: Немає.

(3) НАВЧАННЯ З РЕАГУВАННЯ НА ІНЦИДЕНТИ - ЗЛАМ

Проведіть тренінг з реагування на інциденти щодо того, як ідентифікувати порушення та реагувати на них, включаючи процес організації повідомлень про порушення.

Рекомендації з реалізації: Для державних органів інцидент, пов’язаний із використанням персональних даних, вважається порушенням. Порушення призводить до втрати контролю, компрометації, неавторизованого розголошення, несанкціонованого придбання або випадку, коли особа, яка не є авторизованим користувачем, отримує доступ або потенційно може отримати доступ до персональних даних, авторизований користувач отримує доступ або потенційно міг отримати доступ до таких даних не для авторизованих цілей. Навчання з реагування на інциденти нагадує про обов’язок осіб повідомляти як про підтверджені, так і про ймовірні порушення, пов’язані з інформацією на будь-якому носії чи у будь-якій формі (включаючи паперовий, усний та електронний). Тренування з реагування на інциденти включають вправи, які імітують порушення. Див. IR-2(1).

Пов’язані заходи: Немає.

Посилання: [OMB M-17-12], [SP 800-50].

## IR-3 ПЕРЕВІРКА РЕАГУВАНЬ НА ІНЦИДЕНТИ

Заходи захисту:
Перевіряти ефективність реагування системи на інциденти [*Призначення: з визначеною організацією частотою*] за допомогою [*Призначення: визначених організацією тестів*].

Рекомендації з реалізації: Організації мають проводити перевірку можливості реагування на інциденти для визначення загальної ефективності та виявлення потенційних недоліків і слабких місць. Перевірка реагування на інциденти охоплює, наприклад, використання контрольних списків, моделювання та комплексні тестування. Перевірка реагування на інциденти також може містити визначення впливу на організаційні операції, активи й осіб. Для визначення ефективності процесів реагування на інциденти мають використовуватися якісні та кількісні показники.

Пов’язані заходи: CP-3, CP-4, IR-2, IR-4, IR-8, PM-14.

Посилення заходів:

(1) ПЕРЕВІРКА РЕАГУВАНЬ НА ІНЦИДЕНТИ - АВТОМАТИЧНЕ ТЕСТУВАННЯ

Перевірте здатність реагування на інциденти за допомогою [*Призначення: автоматизовані механізми, визначені організацією*].

Рекомендації з реалізації: Організації можуть використовувати автоматизовані механізми для більш ретельної та ефективної перевірки можливостей реагування на інциденти. Це може бути досягнуто, наприклад, шляхом вибору більш реалістичних сценаріїв перевірки та тестових середовищ та методів реагування на інциденти.

Пов’язані заходи: Немає.

(2) ПЕРЕВІРКА РЕАГУВАНЬ НА ІНЦИДЕНТИ - КООРДИНАЦІЯ З ПОВ’ЯЗАНИМИ ПЛАНАМИ

Координувати тестування реагування на інциденти з елементами організації, що відповідають за пов’язані плани.

Рекомендації з реалізації: Планування тестування щодо реагування на інциденти має бути пов’язане з плануванням: системи забезпечення безперервної роботи та відновлення функціонування; безперервності; відновлення після стихійних лих; безперервності операцій; критичної інфраструктури тощо.

Пов’язані заходи: Немає.

(3) ПЕРЕВІРКА РЕАГУВАНЬ НА ІНЦИДЕНТИ - ПОСТІЙНЕ ПОЛІПШЕННЯ

Використовувати якісні та кількісні дані за результатами тестування для:

(a) визначення ефективності процесів реагування на інциденти;

(b) постійного вдосконалення процесів реагування на інциденти;

(c) впровадження показників та метрик реагування на інциденти, які є точними, послідовними та відтворюваними.

Рекомендації з реалізації: Для постійного вдосконалення діяльності з реагування на інциденти організації можуть використовувати показники та критерії для оцінювання програм реагування на інциденти. Ці дії сприяють поліпшенню ефективності реагування на інциденти та зменшують можливий негативний вплив інцидентів.

Пов’язані заходи: Немає.

Посилання: [OMB A-130], [SP 800-84], [SP 800-115].

## IR-4 ОБРОБКА ІНЦИДЕНТУ

Заходи захисту:

a. Впровадити можливості обробки інцидентів безпеки та приватності, включно з підготовкою, виявленням і аналізом, локалізацією, ліквідацією та відновленням.

b. Координувати діяльність з обробки інцидентів із заходами із забезпечення безперервності функціонування.

c. Вводити уроки, що отримані з поточних дій з обробки інцидентів, у процедури реагування на інциденти, навчання й тестування та вносити відповідні зміни.

d. Забезпечити, щоб строгість, інтенсивність, обсяг і результати діяльності з обробки інцидентів можна було порівняти та передбачити у всій організації.

Рекомендації з реалізації: Здатність реагувати на інциденти залежить від можливостей систем і процесів в організації, які підтримуються ними. Тому організації мають проєктувати систему реагування на інциденти під час визначення функцій/процесів і розробки систем. Інформація, пов'язана з інцидентами, може бути отримана з різних джерел, включно, наприклад, з: моніторингу аудиту, мережі, фізичного доступу, звітів користувачів/адміністраторів, повідомленях подій ланцюга поставок. Ефективна спроможність поводження з інцидентами містить координацію між багатьма підрозділами організації, включно, наприклад, з власниками представництва, власниками системи, уповноваженими посадовими особами, кадровою службою, службами безпеки, юридичними департаментами, оперативним персоналом, службою закупівель. Передбачувані інциденти безпеки включають отримання підозрілих електронних листів, які можуть містити шкідливий код. Підозрілі інциденти в ланцюзі поставок включають внесення підробленого обладнання або шкідливого коду в системи або системні компоненти організації. Для державних органів інцидент, пов'язаний із персональними даними, вважається порушенням. Порушення призводить до несанкціонованого розголошення, втрати контролю, неавторизованого отримання, компрометації або подібного випадку, коли особа, яка не є авторизованим користувачем, отримує доступ або потенційно отримує доступ до персональних даних, або авторизований користувач отримує доступ або потенційно отримує доступ до таких даних не для авторизованих цілей.

Пов'язані заходи: AC-19, AU-6, AU-7, CM-6, CP-2, CP-3, CP-4, IR-2, IR-3, IR-5, IR-6, IR-8, PE-6, PL-2, PM-12, SA-8, SC-5, SC-7, SI-3, SI-4, SI-7.

Посилення заходів:

(1) ОБРОБКА ІНЦИДЕНТУ - АВТОМАТИЗОВАНІ ПРОЦЕСИ ОБРОБКИ ІНЦИДЕНТІВ

Використовувати автоматизовані механізми для підтримки процесу обробки інцидентів.

Рекомендації з реалізації: До автоматизованих механізмів обробки інцидентів належать: онлайн-системи управління інцидентів, а також інструменти, що підтримують збір даних у режимі реального часу, системи захоплення мережевих пакетів та системи криміналістичного аналізу.

Пов'язані заходи: Немає.

(2) ОБРОБКА ІНЦИДЕНТУ - ДИНАМІЧНА РЕКОНФІГУРАЦІЯ

Внести динамічну реконфігурацію [*Призначення: у визначені організацією системні компоненти*] як частину здатності реагування на інциденти

[*Призначення: типи динамічної реконфігурації, визначені організацією*].

Рекомендації з реалізації: Динамічна реконфігурація містить, наприклад, зміни правил маршрутизаторів, списків контролю доступу, параметрів системи виявлення/запобігання вторгненням та правил фільтрації брандмауерів і шлюзів. Організації можуть проводити динамічну реконфігурацію систем для зупинки атак, нейтралізації порушників та ізоляції компонентів систем, обмежуючи тим самим масштаби негативного впливу. Мають бути визначені часові рамки для досягнення реконфігурації систем, враховуючи потенційну потребу швидкого реагування для ефективної протидії кіберзагрозам.

Пов'язані заходи: AC-2, AC-4, CM-2.

(3) ОБРОБКА ІНЦИДЕНТУ - БЕЗПЕРЕРВНІСТЬ ОПЕРАЦІЙ

Ідентифікувати [*Призначення: визначені організацією класи інцидентів*] та [*Призначення: визначені організацією дії, які необхідно вжити у відповідь згідно з класом інциденту*] для забезпечення безперервності виконання завдань та функцій організації.

Рекомендації з реалізації: Інциденти можуть класифікуватися як: несправності через помилки проєктування/впровадження, цілеспрямовані зловмисні атаки та ненавмисні атаки. Відповідні дії щодо реагування на інциденти охоплюють, наприклад, деградацію, вимкнення системи, запровадження ручного режиму/альтернативної технології, згідно з якою система працює по-іншому, застосовуючи оманливі заходи, чергуючи інформаційні потоки або працюючи в позаштатному режимі. Організації розглядають, чи вимоги безперервності роботи під час інциденту конфліктують із можливістю автоматичного вимкнення системи, як визначено у IR-4(5).

Пов'язані заходи: Немає.

(4) ОБРОБКА ІНЦИДЕНТУ - ІНФОРМАЦІЙНА КОРЕЛЯЦІЯ

Зіставляти інформацію про інцидент та про індивідуальне реагування на інцидент з метою досягнення загальноорганізаційного бачення на обізнаність про інциденти та реагування на них.

Рекомендації з реалізації: Є типи інцидентів, які можна виявити лише шляхом збору інформації з різних джерел, серед яких різні звіти та процедури звітування, встановлені організаціями.

Пов'язані заходи: Немає.

(5) ОБРОБКА ІНЦИДЕНТУ - АВТОМАТИЧНЕ ВИМКНЕННЯ СИСТЕМИ

Реалізувати налаштовувані можливості для автоматичного вимикання системи, якщо виявлено [*Призначення: визначені організацією порушення безпеки*].

Рекомендації з реалізації: Організації розглядають, чи здатність автоматичного вимкнення системи конфліктує з вимогами безперервності роботи, визначеними як частина CP-2 або IR-4(3). Порушення безпеки включають кібератаки, які порушили цілісність системи або викрали інформацію, що належить організації, а також серйозні помилки у програмному забезпеченні, які можуть негативно вплинути на процеси чи функції організації або поставити під загрозу безпеку

окремих осіб.

Пов’язані заходи: Немає.

(6) ОБРОБКА ІНЦИДЕНТУ - ВНУТРІШНІ ЗАГРОЗИ — ОСОБЛИВІ МОЖЛИВОСТІ

Реалізувати можливість обробки інцидентів, пов’язаних з внутрішніми загрозами.

Рекомендації з реалізації: Реагування на внутрішні загрози мають розглядатися як невіддільна частина спроможності організації реагувати на інциденти. Це посилення спрямоване на додатковий акцент на такому типі загрози та потребі в конкретних можливостях реагування на такі типи інцидентів.

Пов’язані заходи: Немає.

(7) ОБРОБКА ІНЦИДЕНТУ - ВНУТРІШНІ ЗАГРОЗИ — ВНУТРІШНЬООРГАНІЗАЦІЙНА КООРДИНАЦІЯ

Координувати здатність обробки інцидентів для внутрішніх загроз через [*Призначення: визначені організацією компоненти або елементи організації*].

Рекомендації з реалізації: Реагування на внутрішні загрози потребує тісної координації між різними компонентами організації або елементами. До таких компонентів належать: власники місії, власники системи, кадрові відділи, служби безпеки тощо. Крім того, організації можуть потребувати зовнішньої підтримки державних і місцевих правоохоронних органів.

Пов’язані заходи: Немає.

(8) ОБРОБКА ІНЦИДЕНТУ - КООРДИНАЦІЯ ІЗ ЗОВНІШНІМИ ОРГАНІЗАЦІЯМИ

Координувати з [*Призначення: визначеними організацією зовнішніми організаціями*] для зіставлення та поширення [*Призначення: інформації, що визначається організацією*], для досягнення міжорганізаційного бачення обізнаності про інциденти та більш ефективного реагування на інциденти.

Рекомендації з реалізації: До зовнішніх організацій належать: партнери, члени коаліцій, замовники та зовнішні розробники. Міжорганізаційна координація щодо подолання інцидентів може підвищити здатність управління ризиками. Це дозволяє організаціям використовувати критичну інформацію з різних джерел для ефективного реагування на інциденти, що пов’язані з інформаційною безпекою, та які потенційно можуть вплинути на діяльність організації, активи та окремих осіб.

Пов’язані заходи: AU-16, PM-16.

(9) ОБРОБКА ІНЦИДЕНТУ - ЗДАТНІСТЬ ДИНАМІЧНОГО РЕАГУВАННЯ

Використовувати [*Призначення: визначені організацією можливості динамічного реагування*] для ефективного реагування на інциденти безпеки.

Рекомендації з реалізації: Це посилення стосується своєчасного використання

нових можливостей організації у відповідь на інциденти безпеки та приватності. Сюди входять можливості, що реалізовані на рівні процесів і на системному рівні.

Пов'язані заходи: Немає.

(10) ОБРОБКА ІНЦИДЕНТУ - КООРДИНАЦІЯ ЛАНЦЮГА ПОСТАЧАННЯ

Координувати діяльність з обробки інцидентів, пов'язану з подіями ланцюжка постачання, з іншими організаціями, що беруть участь у ланцюжку постачання.

Рекомендації з реалізації: До організацій, залучених до ланцюгів постачання, належать: розробники систем/продуктів, інтегратори, виробники, пакувальники, дистриб'ютори та торгові посередники. До інцидентів у ланцюгах постачання належать: порушення, пов'язані з компонентами системи, продуктами інформаційних технологій, процесами розробки або персоналом, а також процесами дистрибуції.

Пов'язані заходи: MA-2, SA-9.

Посилання: Немає.

(11) ОБРОБКА ІНЦИДЕНТУ - ІНТЕГРОВАНА ГРУПА РЕАГУВАННЯ НА ІНЦЕДЕНТИ

Створити та підтримувати інтегровану групу реагування на інциденти, яку можна розгорнути в будь-якому місці, визначеному організацією протягом [*Призначення: період часу, визначений організацією*].

Рекомендації з реалізації: Інтегрована група реагування на інциденти — це команда експертів, яка оцінює, документує і реагує на інциденти, щоб системи організації та мережі могли швидко відновитися та запровадити необхідні заходи захисту, для уникнення майбутніх інцидентів. До складу групи реагування на інциденти входять аналітики з криміналістики, аналітики зловмисного коду, розробники інструментів, інженери з системної безпеки та приватності, а також персонал, який працює в режимі реального часу. Можливості обробки інцидентів включають виконання швидкого криміналістичного збереження доказів, аналіз і реагування на вторгнення. Для деяких організацій група реагування на інциденти може бути міжорганізаційною організацією.
Інтегрована група реагування на інциденти спрощує обмін інформацією та дозволяє персоналу організації (наприклад, розробникам, виконавцям і операторам) використовувати знання команди про виявлену загрозу та впровадити заходи захисту, які дозволяють організаціям ефективніше стримувати вторгнення. Крім того, об'єднані групи сприяють швидкому виявленню вторгнень, розробці відповідних засобів послаблення та розгортанню ефективних захисних заходів. Наприклад, коли виявлено вторгнення, інтегрована команда може швидко розробити відповідну відповідь для операторів, порівняти новий інцидент з інформацією про минулі вторгнення та покращити рівень кіберрозвідки. Інтегровані групи реагування на інциденти можуть краще визначати тактику, методи та процедури супротивника, які пов'язані з темпом операцій або конкретною місією та бізнес-функціями, а також визначати відповідні дії таким чином, щоб не порушувати ці місії та бізнес-функції. Групи

реагування на інциденти можна розподілити в організаціях, щоб зробити їх більш стійкими.

Пов’язані заходи: АТ-3.

(12) ОБРОБКА ІНЦИДЕНТУ - ЗЛОВМИСНИЙ КОД ТА КРИМІНАЛІСТИЧНИЙ АНАЛІЗ

Проаналізуйте шкідливий код та/або інші залишкові артефакти, що залишилися в системі після інциденту.

Рекомендації з реалізації: Ретельний аналіз зловмисного коду та інших залишкових артефактів інциденту або порушення безпеки в ізольованому середовищі може дати організації розуміння тактики, методів та процедур противника. Він також може вказувати на особу чи деякі визначальні характеристики супротивника. Крім того, аналіз шкідливого коду може допомогти організації розробити відповіді на майбутні інциденти.

Пов’язані заходи: Немає.

(13) ОБРОБКА ІНЦИДЕНТУ - АНАЛІЗ ПОВЕДІНКИ

Проаналізувати аномальну або підозрювану ворожу поведінку в [*Завдання: середовища або ресурси, визначені організацією*]

Рекомендації з реалізації: Якщо організація підтримує обманне середовище (пісочницю), аналіз поведінки в цьому середовищі, включаючи ресурси, націлені противником, і час інциденту чи події, може дати розуміння тактики, техніки та процедур змагання. За межами обманного середовища аналіз аномальної ворожої поведінки (наприклад, змін у продуктивності системи чи моделей використання) або підозрюваної поведінки (наприклад, зміни в пошуку розташування певних ресурсів) може дати організації таке розуміння.

Пов’язані заходи: Немає.

(14) ОБРОБКА ІНЦИДЕНТУ - ЦЕНТР БЕЗПЕКИ

Створити та підтримувати оперативний центр безпеки.

Рекомендації з реалізації: Операційний центр безпеки (ОЦБ) є центром безпеки та захисту комп’ютерної мережі організації. Метою ОЦБ є захист і моніторинг систем і мереж організації (тобто кіберінфраструктури) на постійній основі. ОЦБ також відповідає за виявлення, аналіз і своєчасне реагування на інциденти кібербезпеки. Організація укомплектовує ОЦБ кваліфікованим технічним і оперативним персоналом (наприклад, аналітиками безпеки, персоналом з реагування на інциденти, інженерами системної безпеки) і реалізує комбінацію технічних, управлінських і операційних засобів контролю (включно з інструментами моніторингу, сканування та криміналістики) для моніторингу, об’єднання, корелювання, аналізу та реагування на дані про загрози та події, пов’язані з безпекою, з багатьох джерел. Ці джерела включають засоби захисту периметра, мережеві пристрої (наприклад, маршрутизатори, комутатори) і канали даних агентів кінцевих точок. ОЦБ надає можливість цілісної ситуаційної обізнаності, щоб допомогти організаціям визначити рівень безпеки системи та організації. Впровадити ОЦБ можна отримати різними способами. Більші організації можуть запровадити спеціальний ОЦБ, тоді як менші організації

можуть залучати сторонні організації для впровадження ОЦБ.

Пов'язані заходи: Немає.

(15) ОБРОБКА ІНЦИДЕНТУ - ЗВ'ЯЗКИ З ГРОМАДКІСТЮ ТА ВІДНОВЛЕННЯ РЕПУТАЦІЇ

a) керування зв'язками з громадськістю, пов'язаними з інцидентом; і

b) вживання заходів для відновлення репутації організації.

Рекомендації з реалізації: Для організації важливо мати стратегію для вирішення інцидентів, які були доведені до відома широкої громадськості, представили організацію в негативному світлі або вплинули на складові організації (наприклад, партнерів, клієнтів). Така публічність може зашкодити організації та вплинути на її здатність виконувати свою місію та бізнес-функції. Вжиття проактивних заходів для відновлення репутації організації є важливим аспектом відновлення довіри та впевненості її учасників.

Пов'язані заходи: Немає.

Посилання: [FASC18], [41 CFR 201], [OMB M-17-12], [SP 800-61], [SP 800-86], [SP 800-101], [SP 800-150], [SP 800-160-2], [SP 800-184], [IR 7559].

## IR-5 МОНІТОРИНГ ІНЦИДЕНТУ

Заходи захисту:

Відстежувати та документувати інциденти безпеки та приватності.

Рекомендації з реалізації: Документування інцидентів системи безпеки та приватності охоплює: ведення записів про кожен інцидент, стан інциденту та іншу відповідну інформацію, необхідну для судових експертиз, оцінювання деталей, тенденцій та поводження щодо інцидентів. Інформація про інциденти може бути отримана з різних джерел (мережевий моніторинг; повідомлення про інциденти; звіти груп реагування на інциденти; скарги користувачів; моніторинг аудиту; моніторинг фізичного доступу; звіти користувачів та адміністраторів тощо). IR-4 надає інформацію про типи інцидентів, які підходять для моніторингу.

Пов'язані заходи: AU-6, AU-7, IR-4, IR-6, IR-8, PE-6, PM-5, SC-5, SC-7, SI-3, SI-4, SI-7.

Посилення заходів:

(1) МОНІТОРИНГ ІНЦИДЕНТУ - АВТОМАТИЗОВАНЕ ВІДСТЕЖЕННЯ, ЗБІР ДАНИХ І АНАЛІЗ

Відстежувати інциденти, збирати й аналізувати інформацію про інциденти за допомогою [*Призначення: автоматизовані механізми, визначені організацією*].

Рекомендації з реалізації: До автоматизованих механізмів відстеження інцидентів, збору й аналізу даних про інциденти належать центри реагування на комп'ютерні інциденти або інші електронні бази даних інцидентів і пристрої мережевого моніторингу.

Пов'язані заходи: Немає.

Посилання: [SP 800-61].

## IR-6 ЗВІТНІСТЬ ПРО ІНЦИДЕНТИ

Заходи захисту:

a. Вимагати від персоналу повідомляти про підозрілі інциденти з безпеки та приватності відповідно до організаційної спроможності реагування на інциденти впродовж [*Призначення: визначеного організацією періоду часу*].

b. Звітувати про інциденти безпеки, приватності та ланцюжки постачання в [*Призначення: визначений організацією уповноважений орган*].

Рекомендації з реалізації: Типи інцидентів, про які необхідно звітувати, зміст і терміни подання звітів мають відображатися в чинних законах, наказах, директивах, положеннях, політиках і стандартах. Інформація про інциденти може інформувати про оцінку ризиків, оцінку ефективності контролю, вимоги безпеки для придбань і критерії вибору технологічних продуктів.

Пов'язані заходи: CM-6, CP-2, IR-4, IR-5, IR-8, IR-9.

Посилення заходів:

(1) ЗВІТНІСТЬ ПРО ІНЦИДЕНТИ - АВТОМАТИЧНЕ ЗВІТУВАННЯ

Повідомляйте про інциденти за допомогою [ Призначення: автоматизовані механізми, визначені організацією ]..

Рекомендації з реалізації: Одержувачі звітів про інциденти вказані в IR-6b . Механізми автоматизованого звітування включають електронну пошту, публікацію на вебсайтах (з автоматичними оновленнями) та автоматизовані інструменти та програми реагування на інциденти.

Пов'язані заходи: IR-7.

(2) ЗВІТНІСТЬ ПРО ІНЦИДЕНТИ - ВРАЗЛИВІСТЬ, ПОВ'ЯЗАНА З ІНЦИДЕНТАМИ

Повідомляти про вразливості системи, пов'язані із зареєстрованими інцидентами безпеки та приватності [*Призначення: визначеним організацією персоналу чи ролям*].

Рекомендації з реалізації: Повідомлення про інциденти, які виявляють вразливі місця системи, аналізуються персоналом організації, включаючи власників системи, та власників бізнесу, старших офіцерів інформаційної безпеки, старших посадових осіб з питань конфіденційності, авторизованих представників та керівника ризиками. Аналіз може служити для встановлення пріоритетів та ініціювання дій із запобігання виявленій вразливості системи.

Пов'язані заходи: Немає.

(3) ЗВІТНІСТЬ ПРО ІНЦИДЕНТИ - КООРДИНАЦІЯ ЛАНЦЮЖКА ПОСТАЧАННЯ

Надати інформацію про інциденти безпеки та приватності постачальнику продукту або послуги та іншим організаціям, які беруть участь у ланцюжку

постачання систем або компонентів системи, пов'язаних з інцидентом.

Рекомендації з реалізації: До організацій, залучених до ланцюгів постачання, належать: розробники систем/продуктів, інтегратори, виробники, пакувальники, дистриб'ютори та торгові посередники. До інцидентів у ланцюгах постачання належать: порушення, які пов'язані з компонентами системи, продуктами інформаційних технологій, процесами розробки або персоналом, а також процесами дистрибуції. Організації визначають відповідну інформацію для обміну та враховують цінність, отриману від інформування зовнішніх організацій про інциденти в ланцюзі постачання, включаючи можливість покращити процеси або визначити першопричину інциденту.

Пов'язані заходи: SA-8.

Посилання: Немає.

## IR-7 ПІДТРИМКА РЕАГУВАННЯ НА ІНЦИДЕНТИ

Заходи захисту:

Надавати ресурси для підтримки реагування на інциденти, що є невіддільною частиною спроможностей організації реагування на інциденти, які являють собою поради та допомогу користувачам інформаційної системи для обробки та формування звітності про інциденти безпеки та приватності.

Рекомендації з реалізації: До ресурсів підтримки реагування на інциденти належать службові довідники, групи допомоги, підтримка служб судово-медичної експертизи та послуг щодо захисту прав споживачів, якщо це вимагається.

Пов'язані заходи: AT-2, AT-3, IR-4, IR-6, IR-8, PM-22, PM-26, SA-9, SI-18.

Посилення заходів:

(1) ПІДТРИМКА РЕАГУВАННЯ НА ІНЦИДЕНТИ - АВТОМАТИЗАЦІЯ ПІДТРИМКИ ДЛЯ ЗАБЕЗПЕЧЕННЯ ДОСТУПНОСТІ ІНФОРМАЦІЇ ТА ПІДТРИМКИ

Впровадити автоматизовані механізми [*Призначення: автоматизовані механізми, визначені організацією*] для збільшення доступності пов'язаної з реагуванням на інциденти інформації та підтримки.

Рекомендації з реалізації: Автоматизовані механізми можуть реалізовуватися у двох напрямах від та/або до користувача. Наприклад, користувачі можуть мати доступ до вебсайту для запиту допомоги, або механізм надання допомоги може проактивно надсилати інформацію користувачам, як частину підвищення розуміння поточних можливостей реагування та підтримки.

Пов'язані заходи: Немає.

(2) ПІДТРИМКА РЕАГУВАННЯ НА ІНЦИДЕНТИ - КООРДИНАЦІЯ ІЗ ЗОВНІШНІМИ ПОСТАЧАЛЬНИКАМИ

(a) Встановити прямі відносини кооперації між здатністю реагування на інциденти та зовнішніми постачальниками можливостей захисту системи.

(b) Визначити членів команди реагування на інциденти в організації для зовнішніх постачальників послуг.

Рекомендації з реалізації: Зовнішні постачальники можуть допомагати захищати, контролювати, аналізувати, виявляти та реагувати на несанкціоновану діяльність в інформаційних системах і мережах організації. Також можна прописувати пункти в угодах із зовнішніми постачальниками щодо ролей та обов'язків кожної сторони у разі кіберінциденту.

Пов'язані заходи: Немає.

Посилання: [OMB A-130], [IR 7559].

## IR-8 ПЛАН РЕАГУВАННЯ НА ІНЦИДЕНТИ

Заходи захисту:

a. Розробити план реагування на інциденти, який:

1. надає організації дорожню карту для впровадження її можливостей реагування на інциденти;

2. описує структуру та організацію спроможності реагування на інциденти;

3. надає високорівневий підхід до того, як здатність реагування на інциденти вписується в загальну практику організації;

4. відповідає унікальним вимогам організації, які пов'язані із завданнями, розміром, структурою і функціями;

5. визначає підзвітні інциденти;

6. надає показники для вимірювання можливостей реагування на інциденти всередині організації;

7. визначає ресурси та управлінську підтримку, необхідну для ефективної підтримки та розвитку можливостей реагування на інциденти;

8. вирішує питання обміну інформацією про інциденти;

9. явно визначає відповідальність за реагування на інциденти [*Призначення: визначеним організацією персоналом або ролями*];

10. явно визначає відповідальність за реагування на інциденти [*Призначення: визначеним організацією персоналом або ролями*].

b. Поширити копії плану реагування на інциденти серед [*Призначення: визначеного організацією персоналу, який відповідає за конкретні дії, (який визначається за іменем та/або за ролями) та організаційними елементами*].

c. Оновлювати план реагування на інциденти в разі змін в системі та організації або проблем, що виникають при реалізації, виконанні чи тестуванні плану.

d. Повідомляти про зміни плану реагування на інциденти [*Призначення: визначений організацією персонал з реагування на інциденти, визначений за іменем та/або за*

*ролями) й організаційні елементи*].

e. Захистити план реагування на інциденти від несанкціонованого розкриття та модифікації.

Рекомендації з реалізації: Важливо застосовувати комплексний підхід до реагування на інциденти. Організаційні місії, функції, стратегії, цілі та завдання реагування на інциденти допомагають визначити структуру можливостей реагування на інциденти. Як частина можливості всебічного реагування на інциденти, організації розглядають координацію та обмін інформацією із зовнішніми організаціями, включно з, наприклад, зовнішніми постачальниками послуг, що беруть участь у ланцюзі постачань.

Пов'язані заходи: AC-2, CP-2, CP-4, IR-4, IR-7, IR-9, PE-6, PL-2, SA-15, SI-12, SR-8.

Посилення заходів:

(1) ПЛАН РЕАГУВАННЯ НА ІНЦИДЕНТИ - ОБРОБКА ПЕРСОНАЛЬНИХ ДАНИХ

Внести такі додаткові процеси в План реагування на інциденти для інцидентів, пов'язаних з персональними даними:

(a) процес визначення доцільності повідомлення наглядових організацій і надання такого повідомлення, якщо це доречно;

(b) процес оцінювання для визначення ступеня шкоди, труднощів, незручностей або несправедливості щодо постраждалих осіб та будь-які механізми пом'якшення такої шкоди;

(c) ідентифікація застосовних вимог щодо конфіденційності.

Рекомендації з реалізації: Відповідно до закону, нормативно-правових актів або політики організації можуть бути зобов'язані дотримуватися певних процедур, пов'язаних із порушеннями, зокрема повідомляти окремим особам, відповідним організаціям і контролюючим органам; стандарти шкідливості; і помякшення або інші спеціальні вимоги.

Пов'язані заходи: PT-1, PT-2, PT-3, PT-4, PT-5, PT-7.

Посилання: [OMB A-130], [SP 800-61], [OMB M-17-12].

## IR-9 РЕАГУВАННЯ НА ВИТІК ІНФОРМАЦІЇ

Заходи захисту:

Реагувати на витік інформації шляхом:

a. призначення [*Призначення: персонал або ролі, визначені організацією*] відповідального за реагування на витік інформації;

b. визначення конкретної інформації, пов'язаної з джерелом витоку в системі;

c. попередження [*Призначення: визначеного організацією персоналу або ролей*] про

витік інформації за допомогою методу зв'язку, не пов'язаного з витоком;

d. ізолювання системи або системної компоненти, де відбувся витік інформації;

e. видалення інформації із системи або компонента;

f. визначення іншої системи або компонента системи, які згодом могли б бути джерелом витоку інформації;

g. виконання таких додаткових дій: [*Призначення: визначених організацією дій*].

Рекомендації з реалізації: Витік інформації — ситуація, коли критична інформація ненавмисно розміщується в системах, які не мають повноважень її обробляти. Такі витоки інформації виникають, коли інформація, що спочатку мала нижчий рівень критичності, передається в систему, а згодом визначається як інформація з вищим рівнем критичності. Характер реагування, як правило, ґрунтується на ступені критичності розповсюдженої інформації, можливостях системи безпеки, специфічному характері носіїв даних і привілеях осіб, які мають доступ до скомпрометованої інформації. Методи, які використовуються для передачі інформації про витік інформації, не мають бути пов'язані із фактичним джерелом витоку інформації для мінімізації ризиків подальшого його поширення до того, як він буде ізольований або видалений з системи.

Пов'язані заходи: CP-2, IR-6, PM-26, PM-27, PT-2, PT-3, PT-7, RA-7.

Посилення заходів:

(1) РЕАГУВАННЯ НА ВИТІК ІНФОРМАЦІЇ - ВІДПОВІДАЛЬНИЙ ПЕРСОНАЛ

[Вилучено: включено до IR-9]

(2) РЕАГУВАННЯ НА ВИТІК ІНФОРМАЦІЇ - ТРЕНУВАННЯ

Забезпечити навчання з реагування на витік інформації [*Призначення: з визначеною організацією частотою*].

Рекомендації з реалізації: організації встановлюють вимоги щодо реагування на випадки витоку інформації в планах реагування на інциденти. Регулярне навчання з реагування на інциденти допомагає переконатися, що персонал організації розуміє свої особисті обов'язки та які конкретні дії слід вживати, коли трапляються випадки розливу.

Пов'язані заходи: AT-2, AT-3, CP-3, IR-2.

(3) РЕАГУВАННЯ НА ВИТІК ІНФОРМАЦІЇ - РОБОТА ПІСЛЯ ВИТОКУ

Реалізувати [*Призначення: визначені організацією процедури*] з метою забезпечення, щоб персонал організації, на який впливає витік інформації, був спроможний продовжувати виконувати поставлені завдання, тоді як постраждалі системи зазнають коригувальних дій.

Рекомендації з реалізації: Коригувальні дії для систем, постраждалих через витік інформації, можуть забрати багато часу. У ці періоди персонал може не мати доступу до постраждалих систем, що потенційно може вплинути на їхню здатність вести організаційну діяльність.

Пов’язані заходи: Немає.

(4) РЕАГУВАННЯ НА ВИТІК ІНФОРМАЦІЇ - ВИКРИТТЯ НЕАВТОРИЗОВАНОГО ПЕРСОНАЛУ

Застосовуйте [*Призначення: визначені організацією механізми захисту*] для персоналу, що має доступ до інформації, яка не відповідає призначеним правам доступу.

Рекомендації з реалізації: Гарантії безпеки охоплюють, наприклад, забезпечення того, щоб персонал, який має доступ до інформації, був ознайомлений із законами, наказами, директивами, положеннями, правилами, стандартами та вказівками щодо інформації та обмежень, що накладаються в разі ознайомлення з такою інформації.

Пов’язані заходи: Немає.

Посилання: Немає.

## IR-10 ІНТЕГРОВАНА КОМАНДА АНАЛІЗУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

[Вилучено: перенесено до IR-4(11)]

## 10.9 Клас заходів захисту MA — ТЕХНІЧНЕ ОБСЛУГОВУВАННЯ

### MA-1 ПОЛІТИКА ТА ПРОЦЕДУРИ ТЕХНІЧНОГО ОБСЛУГОВУВАННЯ

Заходи захисту:

a. Розробити, задокументувати та поширити серед [*Призначення: визначеного організацією персоналу або посад*]:

   1. Політику технічного обслуговування системи, яка:

      (a) містить мету, сферу застосування, ролі, обов'язки, відповідальність керівництва, координацію між організаційними підрозділами та систему контролю відповідності (complaince);

      (b) відповідає чинному законодавству, виконавчим наказам, директивам, нормам, політикам, стандартам і керівним принципам.

   2. Процедури, що сприяють здійсненню політики та заходів технічного обслуговування систем.

b. Призначити [*Призначення: визначену організацією посадову особу*] для управління політикою та процедурами технічного обслуговування.

c. Переглядати та оновлювати:

   1. Поточну політику технічного обслуговування систем [*Призначення: з визначеною організацією частотою*] та слідувати [*Призначення: події визначені організацією*].

   2. Поточні процедури технічного обслуговування систем [*Призначення: з визначеною організацією частотою*] та слідувати [*Призначення: події визначені організацією*].

Рекомендації з реалізації: Цей захід захисту стосується встановлення політики та процедур для ефективного здійснення заходів і їх посилень у класі MA. Стратегія управління ризиками є важливим фактором у встановленні політики та процедур. Комплексна політика та процедури допомагають забезпечити безпеку та приватність. За наявності політики, а також планів захисту інформації та персональних даних на рівні організації, конкретні системні політики та процедури можуть бути не потрібні. Політика може бути внесена до складу загальної політики безпеки та приватності або може бути представлена кількома політиками (у випадках складної архітектури). Процедури описують, як має реалізуватися політика або заходи захисту та як вони можуть бути спрямовані на персонал або роль, що є об'єктом процедури. Процедури можуть бути задокументовані в планах захисту інформації та персональних даних (як один або декілька документів). Просте переформулювання засобів захисту не є організаційною політикою чи процедурою.

Пов'язані заходи: PM-9, PS-8, SI-12.

Посилення заходів: Немає.

Посилання: [OMB A-130], [SP 800-12], [SP 800-30], [SP 800-39], [SP 800-100].

## MA-2 КОНТРОЛЬОВАНЕ ОБСЛУГОВУВАННЯ

Заходи захисту:

a. Планувати, документувати та переглядати записи з технічного обслуговування, ремонту або заміни компонентів системи відповідно до вимог виробника та постачальників та/або вимог організації.

b. Затвердити та здійснювати моніторинг усіх заходів з технічного обслуговування, незалежно від того, виконуються вони на місці або віддалено, а також чи обслуговуються системи або системні компоненти на місці, чи переміщуються в інше місце.

c. Вимагати, щоб [*Призначення: визначені організацією персонал чи ролі*] явно схвалили видалення системи або компоненту системи з організаційного обладнання для технічного обслуговування, ремонту чи заміни поза об'єктами експлуатації.

d. Очищати обладнання з погляду видалення всієї інформації з носіїв до вилучення обладнання організації для технічного обслуговування, ремонту чи заміни поза об'єктами експлуатації.

e. Перевірити всі потенційно порушені заходи захисту, щоб переконатися, що вони, як і раніше, працюють належним чином після дій з обслуговування, ремонту або заміни.

f. Вносити *[Призначення: визначену організацією інформацію, пов'язану з технічним обслуговуванням*] до записів з технічного обслуговування.

Рекомендації з реалізації: Цей захід безпеки стосується аспектів інформаційної безпеки технічного обслуговування програм і застосунків. Технічне обслуговування системи охоплює також ті компоненти, які безпосередньо не пов'язані з обробкою та/або збереженням даних чи інформації (сканери, копіювальні апарати та принтери). До необхідної інформації при створенні ефективних записів технічного обслуговування належать: дата та час обслуговування; найменування осіб або групи, що виконують технічне обслуговування; назва супроводу, якщо це необхідно; опис проведеного технічного обслуговування; компоненти системи або обладнання, що вилучені або замінені (включно з ідентифікаційними номерами). Рівень деталізації записів технічного обслуговування повинен бути відповідний категоріям безпеки систем організації.

Пов'язані заходи: CM-2, CM-3, CM-4, CM-5, CM-8, MA-4, MP-6, PE-16, SA-12, SA-19, SI-2, SR-3, SR-4, SR-11.
Посилення заходів:

(1) КОНТРОЛЬОВАНЕ ОБСЛУГОВУВАННЯ - ЗМІСТ ЗАПИСУ

[Вилучено: Включено до MA-2]

(2) КОНТРОЛЬОВАНЕ ОБСЛУГОВУВАННЯ - АВТОМАТИЗОВАНА ТЕХНІЧНА ДІЯЛЬНІСТЬ

(a) Використовувати автоматизовані механізми для планування, проведення та документування дій з обслуговування, ремонту та заміни системи або її компонентів.

(b) Надавати оновлені, точні та повні записи про всі дії з технічного обслуговування, ремонту та заміни; замовлених, запланованих, виконуваних та завершених дій.

Рекомендації з реалізації: Використання автоматизованих механізмів для управління та контролю технічного обслуговування дозволяє забезпечити створення своєчасних, повних та точних записів щодо технічного обслуговування.

Пов'язані заходи: MA-3.

Посилання: [OMB A-130], [IR 8023].

## MA-3 ІНСТРУМЕНТИ ДЛЯ ОБСЛУГОВУВАННЯ

Заходи захисту:

a. Затвердити, контролювати та відстежувати використання засобів технічного обслуговування.

b. Переглядати раніше затверджені інструменти технічного обслуговування [*Призначення: з частотою, визначеною організацією*].

Рекомендації з реалізації: Цей захід стосується питань безпеки, пов'язаних з інструментами технічного обслуговування, які не перебувають у межах організаційної системи, але використовуються в діагностичних і ремонтних заходах в системах організації. Організації можуть змінювати ролі відповідальних за затвердження інструментів технічного обслуговування залежно від того, як таке затвердження документується. Інструменти технічного обслуговування мають піддаватися періодичним перевіркам для вилучення або заміни, як такі, що не є актуальними або ефективними. До інструментів технічного обслуговування може належати апаратне та програмне забезпечення. Інструменти технічного обслуговування можуть бути потенційними контейнерами транспортування шкідливого коду (навмисно чи ненавмисно). Цей захід безпеки не охоплює апаратні чи програмні компоненти, які підтримують системи та є її частиною.

Пов'язані заходи: MA-2, PE-16.

Посилення заходів:

(1) ІНСТРУМЕНТИ ДЛЯ ОБСЛУГОВУВАННЯ - ПЕРЕВІРКА ІНСТРУМЕНТІВ

Оглянути інструменти для технічного обслуговування, які доставлені на об'єкт обслуговим персоналом, на предмет неправильних або несанкціонованих модифікацій.

Рекомендації з реалізації: Інструменти технічного обслуговування можна вносити на об'єкт обслуговуючим персоналом або завантажити з веб-сайту постачальника. Якщо після перевірки інструментів технічного обслуговування було визначено, що інструменти модифіковані в неналежний/несанкціонований спосіб або містять шкідливий код, такий інцидент обробляється відповідно до організаційної політики та процедур поводження з інцидентами.

Пов’язані заходи: SI-7.

(2) ІНСТРУМЕНТИ ДЛЯ ОБСЛУГОВУВАННЯ - ПЕРЕВІРКА НОСІЇВ ІНФОРМАЦІЇ

Перед використанням носіїв у системі перевірити носії, що містять діагностичні та тестові програми на наявність шкідливого коду.

Рекомендації з реалізації: Якщо після перевірки носіїв, що містять діагностичні та тестові програми, організація визначила що носії містять шкідливий код. Такий інцидент розглядається відповідно до політики та процедур обробки інцидентів організації.

Пов’язані заходи: SI-3.

(3) ІНСТРУМЕНТИ ДЛЯ ОБСЛУГОВУВАННЯ - ЗАПОБІГАННЯ НЕСАНКЦІОНОВАНОМУ ПЕРЕМІЩЕННЮ

Запобігти переміщенню обладнання для технічного обслуговування, що містить організаційну інформацію, шляхом:

(a) перевірки відсутності організаційної інформації, розміщеної на обладнанні;

(b) очищення або знищення обладнання;

(c) утримання обладнання на об’єкті;

(d) отримання дозволу від [*Призначення: визначених організацією персоналу чи ролей*], які явно дозволяють переміщення обладнання з об’єкта.

Рекомендації з реалізації: До організаційної інформації належить уся інформація, яка є власністю організацій, та інформація, що надається організаціям, у яких вони виконують функції управління щодо інформації.

Пов’язані заходи: MP-6.

(4) ІНСТРУМЕНТИ ДЛЯ ОБСЛУГОВУВАННЯ - ОБМЕЖЕННЯ ВИКОРИСТАННЯ ІНСТРУМЕНТА

Обмежити використання інструментів технічного обслуговування лише авторизованим персоналом.

Рекомендації з реалізації: Це посилення стосується систем, які використовуються для технічного обслуговування.

Пов’язані заходи: AC-3, AC-5, AC-6.

Посилання: Немає.

(5) ІНСТРУМЕНТИ ДЛЯ ОБСЛУГОВУВАННЯ - ПРИВІЛЕЙОВАНЕ ВИКОНАННЯ

Контроль використання засобів обслуговування, які мають підвищені привілеї виконання.

Рекомендації з реалізації: Інструменти обслуговування, які виконуються з

підвищеними системними привілеями, можуть призвести до несанкціонованого доступу до інформації та активів, що належать організації, які в іншому випадку були б недоступні.

Пов'язані заходи: AC-3, AC-6.

(6) ІНСТРУМЕНТИ ДЛЯ ОБСЛУГОВУВАННЯ - ОНОВЛЕННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Перевіряйте засоби захисту, щоб переконатися, що встановлено останні оновлення програмного забезпечення.

Рекомендації з реалізації: Засоби захисту, які використовують застаріле та/або неоновлене програмне забезпечення, можуть стати вектором загрози для зловмисників і призвести до значної вразливості системи та організації.

Пов'язані заходи: AC-3, AC-6.

Посилання: [SP 800-88].

## MA-4 ВІДДАЛЕНЕ ОБСЛУГОВУВАННЯ

Заходи захисту:

a. Впровадити та відстежувати віддалені дії з обслуговування та діагностики.

b. Дозволити використання віддалених засобів технічного обслуговування та діагностики лише відповідно до організаційної політики та в разі, якщо це документально зафіксовано в плані безпеки системи.

c. Використовувати надійну автентифікацію при встановленні віддалених технічних та діагностичних сеансів.

d. Вести облік віддалених дій з обслуговування та діагностики.

e. Припинити сесії та мережеві з'єднання, коли завершено віддалене обслуговування.

Рекомендації з реалізації: Віддалене обслуговування та діагностика — це діяльність, яка проводиться через внутрішню або зовнішню мережі. Локальні заходи з обслуговування та діагностики — це ті заходи, що здійснюються особами, які фізично перебувають у системі чи компоненті системи та не використовують мережеве з'єднання. Методи автентифікації, що використовуються для створення віддалених сеансів обслуговування та діагностики, відображають вимоги доступу до мережі в IA-2. Надійна автентифікація повинна включати інфраструктуру відкритих ключів (PKI), де сертифікати зберігаються на токені, захищеному паролем, парольною фразою, або біометричними даними. Забезпечення вимог до MA-4 частково виконується іншими органами управління. [SP 800-63B] надає додаткові вказівки щодо надійної автентифікації та автентифікаторів.

Пов'язані заходи: AC-2, AC-3, AC-6, AC-17, AU-2, AU-3, IA-2, IA-4, IA-5, IA-8, MA-2, MA-5, PL-2, SC-7, SC-10.

Посилення заходів:

(1) ВІДДАЛЕНЕ ОБСЛУГОВУВАННЯ - АУДИТ І ОГЛЯД

(a) Журналювання заходів [*Призначення: визначені організацією події аудиту*] для віддалених сеансів обслуговування та діагностики.

(б) Здійснювати огляд записів про сеанси віддаленого обслуговування та діагностики.

Рекомендації з реалізації: Журнал аудиту для віддаленого обслуговування забезпечується AU-2. Події аудиту визначені в AU-2a.

Пов'язані заходи: AU-6, AU-12.

(2) ВІДДАЛЕНЕ ОБСЛУГОВУВАННЯ - ДОКУМЕНТУВАННЯ ВІДДАЛЕНОГО ОБСЛУГОВУВАННЯ

[Вилучено: включено до MA-1 та MA-4]

(3) ВІДДАЛЕНЕ ОБСЛУГОВУВАННЯ - ПОРІВНЯЛЬНА БЕЗПЕКА ТА ОЧИЩЕННЯ

(a) Вимагати, щоб віддалені послуги з обслуговування та діагностики виконувалися із системи, яка реалізує заходи безпеки і які можна порівняти із заходами, реалізованими в системі, що обслуговується.

(b) Видалити компонент, який підлягає обслуговуванню, із системи до віддаленого обслуговування або діагностичних послуг; очистити компонент (від інформації, що належить організації) після того, як обслуговування виконано, перевірити та очистити компонент (від потенційно шкідливого програмного забезпечення) перед тим, повторним підключенням компонентів до системи.

Рекомендації з реалізації: Порівнюваність можливостей безпеки систем, діагностичних інструментів та обладнання означає, що реалізований захід безпеки в цих системах, інструментах та обладнанні є, як мінімум, настільки ж комплексним, як і заходи безпеки в системі, що його обслуговує.

Пов'язані заходи: MP-6, SI-3, SI-7.

(4) ВІДДАЛЕНЕ ОБСЛУГОВУВАННЯ - АВТЕНТИФІКАЦІЯ ТА РОЗПОДІЛ СЕСІЇ ОБСЛУГОВУВАННЯ

Захистити віддалені сеанси обслуговування за допомогою:

(a) використання [*Призначення: визначених організацією автентифікаторів, які стійкі до відтворення*];

(b) відокремлення сеансів обслуговування від інших мережевих сеансів із системою шляхом:

(1) фізично відокремленого шляху зв'язку;

(2) логічно розділеного шляху зв'язку на основі шифрування.

Рекомендації з реалізації: Шляхи зв'язку можуть бути логічно розділені за допомогою шифрування.

Пов'язані заходи: Немає.

(5) ВІДДАЛЕНЕ ОБСЛУГОВУВАННЯ - СХВАЛЕННЯ ТА ПОВІДОМЛЕННЯ

(a) вимагати схвалення кожного віддаленого сеансу технічного обслуговування [*Призначення: персоналом або роллю, що визначила організація*];

(b) повідомити [*Призначення: персонал або ролі, що визначила організація*] про дату та час запланованого віддаленого обслуговування.

Рекомендації з реалізації: Сповіщення може здійснюватися технічним персоналом. Затвердження віддалених сесій технічного обслуговування здійснюється організаційним персоналом, який має достатню підготовку в галузі інформаційної безпеки та знання для визначення відповідності запропонованого обслуговування.

Пов'язані заходи: Немає.

(6) ВІДДАЛЕНЕ ОБСЛУГОВУВАННЯ - КРИПТОГРАФІЧНИЙ ЗАХИСТ

Запровадити криптографічні механізми для захисту цілісності та конфіденційності віддаленого обслуговування та діагностичних комунікацій.

Рекомендації з реалізації: Неспроможність захистити віддалені комунікації для технічного обслуговування та діагностики може призвести до того, що неавторизовані особи отримають доступ до організаційної інформації. Несанкціонований доступ під час сеансів віддаленого обслуговування може призвести до різноманітних ворожих дій, включаючи вставку шкідливого коду, несанкціоновану зміну параметрів системи та витік організаційної інформації. Такі дії можуть призвести до втрати або деградації місії або бізнес-можливостей.

Пов'язані заходи: SC-8, SC-12, SC-13.

(7) ВІДДАЛЕНЕ ОБСЛУГОВУВАННЯ - ПЕРЕВІРКА ВІДДАЛЕНОГО РОЗ'ЄДНАННЯ

Реалізувати перевірку віддаленого роз'єднання в разі припинення віддалених сеансів обслуговування та діагностики.

Рекомендації з реалізації: Перевірка розриву з'єднання після завершення обслуговування гарантує, що з'єднання, встановлені під час сеансів віддаленого обслуговування та діагностики, були розірвані і більше не доступні для використання.

Пов'язані заходи: AC-12.

Посилання: FIPS Publications 140-2, 197, 201. [FIPS 140-3], [FIPS 197], [FIPS 201-2], [SP 800-63-3], [SP 800-88].

## MA-5 ТЕХНІЧНИЙ ПЕРСОНАЛ

Заходи захисту:

a. Встановити процедуру авторизації технічного персоналу та вести перелік авторизованих організацій технічного обслуговування або персоналу.

b. Перевіряти, що персонал, який не супроводжується та виконує технічне

обслуговування в системі, має необхідні дозволи на доступ.

c. Визначити персонал організації з необхідними повноваженнями щодо доступу та технічною компетенцією для нагляду за персоналом з технічного обслуговування, який не має необхідних дозволів на доступ.

Рекомендації з реалізації: Цей захід безпеки застосовується до осіб, які виконують технічне або програмне обслуговування в системах організації, тоді як PE-2 стосується фізичного доступу осіб. Особи, які раніше не були визначені як уповноважений персонал з технічного обслуговування (виробники інформаційних технологій, постачальники та консультанти) можуть потребувати привілейованого доступу до систем організації при проведенні заходів обслуговування. На підставі оцінок ризику організації можуть видавати тимчасові повноваження цим особам. Тимчасові повноваження можуть бути одноразовими або дуже обмеженими.

Пов'язані заходи: AC-2, AC-3, AC-5, AC-6, IA-2, IA-8, MA-4, MP-2, PE-2, PE-3, PS-7, RA-3.

Посилення заходів:

(1) ТЕХНІЧНИЙ ПЕРСОНАЛ - ОСОБИ БЕЗ НАЛЕЖНОГО ДОСТУПУ

(a) Реалізувати процедури залучення персоналу з технічного обслуговування, який не має відповідних дозволів (допуску) або не є громадянами України, які (процедури) містять такі вимоги:

(1) обслуговуючий персонал, що не має необхідних прав доступу, рівня допуску, або офіційного затвердженого доступу, повинен супроводжуватися та бути під наглядом уповноваженого організацією персоналу, з необхідним рівнем допуску, а також мати відповідну технічну кваліфікацію для виконання технічного обслуговування та діагностичних заходів у системі;

(2) перед тим, як розпочати технічне обслуговування або діагностику персоналом, який не має необхідних прав допуску, рівня допуску або офіційного затвердженого доступу, упевнитися, що всі компоненти енергонезалежного зберігання інформації в системі очищуються, а всі енергонезалежні носії видаляються або фізично відключаються від системи та надійно захищаються.

(b) Розробити та впровадити альтернативні заходи безпеки, якщо компонент системи не може бути очищено, вилучено або відключено від системи.

Рекомендації з реалізації: Це посилення стосується осіб, які не мають відповідних дозволів (допуску) або не є громадянами України, яким не дозволений доступ до будь-якої секретної або контрольованої некласифікованої інформації, що міститься в системах організації. Процедури використання обслугового персоналу мають бути задокументовані в планах безпеки систем.

Пов'язані заходи: MP-6, PL-2.

(2) ТЕХНІЧНИЙ ПЕРСОНАЛ - ОФОРМЛЕННЯ ДОПУСКУ ДЛЯ СИСТЕМ, ЩО ОБРОБЛЯЮТЬ ІНФОРМАЦІЮ З ОБМЕЖЕНИМ ДОСТУПОМ

Переконатися, що персонал, який виконує технічне обслуговування та

діагностику в системі, що обробляє, зберігає або передає інформацію з обмеженим доступом, має рівень допуску та офіційне схвалення на доступ для найвищого рівня секретності та для всієї інформації в системі.

Рекомендації з реалізації: Персонал, який проводить технічне обслуговування систем організації, може мати доступ до інформації з обмеженим доступом під час виконання робіт з технічного обслуговування. Щоб зменшити ризики, організація використовує персонал, який має допуск відповідний до рівня секретності інформації, що зберігається в системі.

Пов'язані заходи: PS-3.

(3) ТЕХНІЧНИЙ ПЕРСОНАЛ - ВИМОГИ ДО ГРОМАДЯНСТВА

Переконатися, що працівники, які виконують технічне обслуговування та діагностичні заходи з обробки, зберігання або передачі таємної інформації, є громадянами України.

Рекомендації з реалізації: Персонал, який здійснює технічне обслуговування систем організації, може мати доступ до секретної інформації під час виконання робіт з технічного обслуговування. Якщо доступ до до секретної інформації в системах обмежений організації для громадян України, таке ж обмеження поширюється і на персонал, який виконує технічне обслуговування цих систем.

Пов'язані заходи: PS-3.

(4) ТЕХНІЧНИЙ ПЕРСОНАЛ - ІНОЗЕМНІ ГРОМАДЯНИ

Переконайтеся, що:

(a) іноземні громадяни з відповідним рівнем допуску залучаються для проведення технічного обслуговування та діагностичних робіт у системах, що обробляють інформацію з обмеженим доступом тільки тоді, коли ці системи спільно належать і експлуатуються урядами України та закордонних союзників, або належать та експлуатуються виключно іноземними союзними урядами;

(b) схвалення, згоди та додаткові умови експлуатації, що стосуються залучення іноземних громадян для проведення робіт з технічного обслуговування та діагностики систем, що обробляють інформацію з обмеженим доступом, повністю задокументовані в Меморандумі про угоду.

Рекомендації з реалізації: Персонал, який проводить технічне обслуговування та діагностику систем організації, може мати доступ до секретної інформації. Якщо особам, які не є громадянами України, дозволено виконувати роботи з технічного обслуговування та діагностики в системах з обемеженим доступом, то необхідна додаткова перевірка, щоб гарантувати, що угоди та обмеження не порушуються.

Пов'язані заходи: PS-3.

(5) ТЕХНІЧНИЙ ПЕРСОНАЛ - НЕСИСТЕМНЕ ОБСЛУГОВУВАННЯ

Переконатися, що персонал, який не супроводжується та здійснює ремонтні роботи, не пов'язаний безпосередньо із системою, але перебуває фізично

близько від системи, має необхідні дозволи на доступ.

Рекомендації з реалізації: До персоналу, що здійснює ремонтні роботи, які не пов'язані безпосередньо із системою, належить, наприклад, персонал для охорони.

Пов'язані заходи: Немає.

Посилання: Немає.

## MA-6 СВОЄЧАСНЕ ОБСЛУГОВУВАННЯ

Заходи захисту:
Отримати технічну підтримку та/або запасні частини для [*Призначення: визначених організацією компонентів системи*] в межах [*Призначення: визначеного організацією періоду часу*] у разі відмови.

Рекомендації з реалізації: Організації мають визначати найбільш критичні компоненти системи та ключові посадові особи. Дії для отримання технічної підтримки зазвичай передбачають наявність відповідних договорів.

Пов'язані заходи: CM-8, CP-2, CP-7, RA-7, SA-12, SA-15, SI-13, SR-2, SR-3, SR-4.

Посилення заходів:

(1) СВОЄЧАСНЕ ОБСЛУГОВУВАННЯ - ПРОФІЛАКТИЧНЕ ОБСЛУГОВУВАННЯ

Здійснювати профілактичне обслуговування [*Призначення: визначених організацією компонентів системи*] у [*Призначення: визначені організацією часові інтервали*].

Рекомендації з реалізації: Профілактичне обслуговування охоплює активний огляд і перевірку компонентів системи для підтримки обладнання та устаткування у задовільному робочому стані. Таке технічне обслуговування передбачає: систематичне обстеження, випробування, вимірювання, налаштування, заміну деталей, виявлення та виправлення несправностей, що виникають, або до того як вони виникнуть. Основна мета профілактичного обслуговування — уникнути/пом'якшити наслідки відмов обладнання. Профілактичне обслуговування призначене для збереження та відновлення надійності обладнання шляхом заміни зношених компонентів до їх виходу з ладу. Методи визначення того, які профілактичні (або інші) політики управління відмовами застосовуються, містять, наприклад, оригінальні рекомендації виробника обладнання, статистичні записи про несправності, вимоги кодексів, законодавства чи нормативно-правових актів у межах юрисдикції, висновки експертів тощо.

Пов'язані заходи: Немає.

(2) СВОЄЧАСНЕ ОБСЛУГОВУВАННЯ - ПЛАНОВЕ ТЕХНІЧНЕ ОБСЛУГОВУВАННЯ

Здійснювати планове технічне обслуговування [*Призначення: визначених організацією компонентів системи*] у [*Призначення: визначені організацією*

*часові інтервали*].

Рекомендації з реалізації: Планове обслуговування або поточне обслуговування має на меті оцінювання стану обладнання зі здійсненням періодичного або постійного (онлайнового) моніторингу стану обладнання. Метою планового обслуговування є проведення технічного обслуговування в запланований момент часу, коли діяльність з технічного обслуговування є найбільш економічною і до того, як обладнання втратить працездатність. Цей підхід може використовувати принципи контролю статистичних процесів для визначення найбільш прийнятного часу для проведення технічного обслуговування. Більшість планових перевірок технічного обслуговування проводяться під час роботи обладнання, що дозволяє мінімізувати порушення нормальної роботи системи. Планове обслуговування може забезпечити значну економію та більшу надійність системи.

Пов'язані заходи: Немає.

(3) СВОЄЧАСНЕ ОБСЛУГОВУВАННЯ - АВТОМАТИЗОВАНА ПІДТРИМКА ПЛАНОВОГО ТЕХНІЧНОГО ОБСЛУГОВУВАННЯ

Використовувати автоматизовані механізми для передачі даних планового технічного обслуговування до комп'ютеризованої системи управління обслуговуванням [*Призначення: автоматизовані засоби визначені організацією*].

Рекомендації з реалізації: Комп'ютеризована система управління технічним обслуговуванням підтримує базу даних з інформацією про заходи з технічного обслуговування та автоматизує обробку даних про стан обладнання для планування та звітності.

Пов'язані заходи: Немає.

## МА-7 ТЕХНІЧНЕ ОБСЛУГОВУВАННЯ В ПОЛЬОВИХ УМОВАХ

Обмежити або заборонити технічне обслуговування в польових умовах [*Призначення: визначені організацією системи або системні компоненти*] до [*Призначення: визначені організацією довірені засоби технічного обслуговування*]

Рекомендації з реалізації: Технічне обслуговування в польових умовах — це тип технічного обслуговування системи або компонента системи після того, як систему або компонент було розгорнуто в певному місці (тобто в робочому середовищі). У деяких випадках польове технічне обслуговування (тобто локальне технічне обслуговування на об'єкті) може не виконуватися з таким самим ступенем якості або з такими ж перевірками контролю якості, як технічне обслуговування у стандартних умовах. Для критично важливих систем, визначених організацією, може виникнути необхідність обмежити або заборонити польове технічне обслуговування на місці та вимагати, щоб таке технічне обслуговування проводилося на надійних об'єктах із додатковими заходами захисту.

Пов'язані заходи: МА-2, МА-4, МА-5.

Посилення заходів: Немає.

Посилання: Немає.

## 10.10 Клас заходів захисту MP — ЗАХИСТ НОСІЇВ ІНФОРМАЦІЇ

### MP-1 ПОЛІТИКА ТА ПРОЦЕДУРИ ЩОДО ЗАХИСТУ НОСІЇВ ІНФОРМАЦІЇ

Заходи захисту:

a. Розробити, задокументувати та поширити серед [*Призначення: визначеного організацією персоналу або посад*]:

   1. політику захисту носіїв інформації, яка:

      (a) містить мету, сферу застосування, ролі, обов'язки, відповідальність керівництва, координацію між організаційними підрозділами та систему контролю відповідності (complaince);

      (b) відповідає чинному законодавству, виконавчим наказам, директивам, нормам, політикам, стандартам та керівним принципам;

   2. процедури, які сприяють здійсненню політики та заходів захисту носіїв інформації.

b. Призначити [*Призначення: визначену організацією посадову особу*] для управління розробкою, документування, та розповсюдження політики та процедурами захисту носіїв інформації.

c. Переглядати та оновлювати чинну систему захисту носіїв інформації:

   1. поточну політику захисту носіїв інформації [*Призначення: з визначеною організацією частотою*];

   2. поточні процедури захисту носіїв інформації [*Призначення: з визначеною організацією частотою*].

Рекомендації з реалізації: Цей захід захисту стосується встановлення політики та процедур для ефективного здійснення заходів та їх посилень у класі MP. Стратегія управління ризиками є важливим фактором у встановленні політики та процедур. Комплексна політика та процедури допомагають забезпечити безпеку та приватність. За наявності політики, а також планів захисту інформації та персональних даних на рівні організації, конкретні системні політики та процедури можуть бути не потрібні. Політика може бути внесена до складу загальної політики безпеки та приватності або може бути представлена кількома політиками (у випадках складної архітектури). Процедури описують, як має реалізуватися політика чи заходи захисту та як вони можуть бути спрямовані на персонал або роль, що є об'єктом процедури. Процедури можуть бути задокументовані в планах захисту інформації та персональних даних (як один або декілька документів).

Пов'язані заходи: PM-9, PS-8, SI-12.

Посилення заходів: Немає.

Посилання: [OMB A-130], [SP 800-12], [SP 800-30], [SP 800-39], [SP 800-100].

## MP-2 ДОСТУП ДО НОСІЇВ ІНФОРМАЦІЇ

Заходи захисту:

Обмежити доступ до [*Призначення: визначених організацією типів цифрових та/або нецифрових носіїв інформації*] [*Призначення: визначеним організацією персоналом або ролями*].

Рекомендації з реалізації: До носіїв системи належать як цифрові, так і нецифрові носії. До цифрових носіїв належать: дискети, магнітні стрічки, зовнішні/знімні жорсткі диски, флешки, компакт-диски, цифрові відеодиски та інші. До нецифрових носіїв належать, наприклад, папір і мікрофільми. Обмеження доступу до нецифрових носіїв охоплює, наприклад, заборону доступу до медичних записів пацієнтів (за винятком уповноважених медичних працівників). Обмеження доступу до цифрових носіїв інформації охоплює, наприклад, обмеження доступу до проєктних специфікацій дизайну, що зберігаються на компакт-дисках у медіатеці, керівнику проєкту та особам з команди розробників.

Пов'язані заходи: AC-19, AU-9, CP-2, CP-9, CP-10, MA-5, MP-6, MP-4, PE-2, PE-3, SC-13, SC-34, SI-12.

Посилення заходів:

(1) ДОСТУП ДО НОСІЇВ ІНФОРМАЦІЇ - АВТОМАТИЗОВАНИЙ ОБМЕЖЕНИЙ ДОСТУП

[Вилучено: Включено до MP-4(2)].

(2) ДОСТУП ДО НОСІЇВ ІНФОРМАЦІЇ - КРИПТОГРАФІЧНИЙ ЗАХИСТ

[Вилучено: Включено до SC-28(1)].

Посилання: FIPS Publication 199, [OMB A-130], [SP 800-111].

## MP-3 МАРКУВАННЯ НОСІЇВ ІНФОРМАЦІЇ

Заходи захисту:

a. Наносити на носії інформації маркування, що вказують на обмеження поширення, обробки, а також застереження та відповідні мітки безпеки (якщо такі є) інформації.

b. Звільнити [*Призначення: визначені організацією типи носіїв системи*] від маркування, якщо носії залишаються в межах [*Призначення: визначених організацією контрольованих зон*].

Рекомендації з реалізації: Маркування безпеки стосується застосування або використання атрибутів безпеки стосовно внутрішніх структур даних всередині систем. Маркування безпеки, як правило, не вимагається для носіїв, що містять загальнодоступну інформацію. Однак деякі організації можуть вимагати відповідного маркування носіїв інформації, яке свідчить про те, що інформація є загальнодоступною. Маркування носіїв має здійснюватися відповідно до чинного законодавства.

Пов'язані заходи: AC-16, CP-9, MP-5, PE-22, SI-12.

Посилення заходів: Немає.

Посилання: FIPS Publication 199, [EO 13556], [32 CFR 2002].

## MP-4 ЗБЕРІГАННЯ НОСІЇВ ІНФОРМАЦІЇ

Заходи захисту:

a. Фізично контролювати та безпечно зберігати [*Призначення: визначені організацією типи цифрових та/або нецифрових носіїв інформації*] в межах [*Призначення: визначених організацією контрольованих зон*].

b. Захищати системні носії, які визначені в MP-4 до того часу, як носії знищуються або очищаються, з використанням затвердженого обладнання, методів та процедур.

Рекомендації з реалізації: Фізичний контроль носіїв містить, наприклад, проведення інвентаризації, контроль за місцем перебування носіїв тощо. Тип носія інформації, що використовується, має відповідати категорії безпеки або інформації, що зберігається на носії. Контрольовані зони — це зони, які забезпечують достатню фізичну та процедурну гарантію для задоволення вимог, встановлених для захисту інформації та систем. Зберігання носіїв інформації, на яких зберігається загальнодоступна інформація, вимагає меншого рівня гарантій. У цих ситуаціях фізичний контроль доступу може самостійно забезпечити належний захист.

Пов'язані заходи: AC-19, CP-2, CP-6, CP-9, CP-10, MP-2, MP-7, PE-3, PL-2, SC-13, SC-28, SC-34, SI-12, SC-12.

Посилення заходів:

(1) ЗБЕРІГАННЯ НОСІЇВ ІНФОРМАЦІЇ - КРИПТОГРАФІЧНИЙ ЗАХИСТ

[Вилучено: Включено до SC-28(1)].

(2) ЗБЕРІГАННЯ НОСІЇВ ІНФОРМАЦІЇ - АВТОМАТИЗОВАНИЙ ОБМЕЖЕНИЙ ДОСТУП

Впровадити автоматизовані механізми для обмеження доступу до зон зберігання носіїв інформації та для реєстрації спроб доступу та доступу, який надано.

Рекомендації з реалізації: До автоматизованих механізмів належать, наприклад, клавіатури, біометричні зчитувачі або зчитувачі карт на зовнішніх частинах зон.

Пов'язані заходи: AC-3, AU-2, AU-6, AU-9, AU-12, PE-3.

Посилання: FIPS Publication 199, [SP 800-56A], [SP 800-56B], [SP 800-56C], [SP 800-57-1], [SP 800-57-2], [SP 800-57-3], [SP 800-111].

## MP-5 ТРАНСПОРТУВАННЯ НОСІЇВ ІНФОРМАЦІЇ

Заходи захисту:

a. Захищати та контролювати [*Призначення: визначені організацією типи носіїв системи*] під час транспортування за межами контрольованих зон, використовуючи [*Призначення: визначені організацією заходи безпеки*].

b. Вести облік носіїв системи інформації під час транспортування за межами контрольованих зон.

c. Документувати дії, пов'язані з транспортуванням носіїв системи.

d. Обмежити діяльність уповноваженого персоналу, пов'язану з транспортуванням носіїв системи.

Рекомендації з реалізації: Фізичні та технічні засоби захисту носіїв інформації мають відповідати категорії безпеки інформації, що зберігається на носії. До засобів захисту носіїв під час транспортування належать захищені контейнери та криптографічні методи захисту. Криптографічні методи можуть забезпечувати захист конфіденційності й цілісності, залежно від використовуваних механізмів. Діяльність, що пов'язана з транспортуванням, охоплює: власне транспортування, підготовку до транспортування та підготовку до експлуатації після транспортування. До транспортування може бути залучений зовнішній персонал. Процес транспортування має бути відстежуваним (до засобів відстежування можуть належати процедури протоколювання, використання механізмів запобігання та виявлення можливої підробки). Організації мають встановлювати процедури документування відповідно до процесів і носіїв інформації організації, які транспортуються.

Пов'язані заходи: AC-7, AC-19, CP-2, CP-9, MP-3, MP-4, PE-16, PL-2, SC-13, SC-28, SC-34, SC-12.

Посилення заходів:

(1) ТРАНСПОРТУВАННЯ НОСІЇВ ІНФОРМАЦІЇ - ЗАХИСТ ПОЗА КОНТРОЛЬОВАНИМИ ЗОНАМИ

[Вилучено: Включено до MP-5].

(2) ТРАНСПОРТУВАННЯ НОСІЇВ ІНФОРМАЦІЇ - ДОКУМЕНТУВАННЯ ДІЙ

[Вилучено: Включено до MP-5].

(3) ТРАНСПОРТУВАННЯ НОСІЇВ ІНФОРМАЦІЇ - ЗБЕРІГАЧІ

Залучати визначених зберігачів інформації під час транспортування носіїв системи за межі контрольованих зон.

Рекомендації з реалізації: Визначені зберігачі надають організаціям конкретні точки зв'язку під час транспортування носіїв інформації.

Пов'язані заходи: Немає.

(4) ТРАНСПОРТУВАННЯ НОСІЇВ ІНФОРМАЦІЇ - КРИПТОГРАФІЧНИЙ ЗАХИСТ

[Вилучено: Включено до SC-28(1)].

Посилання: FIPS Publication 199, [SP 800-60-1], [SP 800-60-2].

## MP-6 ЗНИЩЕННЯ ІНФОРМАЦІЇ НА НОСІЯХ ІНФОРМАЦІЇ

Заходи захисту:

a. Очищувати [*Призначення: визначені організацією системні носії*] перед утилізацією, випуском за межі організаційного контролю, або перед повторним використанням [*Призначення: методами та процедурами очищення, визначеними організацією*].

b. Використовувати механізми очищення зі стійкістю та цілісністю, що відповідає категорії безпеки або рівню секретності інформації.

Рекомендації з реалізації: Цей захід безпеки поширюється на всі системні носії інформації як цифрові, так і нецифрові, інформація на яких має бути знищена незалежно від того, чи вважається носій знімним. Прикладами носіїв є: цифрові носії інформації, що містяться в сканерах, копіювальних пристроях, принтерах, ноутбуках, робочих станціях, мережевих компонентах, мобільних пристроях; та нецифрові носії інформації — такі як папір і мікрофільми. Процес очищення має видаляти інформацію з носія інформації, щоб її неможливо було отримати чи відновити. Методи очищення запобігають розголошенню інформації стороннім особам у разі, коли такі носії використовуються повторно або передаються на утилізацію (видалення, форматування, криптографічне забілювання тощо). Організації встановлюють механізми очищення відповідно до категорії безпеки інформації, яка розміщена на носіях інформації.

Пов'язані заходи: AC-3, AC-7, AU-11, MA-2, MA-3, MA-4, MA-5, SI-12, SI-18, PM-22, SI-19, SR-11.

Посилення заходів:

(1) ЗНИЩЕННЯ ІНФОРМАЦІЇ НА НОСІЯХ ІНФОРМАЦІЇ - ПЕРЕГЛЯД, ЗАТВЕРДЖЕННЯ, ВІДСТЕЖЕННЯ, ДОКУМЕНТУВАННЯ ТА ПЕРЕВІРКА

Переглядати, затверджувати, відстежувати, документувати та перевіряти очищення носіїв інформації та дії з їх утилізації.

Рекомендації з реалізації: Організації переглядають і затверджують перелік носіїв інформації, які підлягають очищенню для забезпечення дотримання політики збереження записів. Дії відстеження та документування охоплюють: складання переліку персоналу, який переглядає і затверджує заходи щодо очищення; види носіїв інформації; конкретні файли, що зберігаються на носії; застосовувані методи очищення; дату й час проведення очищення; персонал, який здійснив очищеннятощо. Організації перевіряють, чи було очищення носіїв інформації перед знищенням.

Пов'язані заходи: Немає.

(2) ЗНИЩЕННЯ ІНФОРМАЦІЇ НА НОСІЯХ ІНФОРМАЦІЇ - ПЕРЕВІРКА ОБЛАДНАННЯ

Перевіряти обладнання та процедури для очищення [*Призначення: з визначеною організацією частотою*], щоб переконатися в досягненні запланованого очищення.

Рекомендації з реалізації: Перевірка обладнання та процедур очищення може проводитися кваліфікованими й уповноваженими зовнішніми організаціями.

Пов'язані заходи: Немає.

(3) ЗНИЩЕННЯ ІНФОРМАЦІЇ НА НОСІЯХ ІНФОРМАЦІЇ - НЕРУЙНІВНІ МЕТОДИ

Застосовувати методи неруйнівного очищення до портативних запам'ятовувальних пристроїв перед підключенням таких пристроїв до системи за наступних обставин: [*Призначення: визначених організацією умов, що*

*вимагають очищення портативних запам'ятовувальних пристроїв*].

Рекомендації з реалізації: До портативних пристроїв зберігання даних відносяться зовнішні або знімні жорсткі диски (напр., твердотільні, магнітні), оптичні диски, магнітні або оптичні стрічки, пристрої флеш-пам'яті, карти флеш-пам'яті карти пам'яті та інші зовнішні або знімні диски. У портативні пристрої зберігання даних легко може бути вбудований зловмисний код. Багато таких пристроїв отримані з недостовірних джерел і можуть містити шкідливий код, який можна легко перенести в системи через порти USB чи інші портали входу. Рекомендується сканувати пристрої зберігання даних, проте процедура очищення забезпечує додаткову впевненість у тому, що такі пристрої не містять шкідливого коду. Організації розглядають можливість очищення портативних пристроїв зберігання даних, коли пристрої купуються у виробників або постачальників перед початком використанням.

Пов'язані заходи: Немає.

(4) ЗНИЩЕННЯ ІНФОРМАЦІЇ НА НОСІЯХ ІНФОРМАЦІЇ - КЕРОВАНА НЕСЕКРЕТНА ІНФОРМАЦІЯ

[Вилучено: Включено до MP-6].

(5) ЗНИЩЕННЯ ІНФОРМАЦІЇ НА НОСІЯХ ІНФОРМАЦІЇ - СЕКРЕТНА ІНФОРМАЦІЯ

[Вилучено: Включено до MP-6].

(6) ЗНИЩЕННЯ ІНФОРМАЦІЇ НА НОСІЯХ ІНФОРМАЦІЇ - ЗНИЩЕННЯ НОСІЇВ ІНФОРМАЦІЇ

[Вилучено: Включено до MP-6].

(7) ЗНИЩЕННЯ ІНФОРМАЦІЇ НА НОСІЯХ ІНФОРМАЦІЇ - ПОДВІЙНА АВТОРИЗАЦІЯ

Здійснювати подвійну авторизацію для очищення [*Призначення: визначених організацією носіїв системи*].

Рекомендації з реалізації: Організації використовують подвійну авторизацію для очищення, щоб гарантувати, що очищення носіїв інформації системи не може відбутися без участі двох технічно кваліфікованих осіб, які виконують призначене завдання. Особи, які проводять очищення носіїв інформації системи, повинні володіти достатніми навичками та досвідом для визначення чи відповідає запропонована процедура очищення чинним стандартам, політикам, і процедурам організації. Подвійна авторизація також повинна гарантувати, що очищення відбувається за призначенням, захищаючи від помилок і неправдивих заяв про виконання процедури очищення. Подвійна авторизація являє собою двоосібний контроль. Механізми подвійної авторизації вимагають схвалення двох уповноважених осіб для виконання дії. Щоб зменшити ризик змови, організація розглядає можливість ротації обов'язків подвійної авторизації з іншими особами.

Пов'язані заходи: AC-3, MP-2.

(8) ЗНИЩЕННЯ ІНФОРМАЦІЇ НА НОСІЯХ ІНФОРМАЦІЇ - ВІДДАЛЕНЕ ОЧИЩЕННЯ АБО СТИРАННЯ ІНФОРМАЦІЇ

Забезпечити віддалену можливість очищення або стирання інформації з [*Призначення: визначених організацією систем або компонентів системи*] або за: [*Призначення: визначених організацією умов*].

Рекомендації з реалізації: Це удосконалення забезпечує захист даних/інформації про організаційні системи та компоненти системи, якщо такі системи або компоненти отримані від сторонніх осіб. Для віддалених команд очищення/стирання вимагається надійна автентифікація. Функція очищення або стирання може бути реалізована різними способами, включно з, наприклад, перезаписом даних/інформації кілька разів або знищенням ключа, необхідного для розшифрування зашифрованих даних.

Пов'язані заходи: Немає.

Посилання: [32 CFR 2002], [OMB A-130], [NARA CUI], [FIPS 199], [SP 800-60-1], [SP 800-60-2], [SP 800-88], [SP 800-124], [IR 8023], [NSA MEDIA].

## MP-7 ВИКОРИСТАННЯ НОСІЇВ ІНФОРМАЦІЇ

Заходи захисту:

a. [*Вибір: обмежити; заборонити*] використання [*Призначення: визначених організацією типів носіїв системи*] на [*Призначення: визначені організацією системи або компоненти системи*], використовуючи [*Призначення: визначені організацією заходи безпеки*].

b. Заборонити використання портативних пристроїв зберігання даних в системах організації, якщо такі пристрої не мають визначеного власника.

Рекомендації з реалізації: Цей захід безпеки також застосовується до мобільних пристроїв. На відміну від MP-2, який обмежує доступ користувача до носіїв інформації, (MP-7) обмежує використання певних типів носіїв у системах, наприклад, обмежуючи/забороняючи використання флеш-накопичувачів або зовнішніх накопичувачів. Організації можуть використовувати технічні та нетехнічні засоби для обмеження використання носіїв інформації системи. Організації можуть обмежувати використання переносних пристроїв зберігання даних, наприклад, використовуючи фізичні перешкоди для запобігання доступу до певних зовнішніх портів, або відключити/видалити можливість вставляти, зчитувати чи записувати на такі пристрої. Організації можуть також обмежувати використання портативних пристроїв зберігання, обмеживши перелік дозволених до використання лише затвердженими пристроями, включно з, наприклад, пристроями, що надаються організацією, пристроями, наданими іншими затвердженими організаціями.

Пов'язані заходи: AC-19, AC-20, PL-4, PM-12, SC-34, SC-41.

Посилення заходів:

(1) ВИКОРИСТАННЯ НОСІЇВ ІНФОРМАЦІЇ - ЗАБОРОНА ВИКОРИСТАННЯ БЕЗ ВИЗНАЧЕНОГО ВЛАСНИКА

[Вилучено: Включено до MP-7].

(2) ВИКОРИСТАННЯ НОСІЇВ ІНФОРМАЦІЇ - ЗАБОРОНА ВИКОРИСТАННЯ СТІЙКИХ ДО ОЧИЩЕННЯ НОСІЇВ ІНФОРМАЦІЇ

Заборонити використання в системах організації засобів, що не піддаються очищенню.

Рекомендації з реалізації: Окремі типи носіїв не підтримують команди очищення; або якщо вони підтримуються, інтерфейси на цих пристроях не підтримуються стандартизовано.

Пов'язані заходи: MP-6.

Посилання: FIPS Publication 199, [SP 800-111].

## MP-8 ЗНИЖЕННЯ КАТЕГОРІЇ БЕЗПЕКИ НОСІЇВ ІНФОРМАЦІЇ

Заходи захисту:

a. Встановити [*Призначення: визначений організацією процес зниження категорії безпеки носіїв інформації*], який охоплює використання механізмів зниження грифа секретності носіїв інформації за стійкістю та цілісністю, що відповідає категорії безпеки або рівню секретності інформації.

b. Забезпечити, щоб процес зниження категорії безпеки носія відповідав категорії безпеки або рівню секретності інформації, яку потрібно видалити, а також рівню доступу потенційних одержувачів до інформації з меншим рівнем секретності.

c. Визначати [*Призначення: визначені організацією системні носії, що вимагають зниження категорії безпеки*].

d. Знижувати категорію безпеки визначеного носія за допомогою встановленого процесу.

Рекомендації з реалізації: Цей захід безпеки застосовується до всіх носіїв інформації системи — цифрових та нецифрових, — які можуть покидати межі організації. Процес пониження категорії безпеки носіїв інформації передбачає надійну передачу інформації з носія. Також можливе редагування змісту інформації на носії для пониження категорії безпеки.

Пов'язані заходи: Немає.

Посилення заходів:

(1) ЗНИЖЕННЯ КАТЕГОРІЇ БЕЗПЕКИ НОСІЇВ ІНФОРМАЦІЇ - ДОКУМЕНТУВАННЯ ПРОЦЕСУ

Документувати дії зі зниження категорії безпеки носіїв інформації.

Рекомендації з реалізації: При проведенні процедури пониження категорії безпеки носіїв інформації має бути задокументовано: ідентифікаційний номер носія; уповноважену особу, яка проводила процес пониження категорії безпеки; метод пониження та уповноважену особу, яка віддала розпорядження щодо

пониження категорії безпеки.

Пов’язані заходи: Немає.

(2) ЗНИЖЕННЯ КАТЕГОРІЇ БЕЗПЕКИ НОСІЇВ ІНФОРМАЦІЇ - ПЕРЕВІРКА ОБЛАДНАННЯ

Перевіряти обладнання та процедури заниження категорії безпеки [*Призначення: з визначеною організацією частотою*], щоб переконатися в досягненні запланованих заходів щодо зниження.

Рекомендації з реалізації: Немає.

Пов’язані заходи: Немає.

(3) ЗНИЖЕННЯ КАТЕГОРІЇ БЕЗПЕКИ НОСІЇВ ІНФОРМАЦІЇ - КРИТИЧНА ІНФОРМАЦІЯ

Знижувати категорію безпеки носіїв, що містять [*Призначення: визначену організацією критичну інформацію*] до рівня публічного доступу.

Рекомендації з реалізації: Для пониження категорії безпеки носіїв інформації використовуйте затверджені інструменти, методи і процедури очищення.

Пов’язані заходи: Немає.

(4) ЗНИЖЕННЯ КАТЕГОРІЇ БЕЗПЕКИ НОСІЇВ ІНФОРМАЦІЇ - ТАЄМНА ІНФОРМАЦІЯ

Знижувати категорію безпеки носіїв, що містять секретну інформацію, до категорії безпеки для осіб без необхідних дозволів на доступ.

Рекомендації з реалізації: Зниження категорії безпеки носіїв інформації має відбуватися відповідно до затверджених положень з використанням надійних методів та інструментів.

Пов’язані заходи: Немає.

Посилання: [32 CFR 2002], [NSA MEDIA].

## 10.11 Клас заходів захисту PE — ФІЗИЧНИЙ ЗАХИСТ І ЗАХИСТ РОБОЧОГО СЕРЕДОВИЩА

### PE-1 ПОЛІТИКА ТА ПРОЦЕДУРИ ФІЗИЧНОГО ЗАХИСТУ ТА ЗАХИСТУ РОБОЧОГО СЕРЕДОВИЩА

Заходи захисту:

a. Розробляє, документує та поширює серед [*Призначення: визначеного організацією персоналу або ролей*]:

   1. політику в галузі фізичного захисту та захисту робочого середовища, яка:

      (a) містить мету, сферу застосування, ролі, обов'язки, відповідальність керівництва, координацію між організаційними підрозділами та систему контролю відповідності (complaince);

      (b) відповідає чинному законодавству, виконавчим наказам, директивам, нормам, політикам, стандартам і керівним принципам;

   2. процедури, які сприяють виконанню політики та заходів у галузі фізичного захисту та захисту робочого середовища.

b. Призначити [*Призначення: визначену організацією посадову особу*] для управління політикою та процедурами фізичного захисту та захисту робочого середовища.

c. Переглядати та оновлювати:

   1. поточну політику фізичного захисту та захисту робочого середовища [*Призначення: з визначеною організацією частотою*];

   2. поточні процедури фізичного захисту та захисту робочого середовища [*Призначення: з визначеною організацією частотою*].

Рекомендації з реалізації: Цей захід захисту стосується встановлення політики та процедур для ефективного здійснення заходів та їх посилень у класі PE. Стратегія управління ризиками є важливим фактором у встановленні політики та процедур. Комплексна політика та процедури допомагають забезпечити безпеку та приватність. За наявності політики, а також планів захисту інформації та персональних даних на рівні організації, конкретні системні політики та процедури можуть бути не потрібні. Політика може бути внесена до складу загальної політики безпеки та приватності або може бути представлена кількома політиками (у випадках складної архітектури). Процедури описують, як має реалізуватися політика чи заходи захисту та як вони можуть бути спрямовані на персонал або роль, що є об'єктом процедури. Процедури можуть бути задокументовані в планах захисту інформації та персональних даних (як один або декілька документів).

Пов'язані заходи: AT-3, PM-9, PS-8, SI-12.

Посилення заходів: Немає.

Посилання: [SP 800-12], [SP 800-30], [SP 800-39], [SP 800-100].

### PE-2 АВТОРИЗАЦІЯ ФІЗИЧНОГО ДОСТУПУ

Заходи захисту:

a. Розробити, затвердити та вести перелік осіб, які мають право авторизованого доступу до об'єкта, де перебуває система.

b. Надати повноваження для доступу до об'єкта.

c. Переглядати список доступу, у якому закріплений перелік персоналу або ролей, яким дозволений санкціонований доступ до об'єкта [*Призначення: з визначеною організацією частотою*].

d. Видалити персонал зі списку доступу до об'єкта, коли такий доступ більше не потрібний.

Рекомендації з реалізації: Цей захід застосовується до працівників і відвідувачів. Особи, які мають постійні посвідчення фізичного доступу, не вважаються відвідувачами. Вхідні дані авторизації містять, наприклад, значки, ідентифікаційні картки та смарткарти. Організації визначають необхідний рівень авторизації відповідно до чинного законодавства, політики, стандартам та інструкцій. Цей захід захисту застосовується лише до територій всередині об'єктів, які не були визначені як загальнодоступні.

Пов'язані заходи: AT-3, AU-9, IA-4, MA-5, MP-2, PE-3, PE-4, PE-5, PE-8, PM-12, PS-3, PS-4, PS-5, PS-6.

Посилення заходів:

(1) АВТОРИЗАЦІЯ ФІЗИЧНОГО ДОСТУПУ - ДОСТУП НА ОСНОВІ ПОСАДИ АБО РОЛІ

Авторизувати фізичний доступ до об'єкта, де перебуває система, на основі ролі або посади.

Рекомендації з реалізації: Доступ до об'єкта на основі ролі включає доступ уповноваженого постійного персоналу та включає регулярне/постійне технічне обслуговування, чергових офіцерів та медичний персонал.

Пов'язані заходи: AC-2, AC-3, AC-6.

(2) АВТОРИЗАЦІЯ ФІЗИЧНОГО ДОСТУПУ - ДВІ ФОРМИ ІДЕНТИФІКАЦІЇ

Вимагати дві форми ідентифікації від [*Призначення: визначеного організацією списку прийнятних форм ідентифікації*] для доступу відвідувачів до об'єкта, де перебуває система.

Рекомендації з реалізації: До форм ідентифікації належать, наприклад, ідентифікація за допомогою паспорту, посвідчення особистості, посвідчення водія. Для отримання доступу до об'єктів за допомогою автоматизованих механізмів організації можуть використовувати картки доступу, ключові картки, PIN-коди та біометричні дані.

Пов'язані заходи: IA-2, IA-4, IA-5.

(3) АВТОРИЗАЦІЯ ФІЗИЧНОГО ДОСТУПУ - ОБМЕЖЕННЯ ДОСТУПУ БЕЗ СУПРОВОДУ

Заборонити доступ без супроводу до об’єкта, де перебуває система, персоналу з [*Вибір (один або більше): рівень допуску для всієї інформації, що міститься в системі; авторизація офіційного доступу до всієї інформації, що міститься в системі; необхідність доступу до всієї інформації, що міститься в системі*; [*Призначення: визначені організацією повноваження*]].

Рекомендації з реалізації: Через надзвичайно чутливий характер інформації з обмеженим доступом, що зберігається в певних установах, важливо, щоб особи, які не мають дозволу доступу, супроводжувалися відповідальними авторизованими особами.

Пов’язані заходи: PS-2, PS-6.

Посилання: [FIPS 201-2], [SP 800-73-4], [SP 800-76-2], [SP 800-78-4].

## PE-3 КЕРУВАННЯ ФІЗИЧНИМ ДОСТУПОМ

Заходи захисту:

a. Забезпечити авторизацію фізичного доступу за адресою [*Призначення: визначені організацією точки входу й виходу до об’єкта, де перебуває система*] шляхом:

   1. перевірки індивідуального дозволу доступу до об’єкта;

   2. управління входом та виходом на об’єкт за допомогою [*Вибір (один або кілька):* [*Призначення: визначених організацією фізичних систем або пристроїв контролю доступу*]*; охорони*].

b. Вести журнали контролю фізичного доступу для [*Призначення: визначені організацією точки входу/виходу*].

c. Забезпечити [*Призначення: визначені організацією заходи захисту*] для контролю доступу в зони всередині об’єкта, позначені як загальнодоступні.

d. Супроводжувати відвідувачів та контролювати активність відвідувачів [*Призначення: визначені організацією умови, що вимагають супроводу відвідувачів і моніторингу*].

e. Забезпечити захист ключів, кодів доступу та інших пристроїв фізичного доступу.

f. Проводити інвентаризацію [*Призначення: визначених організацією пристроїв фізичного доступу*] кожен [*Призначення: визначена організацією частота*].

g. Здійснювати зміну кодів доступу та ключів [*Призначення: з визначеною організацією частотою*], коли ключі втрачені, комбінації скомпрометовані або фізичні особи переведені чи звільнені.

Рекомендації з реалізації: Цей захід застосовується до працівників і відвідувачів. Особи, які мають постійні посвідчення фізичного доступу, не вважаються відвідувачами. До пристроїв фізичного доступу належать, наприклад, клавіші, замки та зчитувачі карт. Фізичні системи контролю доступу мають відповідати чинному законодавству. Організації можуть вести журнали аудиту (процедурні та/або автоматизовані). До фізичних точок доступу належать точки доступу до об’єктів,

внутрішні точки доступу до систем або компонентів системи, що потребують додаткових засобів захисту.

Пов'язані заходи: AT-3, AU-2, AU-6, AU-9, AU-13, CP-10, IA-3, IA-8, MA-5, MP-2, MP-4, PE-2, PE-4, PE-5, PE-8, PS-2, PS-3, PS-7, RA-3, SC-28, SI-4, SR-3.

Посилення заходів:

(1) КЕРУВАННЯ ФІЗИЧНИМ ДОСТУПОМ - ДОСТУП ДО СИСТЕМИ

Застосовувати авторизацію фізичного доступу до системи на додаток до керування фізичного доступу до об'єкта в [*Призначення: визначені організацією фізичні приміщення, що містять один або більше компонентів системи*].

Рекомендації з реалізації: Це посилення забезпечує додаткову фізичну безпеку для тих областей, що розташовані в приміщеннях, з великою кількістю компонентів системи.

Пов'язані заходи: PS-2.

(2) КЕРУВАННЯ ФІЗИЧНИМ ДОСТУПОМ - МЕЖІ ОБ'ЄКТУ ТА СИСТЕМИ

Здійснювати перевірку безпеки [*Призначення: з визначеною організацією частотою*] на фізичній межі об'єкта або системи для видалення інформації або вилучення компонентів системи.

Рекомендації з реалізації: Організації мають визначати ступінь, частоту та/або випадковість перевірок безпеки для адекватного зменшення ризику, пов'язаного з ексфільтрацією.

Пов'язані заходи: AC-4, SC-7.

(3) КЕРУВАННЯ ФІЗИЧНИМ ДОСТУПОМ - БЕЗПЕРЕРВНА ОХОРОНА

Забезпечити цілодобову безперервну охорону для контролю доступу [*Призначення: визначені організацією фізичні точки доступу*] до об'єкта, де перебуває система.

Рекомендації з реалізації: Розміщення охорони у місцях фізичного доступу до об'єкту забезпечує організації можливість швидкого реагування. Охорона також надає можливість для спостереженням за людьми в зоні об'єктів, не охоплених відеоспостереженням.

Пов'язані заходи: CP-6, CP-7, PE-6.

(4) КЕРУВАННЯ ФІЗИЧНИМ ДОСТУПОМ – ШАФИ З БЛОКУВАННЯМ

Використовувати шафи з блокуванням для захисту [*Призначення: визначених організацією компонентів системи*] від несанкціонованого фізичного доступу.

Рекомендації з реалізації: Найбільший ризик несанкціонованого використання портативних пристроїв, таких як смартфонів, планшетів та ноутбуків – це крадіжка. Організації можуть використовувати шафи з блокуванням, щоб зменшити або усунути ризик крадіжки обладнання. Такі шафи бувають різних розмірів, від тих що захищають один ноутбук, до шаф, які можуть захистити

декілька серверів, комп'ютерів та периферійних пристроїв.

Пов'язані заходи: Немає.

(5) КЕРУВАННЯ ФІЗИЧНИМ ДОСТУПОМ - ЗАХИСТ ВІД ЗЛОМУ

Застосовувати [*Призначення: визначені організацією заходи захисту*] для [*Вибір (один або більше): виявлення; запобігання*] фізичної підробки або підміни [*Призначення: визначених організацією апаратних компонентів*] всередині системи.

Рекомендації з реалізації: Має бути забезпечене виявлення та запобігання несанкціонованому втручанню або несанкціонованому впливу в апаратні компоненти. У заходах щодо виявлення та запобігання можуть використовуватися різні типи технологій протидії несанкціонованому впливу.

Пов'язані заходи: SA-16, SR-9, SR-11.

(6) КЕРУВАННЯ ФІЗИЧНИМ ДОСТУПОМ - ТЕСТУВАННЯ НА МОЖЛИВІСТЬ ПРОНИКНЕННЯ

[Вилучено: включено до CA-8].

(7) КЕРУВАННЯ ФІЗИЧНИМ ДОСТУПОМ - ФІЗИЧНІ ПЕРЕШКОДИ

Обмежити доступ за допомогою фізичних перешкод.

Рекомендації з реалізації: До фізичних перешкод належать, наприклад, кронштейни, бетонні плити, стінки та гідравлічні бар'єри.

Пов'язані заходи: Немає.

Посилання: FIPS Publication 201.

(8) КЕРУВАННЯ ФІЗИЧНИМ ДОСТУПОМ - КОНТРОЛЬ ДОСТУПУ У ВЕСТИБЮЛІ (ХОЛІ)

Запроваджуйте контроль доступу у вестибюлі в [*Завдання: місця, визначені організацією в межах закладу*].

Рекомендації з реалізації: Контроль доступу у вестибюлі є частиною фізичної системи контролю доступу між двома наборами блокованих дверей. Вестибюлі призначені для запобігання проникненню сторонніх осіб за авторизованими особами в приміщення з контрольованим доступом. Відсутність такого контролю може призвести до несанкціонованого доступу до об'єкта. Блокувальні дверні контролери можна використовувати для обмеження кількості осіб, які входять до контрольованих точок доступу, і для забезпечення зон утримання під час перевірки авторизації фізичного доступу. Блокувальні дверні контролери можуть бути повністю автоматизованими (тобто контролювати відкриття та закриття дверей) або частково автоматизованими (тобто можна використовувати охоронців для контролю кількості осіб, які входять у зону утримання).

Пов'язані заходи: Немає.

Посилання: [FIPS 201-2], [SP 800-73-4], [SP 800-76-2], [SP 800-78-4], [SP 800-116].

## PE-4 КОНТРОЛЬ ДОСТУПУ ДО ДЖЕРЕЛ І ЛІНІЙ ЕЛЕКТРОЖИВЛЕННЯ

Заходи захисту:

Контролювати фізичний доступ до [*Призначення: визначених організацією систем розподілу та постачання живлення*] у рамках можливостей організації, використовуючи [*Призначення: встановлені організацією заходи та засоби захисту*].

Рекомендації з реалізації: Засоби безпеки джерел і ліній електроживлення запобігають випадковим пошкодженням, збоям та фізичним підробкам. Такі заходи також можуть бути необхідними для запобігання підслуховуванню або модифікації незашифрованих передач. Засоби, що використовуються для контролю фізичного доступу до розподільних ліній і ліній електроживлення системи, містять: блокування електропроводки; відключення або блокування запасних гнізд; захист кабельних каналів трубопроводами або кабельними лотками; встановлення датчиків прослуховування та інше.

Пов'язані заходи: AT-3, IA-4, MP-2, MP-4, PE-2, PE-3, PE-5, PE-9, SC-7, SC-8.

Посилення заходів: Немає.

Посилання: Немає.

## PE-5 КОНТРОЛЬ ДОСТУПУ ДО ПРИСТРОЇВ ВИВЕДЕННЯ ІНФОРМАЦІЇ

Заходи захисту:

Керувати фізичним доступом до вихідних даних з [*Призначення: визначені організацією пристрої для виведення інформації*], для запобігання несанкціонованому отриманню користувачами вихідних даних.

Рекомендації з реалізації: Контроль фізичного доступу до пристроїв виведення інформації охоплює: розміщення пристроїв виведення інформації в ізольованих приміщеннях або інших захищених зонах і забезпечення доступу лише уповноважених осіб; розміщення пристроїв виведення інформації в місцях, за якими може бути встановлений контроль; встановлення моніторних або екранних фільтрів; використання навушників тощо. До пристроїв виведення інформації належать, наприклад, монітори, принтери, копіювальні пристрої, сканери, факсимільні машини та аудіопристрої.

Пов'язані заходи: PE-2, PE-3, PE-4, PE-18.

Посилення заходів:

(1) КОНТРОЛЬ ДОСТУПУ ДО ПРИСТРОЇВ ВИВЕДЕННЯ ІНФОРМАЦІЇ - ДОСТУП ДО ВИХІДНИХ ДАНИХ УПОВНОВАЖЕНИМИ ОСОБАМИ

[Вилучено: включено до PE-5].

(2) КОНТРОЛЬ ДОСТУПУ ДО ПРИСТРОЇВ ВИВЕДЕННЯ ІНФОРМАЦІЇ - ДОСТУП ДО ВИХІДНИХ ДАНИХ ФІЗИЧНИМИ ОСОБАМИ

Пов'язувати дані про цифрову ідентичність з підтвердженням отримання даних від вихідних пристроїв.

Рекомендації з реалізації: До методів прив'язки ідентичності до даних, отриманих з пристроїв виведення належать, наприклад, встановлення функцій захисту на факсимільних машинах, копіювальних апаратах і принтерах. Така функціональність дозволяє здійснювати автентифікацію на пристроях виведення інформації.

Пов'язані заходи: Немає.

(3) КОНТРОЛЬ ДОСТУПУ ДО ПРИСТРОЇВ ВИВЕДЕННЯ ІНФОРМАЦІЇ - МАРКУВАННЯ ПРИСТРОЇВ ВИВЕДЕННЯ ІНФОРМАЦІЇ

[Вилучено: включено до PE-22].

Посилання: [IR 8023].

## PE-6 МОНІТОРИНГ ФІЗИЧНОГО ДОСТУПУ

Заходи захисту:

a. Проводити моніторинг фізичного доступу до об'єкта, де перебуває система, з метою виявлення та реагування на інциденти фізичної безпеки.

b. Переглядати журнали фізичного доступу [*Призначення: з визначеною організацією частотою*] на предмет наявності [*Призначення: визначених організацією подій або потенційних ознак подій*].

c. Узгоджувати результати перегляду та розслідувань з організаційними можливостями реагування на інциденти.

Рекомендації з реалізації: Моніторинг фізичного доступу має поширюватися і на загальнодоступні зони в межах об'єктів організації. Це може бути досягнуто, наприклад, за допомогою охоронців, використання обладнання для відеоспостереження або використання сенсорних пристроїв. Моніторинг може підтримуватись засобами контролю аудиту журналів, такими як AU-2, в разі якщо журнал є частиною автоматизованої системи. До можливостей реагування на інциденти вносять розслідування та реагування на виявлені інциденти фізичної безпеки. До інцидентів безпеки належать, наприклад, порушення безпеки або підозрілі фізичні дії (доступ поза межами звичайного робочого часу; повторний доступ тощо).

Пов'язані заходи: AU-2, AU-6, AU-9, AU-12, CA-7, CP-10, IR-4, IR-8.

Посилення заходів:

(1) МОНІТОРИНГ ФІЗИЧНОГО ДОСТУПУ - ОХОРОННА СИГНАЛІЗАЦІЯ ТА ОБЛАДНАННЯ ДЛЯ СПОСТЕРЕЖЕННЯ

Здійснювати моніторинг фізичного доступу до об'єкта, де розміщується система, використовуючи засоби сигналізації та обладнання для спостереження.

Рекомендації з реалізації: Використання сигналізації дозволяє попереджати персонал охорони про спробу несанкціонованого доступу на об'єкт. Система сигналізації працює у поєднанні з фізичними бар'єрами, системами відеоспостереження та охороною, з реагуванням коли ці заходи безпеки

скомпроментовані чи порушені.

Пов’язані заходи: Немає.

(2) МОНІТОРИНГ ФІЗИЧНОГО ДОСТУПУ - АВТОМАТИЧНЕ РОЗПІЗНАВАННЯ ВТОРГНЕНЬ ТА ВІДПОВІДНА РЕАКЦІЯ

Впровадити автоматизовані механізми для розпізнавання [*Призначення: визначених організацією класів або типів вторгнень*] та ініціювання [*Призначення: визначених організацією відповідних реакцій*].

Рекомендації з реалізації: Заходи реагування можуть включати в себе оповіщення окремих співробітників організації або правоохоронних органів. Автоматизовані механізми, впроваджені для реагування включають системні сповіщення, електроні та текстові повідомлення, а також активацію механізму блокування дверей. Моніторинг фізичного доступу може бути скоординований з системами виявлення вторгнень та можливостями системного моніторингу, для забезпеченян комплексного захисту організації від загроз.

Пов’язані заходи: SI-4.

(3) МОНІТОРИНГ ФІЗИЧНОГО ДОСТУПУ - ВІДЕОСПОСТЕРЕЖЕННЯ

a) Впровадити відеоспостереження за [*Призначення: визначеними організацією зонами*];

b) Переглядати відеозаписи [*Призначення: з визначеною організацією частотою*];

c) Зберігати відеозапи протягом [*Призначення: визначеними організацією періодами часу*];

Рекомендації з реалізації: Це посилення стосується запису відеоспостереження з метою подальшого перегляду (за необхідністю). Моніторинг відеоспостереження не є обов’язковим та має впроваджуватися на розсуд організації. Необхідно брати до уваги можливі правові нюанси, особливо якщо таке спостереження проводиться в громадському місці.

Пов’язані заходи: Немає.

(4) МОНІТОРИНГ ФІЗИЧНОГО ДОСТУПУ - МОНІТОРИНГ ФІЗИЧНОГО ДОСТУПУ ДО СИСТЕМИ

Здійснювати моніторинг фізичного доступу до системи на додаток до моніторингу фізичного доступу до об’єкта в [*Призначення: визначені організацією фізичні приміщення, що містять один або більше компонентів системи*].

Рекомендації з реалізації: Це посилення контролю забезпечує додатковий моніторинг областей, де зосереджені компоненти системи (наприклад, серверні зали, зони зберігання носіїв інформації та центри зв’язку). Моніторинг фізичного доступу може бути скоординований з системами виявлення вторгнень та можливостями системного моніторингу, щоб забезпечити комплексний та інтегрований захист організації від загроз.

Пов’язані заходи: Немає.

Посилання: Немає.

## PE-7 КОНТРОЛЬ ВІДВІДУВАЧІВ

[Вилучено: Включено до PE-2 і PE-3].

## PE-8 РЕЄСТР ДОСТУПУ ВІДВІДУВАЧІВ

Заходи захисту:

a. Вести реєстр доступу відвідувачів до об’єкта, де перебуває система, впродовж [*Призначення: визначеного організацією періоду часу*].

b. Переглядати реєстр доступу відвідувачів [*Призначення: з визначеною організацією частотою*].

c. Повідомляти про порушення в реєстрі відвідувачів [*Призначення: персонал визначений організацією*].

Рекомендації з реалізації: Реєстри доступу відвідувачів зазвичай мають містити: імена й організації відвідувачів, підписи відвідувачів, форми ідентифікації, дати доступу, часи в’їзду та виїзду, мету відвідувань. Перевірка реєстру дозволяє визначити, чи дозволи на доступ є актуальними та необхідними для пітримки завдань організації та її функцій. Записи доступу не є обов’язковими для публічного доступу.

Пов’язані заходи: PE-2, PE-3, PE-6 .

Посилення заходів:

(1) РЕЄСТР ДОСТУПУ ВІДВІДУВАЧІВ - АВТОМАТИЗОВАНЕ ВЕДЕННЯ ТА ПЕРЕГЛЯД РЕЄСТРУ ВІДВІДУВАЧІВ

Впровадити автоматизовані механізми для ведення та перегляду (аналізу) реєстру відвідувачів.

Рекомендації з реалізації: Записи про доступ відвідувачів можуть зберігатися тп підтримуватись в базі даних, доступ до якої має персонал організації. Автоматизований доступ до таких записів полегшує регулярний перегляд записів, щоб визначити, чи є дозвіл на доступ актуальним.

Пов’язані заходи: Немає.

(2) РЕЄСТР ДОСТУПУ ВІДВІДУВАЧІВ - РЕЄСТР ФІЗИЧНОГО ДОСТУПУ

[Вилучено: включено до PE-2].

Посилання: Немає.

(3) РЕЄСТР ДОСТУПУ ВІДВІДУВАЧІВ – ОБМЕЖЕННЯ ІНФОРМАЦІЇ, ЩО ІДЕНТИФІКУЮТЬ ОСОБУ

Обмежте доступ до персональних даних, що міститься в реєстрі відвідувачів, та

визначені в оцінці ризиків конфіденційності [*Призначення: елементи визначені організацією*].

Рекомендації з реалізації: Організації можуть мати вимоги, які визначають вміст реєстрів про доступ відвідувачів. Обмеження персональних даних, що ідентифікують особу, в реєстрі доступу відвідувачів допомагає знизити ризики конфіденційності.

Пов'язані заходи: RA-3, SA-8.

Посилання: немає.

## PE-9 ЕНЕРГЕТИЧНЕ ОБЛАДНАННЯ ТА КАБЕЛІ

Заходи захисту:
Захищати енергетичне обладнання і силові кабелі системи від пошкоджень і руйнувань.

Рекомендації з реалізації: Організація визначає тип захисту, необхідний для енергетичного обладнання та кабелів, що використовуються в різних місцях. Вони можуть бути як внутрішніми так і зовнішніми по відношенню до об'єктів організації та середовища експлуатації. Це посилення забезпечує додатковий моніторинг областей, де є концентрація компонентів системи (серверні зали, зони зберігання носіїв інформації та центри зв'язку).

Пов'язані заходи: PE-4.

Посилення заходів:

(1) ЕНЕРГЕТИЧНЕ ОБЛАДНАННЯ ТА КАБЕЛІ - РЕЗЕРВНІ КАБЕЛІ

Використовувати резервні силові кабельні системи, які фізично відокремлені на відстань [*Призначення: визначена організацією відстань*].

Рекомендації з реалізації: Наявність фізично відокремлених та надлишкових силових кабелів забезпечить живлення у випадку, якщо один з кабелів буде пошкоджений.

Пов'язані заходи: Немає.

(2) ЕНЕРГЕТИЧНЕ ОБЛАДНАННЯ ТА КАБЕЛІ - АВТОМАТИЧНЕ КЕРУВАННЯ НАПРУГОЮ

Впровадити механізми автоматичного керування напругою для [Призначення: визначених організацією критичних компонентів системи].

Рекомендації з реалізації: Автоматичні регулятори напруги можуть контролювати й регулювати напругу.

Пов'язані заходи: Немає.

Посилання: Немає.

## PE-10 АВАРІЙНЕ ВІДКЛЮЧЕННЯ

Заходи захисту:

a. Забезпечити можливість відключення системи або окремих компонентів системи від живлення в надзвичайних ситуаціях.

b. Встановити перемикачі або пристрої аварійного відключення в [Призначення: визначені організацією місця розташування в системі або в компоненті системи] для забезпечення безпечного та легкого доступу персоналу.

c. Захищати механізми (систему) аварійного відключення живлення від несанкціонованої активації.

Рекомендації з реалізації: Це посилення застосовується до областей, де є концентрація компонентів системи (серверні зали, зони зберігання носіїв інформації та центри зв'язку).

Пов'язані заходи:PE-15.

Посилення заходів:

(1) АВАРІЙНЕ ВІДКЛЮЧЕННЯ - ВИПАДКОВА І НЕСАНКЦІОНОВАНА АКТИВАЦІЯ

[Виключено: включено до PE-10].

Посилання: Немає.

## PE-11 АВАРІЙНЕ ЕНЕРГОЗАБЕЗПЕЧЕННЯ

Заходи захисту: Впровадити тимчасове джерело безперебійного живлення для забезпечення [*Вибір (один або кілька): впорядковане виключення системи; перехід системи на довгострокову альтернативну систему живлення*] в разі втрати первинного джерела живлення.

Рекомендації з реалізації: Джерело безперебійного живлення (ДБЖ) – це електрична система або механізм, який забезпечує аварійне живлення в разі виходу з ладу основного джерела живлення. ДЖБ зазвичай використовується для захисту комп'ютерів, центрів обробки даних, комунікаційного обладнання або іншого електричного обладнання, де несподіване відключення живлення може призвести до збоїв роботи, втрати даних або інформації, травм чи смертельних випадків. ДБЖ відрізняється від аварійної системи електроживлення або резервного генератора тим, що ДБЖ забезпечує миттєвий захист від перебоїв у подачі електроенергії від основного джерела живлення. Час автономного ДБЖ відносно невеликий, але забезпечує достатній час для запуску резервного джерела живлення, або належного вимкнення системи.

Пов'язані заходи: AT-3, CP-2, CP-7.

Посилення заходів:

(1) АВАРІЙНЕ ЕНЕРГОЗАБЕЗПЕЧЕННЯ - ДОВГОСТРОКОВЕ АЛЬТЕРНАТИВНЕ ДЖЕРЕЛО ЖИВЛЕННЯ — МІНІМАЛЬНІ ЕКСПЛУАТАЦІЙНІ МОЖЛИВОСТІ

Забезпечити для системи наявність довгострокового альтернативного джерела живлення, яке може підтримувати мінімально необхідну експлуатаційну спроможність у разі тривалої втрати первинного джерела живлення.

Рекомендації з реалізації: Це посилення може бути реалізоване, наприклад, за допомогою вторинного джерела живлення або іншого зовнішнього джерела живлення. Довгострокові альтернативні джерела живлення для систем організації можуть активуватися вручну або автоматично.

Пов'язані заходи: Немає.

(2) АВАРІЙНЕ ЕНЕРГОЗАБЕЗПЕЧЕННЯ - ДОВГОСТРОКОВЕ АЛЬТЕРНАТИВНЕ ДЖЕРЕЛО ЖИВЛЕННЯ — АВТОНОМНЕ ЖИВЛЕННЯ

Забезпечити для системи наявність довгострокового альтернативного джерела живлення, яке:

(a) є автономним;

(b) не залежить від зовнішнього постачання енергії;

(c) здатне підтримувати [*Вибір: мінімально необхідні операційні можливості; повна експлуатаційна здатність*] у разі тривалої втрати первинного джерела живлення.

Рекомендації з реалізації: Це посилення можна забезпечити, наприклад, за допомогою одного або декількох генераторів достатньої потужності. Довгострокові альтернативні джерела живлення можуть активуватися вручну або автоматично.

Пов'язані заходи: Немає.

Посилання: Немає.

## PE-12 АВАРІЙНЕ ОСВІТЛЕННЯ

Заходи захисту:
Використовувати та підтримувати системи автоматичного аварійного освітлення, які активуються в разі відключення електроживлення або збою та які охоплюють аварійні виходи та маршрути евакуації всередині об'єкта.

Рекомендації з реалізації: Цей захід безпеки застосовується до областей, де є концентрація компонентів системи (серверні зали, зони зберігання носіїв інформації та центри зв'язку).

Пов'язані заходи: CP-2, CP-7.

Посилення заходів:

(1) АВАРІЙНЕ ОСВІТЛЕННЯ - ОСНОВНІ ЗАВДАННЯ ТА ФУНКЦІЇ

Забезпечити аварійне освітлення для всіх зон, які підтримують виконання основних завдань і функцій.

Рекомендації з реалізації: Організація визначає свої основні функції.

Пов’язані заходи: Немає.

Посилання: Немає.

## PE-13 ПРОТИПОЖЕЖНИЙ ЗАХИСТ

Заходи захисту: Використовувати та підтримувати в працездатньому стані пристрої та системи пожежогасіння й виявлення пожежі. Забезпечити роботу систем протипожежного захисту незалежним джерелом живлення.

Рекомендації з реалізації: Цей захід безпеки застосовується до областей, де є концентрація компонентів системи, включно з, наприклад, серверними залами, зонами зберігання носіїв інформації та центрами зв’язку. До приладів або систем пожежогасіння, які можуть потребувати незалежного джерела енергії, належать спринклерні системи, нерухомі пожежні шланги та детектори диму.

Пов’язані заходи: AT-3.

Посилення заходів:

(1) ПРОТИПОЖЕЖНИЙ ЗАХИСТ - ПРИСТРОЇ ТА СИСТЕМИ ВИЯВЛЕННЯ

Використовувати такі пристрої/системи для виявлення пожежі в системі, які активуються автоматично та повідомляють [*Призначення: визначені організацією персонал або посадові особи*] та [*Призначення: визначену організацією аварійну команду*] у разі пожежі.

Рекомендації з реалізації: Організації можуть заздалегідь визначити персонал або ролі, яким має бути наданий доступ до необхідного обладнання в разі виникнення позаштатної ситуації.

Пов’язані заходи: Немає.

(2) ПРОТИПОЖЕЖНИЙ ЗАХИСТ - ПРИСТРОЇ ТА СИСТЕМИ АВТОМАТИЧНОГО ПОЖЕЖОГАСІННЯ

(a) Використовувати такі пристрої/системи пожежогасіння для системи, які забезпечують автоматичне сповіщення про будь-яку активацію [*Призначення: визначені організацією персонал або ролі*] і [*Призначення: визначену організацією аварійну команду*].

(b) Впровадити системи та засоби автоматичного гасіння пожежі, коли об’єкт не укомплектований відповідним персоналом на постійній основі.

Рекомендації з реалізації: Організації можуть заздалегідь визначити персонал або ролі організації, яким має бути наданий доступ до відповідного обладнання в разі виникнення позаштатної ситуації.

Пов’язані заходи: Немає.

(3) ПРОТИПОЖЕЖНИЙ ЗАХИСТ - АВТОМАТИЧНЕ ПОЖЕЖОГАСІННЯ

[Виключено: включено до PE-13 (2)].

(4) ПРОТИПОЖЕЖНИЙ ЗАХИСТ - ПЕРЕВІРКИ

Переконатися, що об’єкт проходить перевірки пожежної безпеки [*Призначення: з визначеною організацією частотою*], переконатися, що на об’єкті усуваються виявлені недоліки в межах [*Призначення: визначеного організацією часу*].

Рекомендації з реалізації: Уповноважений та кваліфікований персонал, що перебуває під юрисдикцією організації включають пожежних інспекторів. Організації надають супровід під час перевірок у ситуаціях, коли системи, що знаходяться на об’єкті містять конфіденційну інформацію.

Пов’язані заходи: Немає.

Посилання: Немає.

## PE-14 КОНТРОЛЬ ТЕМПЕРАТУРИ ТА ВОЛОГОСТІ

Заходи захисту:

a. Підтримувати температуру та вологість у приміщенні, де розташована система в рамках [*Призначення: визначеного організацією рівня*].

b. Контролювати рівні температури та вологості [*Призначення: з визначеною організацією частотою*].

Рекомендації з реалізації: Цей захід безпеки застосовується до областей, де є концентрація компонентів системи (серверні зали, зони зберігання носіїв інформації та центри зв’язку).

Пов’язані заходи: AT-3, CP-2.

Посилення заходів:

(1) КОНТРОЛЬ ТЕМПЕРАТУРИ ТА ВОЛОГОСТІ - АВТОМАТИЧНИЙ КОНТРОЛЬ

Впровадити автоматичне регулювання температури та вологості на об’єкті для запобігання потенційно шкідливим для інформаційної системи коливанням.

Рекомендації з реалізації: Немає.

Пов’язані заходи: Немає.

(2) КОНТРОЛЬ ТЕМПЕРАТУРИ ТА ВОЛОГОСТІ - МОНІТОРИНГ ЗА ДОПОМОГОЮ СИГНАЛІЗАЦІЙ ТА СПОВІЩЕНЬ

Впровадити моніторинг температури та вологості з використанням засобів сигналізації або сповіщення до [*Призначення: визначеного організацією персоналу або ролей*] про потенційно небезпечні зміни для персоналу або обладнання.

Рекомендації з реалізації: Сигнал тривоги або сповіщення може бути звуковим сигналом або візуальним повідомленням у режимі реального часу для персоналу

або ролей, визначених організацією. Такі тривоги та сповіщення можуть допомагти мінімізувати шкоду для людей та шкоду для активів організації, сприяючи своєчасному реагуванню на інциденти.

Пов'язані заходи: Немає.

Посилання: Немає.

## PE-15 ЗАХИСТ ВІД ПОШКОДЖЕННЯ ВОДОЮ

Заходи захисту: Забезпечити захист інформаційної системи від пошкоджень, що виникають у разі витоку води, використовуючи відповідні ізоляційні або запірні клапани.

Рекомендації з реалізації: Цей захід безпеки застосовується до областей, де є концентрація компонентів системи (серверні зали, зони зберігання носіїв інформації та центри зв'язку). Ізоляційні клапани можуть застосовуватися на додаток до або замість головних запірних клапанів для відключення подачі води в конкретних проблемних точках.

Пов'язані заходи: AT-3, PE-10.

Посилення заходів:

(1) ЗАХИСТ ВІД ПОШКОДЖЕННЯ ВОДОЮ - АВТОМАТИЧНА ПІДТРИМКА

Впровадити автоматизовані механізми виявлення води поблизу інформаційної системи та оповіщення [*Призначення: визначеного організацією персоналу або ролей*].

Рекомендації з реалізації: До автоматизованих механізмів належать, наприклад, датчики виявлення води, тривожні сигнали та системи оповіщення.

Пов'язані заходи: Немає.

Посилання: Немає.

## PE-16 ДОСТАВКА ТА ВИДАЛЕННЯ

Заходи захисту:

a. Проводити авторизацію, моніторинг і контроль [*Призначення: визначені організацією типи компонентів інформаційної системи*], що входять і виходять з об'єкта;

b. вести облік цих елементів.

Рекомендації з реалізації: Для посилення дозволів на вхід і вихід з компонентів системи може знадобитися обмеження доступу до областей доставки та ізоляція областей від системи.

Пов'язані заходи: CM-3, CM-8, MA-2, MA-3, MP-5, PE-20, SR-2, SR-3, SR-4, SR-6.

Посилення заходів: Немає.

Посилання: Немає.

## PE-17 АЛЬТЕРНАТИВНЕ РОБОЧЕ МІСЦЕ

Заходи захисту:

a. Визначити та задокументувати [*Призначення: визначені організацією альтернативні робочі місця*], які дозволені для використання працівниками.

b. Впровадити [*Призначення: визначені організацією заходи захисту*] на альтернативних робочих місцях.

c. Оцінити ефективність заходів захисту на альтернативних робочих місцях.

d. Надати працівникам засоби комунікації з персоналом служби інформаційної безпеки в разі інцидентів безпеки.

Рекомендації з реалізації: До альтернативних робочих місць належать, наприклад, урядові установи або приватні помешкання працівників. Альтернативні робочі місця можуть використовуватися попри їхню територіальну відокремленість. Організації можуть визначати різні набори заходів захисту для конкретних альтернативних робочих місць. Цей захід пов'язаний з діяльністю щодо планування забезпечення безперервної роботи та відновлення функціонування.

Пов'язані заходи: AC-17, AC-18, CP-7.

Посилення заходів: Немає.

Посилання: [SP 800-46].

## PE-18 РОЗТАШУВАННЯ КОМПОНЕНТІВ СИСТЕМИ

Заходи захисту: Встановити компоненти інформаційної системи на об'єкті, з метою мінімізації потенційної шкоди від [*Призначення: визначеної організацією фізичної та екологічної небезпеки*], та мінімізації можливості несанкціонованого доступу.

Рекомендації з реалізації: До фізичних та екологічних небезпек належать повені, пожежі, смерчі, землетруси, урагани, терористичні акти, вандалізм, інші форми електромагнітного випромінювання. Близьке розташування точок входу для авторизованих осіб близько до основних точок входу може збільшити ризик несанкціонованого доступу до комунікацій організації, включно з, наприклад, використанням бездротових снайферів або мікрофонів.

Пов'язані заходи: CP-2, PE-5, PE-19, PE-20, RA-3.

Посилення заходів:

(1) РОЗТАШУВАННЯ КОМПОНЕНТІВ СИСТЕМИ - МІСЦЕ РОЗМІЩЕННЯ ОБ'ЄКТА

[Вилучено: перенесено до PE-23].

Посилання: Немає.

## PE-19 ВИТІК ІНФОРМАЦІЇ

Заходи захисту: Забезпечити захист від витоку інформації шляхом випромінювання електромагнітних сигналів.

Рекомендації з реалізації: Витік інформації — це навмисне чи ненавмисне розміщення даних або інформації в ненадійному середовищі. Засоби та порядок захисту має бути затверджений у документації щодо категорії безпеки, планах і політиках.

Пов'язані заходи: AC-18, PE-18, PE-20.

Посилення заходів:

(1) ВИТІК ІНФОРМАЦІЇ - НАЦІОНАЛЬНІ ПОЛІТИКИ ТА ПРОЦЕДУРИ ЩОДО ПЕМВ

Забезпечити захист інформаційної системи, передачу даних та мережі відповідно до національних політик і процедур захисту від ПЕМВ на основі категорії безпеки або класифікації інформації.

Пов'язані заходи: Немає.

Посилання: FIPS Publication 199.

## PE-20 МОНІТОРИНГ ТА ВІДСТЕЖЕННЯ АКТИВІВ

Заходи захисту:

Використовувати [*Призначення: визначені організацією технології визначення місця розташування*] для моніторингу та відстеження місця розташування та переміщення [*Призначення: визначених організацією активів*] у [*Призначення: визначені організацією контрольовані зони*].

Рекомендації з реалізації: Технології розташування активів можуть допомогти організаціям забезпечити збереження критичних ресурсів, зокрема транспортних засобів, обладнання або основних компонентів системи в дозволених місцях. Організації можуть консультуватися з уповноваженими компетентними особами щодо розгортання та використання технологій розташування активів для розв'язання потенційних проблем приватності.

Пов'язані заходи: CM-8, PM-8, PE-16.

Посилення заходів: Немає.

Посилання: Немає.

## PE-21 ЗАХИСТ ВІД ЕЛЕКТРОМАГНІТНОГО ІМПУЛЬСУ

Заходи захисту:
Використовувати [*Призначення: визначені організацією заходи захисту*] проти пошкодження електромагнітним імпульсом для [*Призначення: визначених організацією*

*систем*].

Рекомендації з реалізації: Електромагнітний імпульс (EMI) — це короткий сплеск електромагнітної енергії, який розповсюджується по діапазону частот. Такі енергетичні сплески можуть бути природними або техногенними. Втручання EMI може пошкоджувати електронне обладнання. Заходи захисту, що застосовуються для зменшення ризику EMI, охоплюють: екранування, запобігання перенапрузі, ферорезонансні трансформатори, заземлення та інше.

Пов'язані заходи: PE-18, PE-19.

Посилення заходів: Немає.

Посилання: Немає.

## PE-22 МАРКУВАННЯ КОМПОНЕНТІВ

Заходи захисту:

Позначати [*Призначення: визначені організацією апаратні компоненти*], що вказують рівень впливу або класифікацію інформації, яка дозволена для обробки, зберігання або передачі з використанням апаратних компонентів.

Рекомендації з реалізації: До апаратних компонентів, які можуть потребувати маркування, належать, наприклад, пристрої введення/виведення інформації, багатофункціональні пристрої, копіювальні пристрої. Маркування має містити інформацію щодо атрибутів безпеки. Маркування зазвичай не потрібне для апаратних пристроїв, які обробляють загальнодоступну інформацію (проте організації можуть вимагати наявність маркування на таких апаратних компонентах). Маркування апаратних компонентів має відповідати чинному законодавству.

Пов'язані заходи: AC-3, AC-4, AC-16, MP-3.

Посилення заходів: Немає.

Посилання: [IR 8023].

## PE-23 РОЗТАШУВАННЯ ОБ'ЄКТА

Заходи захисту:

a. сплануйте розташування або ділянку об'єкта, де знаходиться система, враховуючи фізичні та екологічні ризики;

b. для існуючих об'єктів врахуйте фізичні та екологічні ризики в організаційній стратегії управління ризиками.

Рекомендації з реалізації: Фізичні та екологічні ризики включають повені, пожежі, торнадо, землетруси, урагани, тероризм, вандалізм, електромагнітні імпульси, електричні перешкоди та інші форми вхідного електромагнітного випромінювання. Розташування компонентів системи на об'єкті розглядається в PE-18.

Пов'язані заходи: CP-2, PE-18, PE-19, PM-8, PM-9, RA-3.

Посилання: Немає.

## 10.12 Клас заходів захисту PL — ПЛАНУВАННЯ БЕЗПЕКИ

### PL-1 ПОЛІТИКИ ТА ПРОЦЕДУРИ ПЛАНУВАННЯ БЕЗПЕКИ

Заходи захисту:

a. Розробити, задокументувати та поширити серед [*Призначення: визначеного організацією персоналу або ролей*]:

   1. [*вибір (один або декілька): рівень організації; рівень місії/бізнес процесу; рівень системи*] політику планування, яка:

      (a) містить мету, сферу застосування, ролі, обов'язки, відповідальність керівництва, координацію між організаційними підрозділами та системою контролю (complaince);

      (b) відповідає чинному законодавству, виконавчим наказам, директивам, нормам, політикам, стандартам та керівним принципам;

   2. процедури, що полегшують здійснення планування політики безпеки та приватності й пов'язані з ними заходи.

b. Призначити [*Призначення: визначену організацією посадову особу*] для управління політикою та процедурами планування політики безпеки та приватності.

c. Переглядати та оновлювати поточне планування:

   1. політики планування безпеки та приватності [*Призначення:з визначеною організацією частотою*] та наступні [*Призначення: визначені організацією події*];

   2. поточні процедури планування політики безпеки та приватності [*Призначення: з визначеною організацією частотою*] та наступні [*Призначення: визначені організацією події*].

Рекомендації з реалізації: Цей захід захисту стосується встановлення політики та процедур для ефективного здійснення заходів і їх посилень у класі PL. Стратегія управління ризиками є важливим фактором у встановленні політики та процедур. Комплексна політика та процедури допомагають забезпечити безпеку та приватність. За наявності політики, а також планів захисту інформації та персональних даних на рівні організації, конкретні системні політики та процедури можуть бути не потрібні. Політика може бути внесена до складу загальної політики безпеки та приватності або може бути представлена кількома політиками (у випадках складної архітектури). Процедури описують, як має реалізуватися політика чи заходи захисту та як вони можуть бути спрямовані на персонал або роль, яка є об'єктом процедури. Процедури можуть бути задокументовані в планах захисту інформації та персональних даних (як один або декілька документів). Події, які можуть спричинити оновлення політики та процедур планування, включають, але не обмежуються, висновки оцінки чи аудиту, інциденти чи порушення безпеки або зміни в законах, розпорядженнях, директивах, положеннях, політиках, стандартах і рекомендаціях. Просте повторне встановлення засобів контролю не є організаційною політикою чи процедурою.)

Пов'язані заходи: PM-9, PS-8, SI-12.

Посилення заходів: Немає.

Посилання: [OMB A-130], [SP 800-12], [SP 800-18], [SP 800-30], [SP 800-39], [SP 800-100].

## PL-2 ПЛАНИ ЗАХИСТУ ІНФОРМАЦІЇ ТА ПЕРСОНАЛЬНИХ ДАНИХ

Заходи захисту:

a. Розробити план захисту інформації та персональних даних для інформаційної системи, який:

1. узгоджується з архітектурою підприємства організації;
2. чітко визначає складові компоненти системи;
3. описує оперативний контекст інформаційної системи з точки зору завдань та процесів;
4. визначає осіб, які виконують системні ролі та обов'язки;
5. визначає тип інформації, яка обробляється, зберігається та передається системою;
6. надає огляд вимог безпеки та приватності інформаційної системи;
7. описує будь які конкретні загрози системи, які викликають стурбованість організації;
8. надає результати оцінки ризику конфіденційності для систем, в яких обробляються персональні дані;
9. описує робоче середовище інформаційної системи та будь які залежності від систем або компонентів систем або підключень до таких систем та їх компонентів;
10. надає огляд вимог безпеки та конфіденційності системи;
11. визначає будь які відповідні контрольні базові рівні або накладання, якщо вони застосовуються;
12. описує чинні або заплановані заходи щодо забезпечення безпеки та приватності, включно з обґрунтуванням рішень щодо налаштування
13. включає виявлення ризиків для архітектури безпеки і приватності, а також проєктних рішень;
14. включає дії, пов'язані з безпекою та конфіденційністю, які впливають на систему, виконання яких вимагає планування та координацію з [*Призначення: визначені організацією окремі особи або групи*];
15. розглядається та затверджується уповноваженою посадовою особою або призначеним представником до початку реалізації плану.

b. Поширити копії планів захисту інформації та персональних даних і повідомляти про подальші зміни планів серед [*Призначення:визначеного організацією персоналу або ролей*].

c. Переглядати плани захисту інформації та персональних даних [*Призначення: з визначеною організацією частотою*].

d. Оновлювати плани захисту інформації та персональних даних для врахування змін в інформаційній системі й робочому середовищі або проблем, виявлених у ході реалізації або оцінювання заходів безпеки та приватності.

e. забезпечити захист планів захисту інформації та персональних даних від несанкціонованого розголошення та змін.

Рекомендації з реалізації: Плани захисту інформації та персональних даних системи охоплюють цю систему та її компоненти у визначених відповідними дозволами межах. Вони містять огляд вимог безпеки та приватності системи, а також заходи захисту, які відповідатимуть цим вимогам. Плани містять деталізований опис призначення кожного із визначених заходів захисту, що дозволить здійснити їх правильне впровадження та оцінити ефективність застосування.
Документація повинна відображати вичерпну інформацію щодо впровадження заходів захисту з урахуванням їх гібридності відповідно до специфіки конкретної системи, а також відповідності намірам щодо функціональності такої системи. Плани захисту інформації та персональних даних також можуть використовуватися при проєктуванні та розробці систем для підтримки життєвого циклу процесів захисту інформації та персональних даних. Плани захисту інформації та персональних даних повинні бути живими документами, які підлягають оновленню та адаптації протягом життєвого циклу розробки системи (наприклад, під час визначення можливостей системи, аналізу альтернатив, відповідності попиту та пропозиції, а також огляди проектних рішень). Розділ 2.1 описує різні типи вимог, які мають відношення до організацій протягом життєвого циклу системи, а також взаємозвязок між вимогами та заходами захисту. Організація може розробляти єдиний для впровадження план захисту інформації та приватності або підтримувати декілька планів. Плани захисту інформації та приватності пов’язують вимоги щодо захисту інформації та приватності з набором заходів захисту та вдосконаленням контролю. Плани захисту інформації та персональних даних повинні містити достатню інформацію (включно зі специфікацією значень параметрів), щоб дозволити розробку та реалізацію, яка однозначно відповідає намірам планів і подальшому визначенню ризиків для операцій і активів організації, фізичних осіб, інших організацій. Це зменшує обсяг документації, пов’язаної з концепцією інформаційної безпеки. Плани захисту інформації та персональних даних не містять детальної інформації щодо планування безперервної роботи та відновлення функціонування чи інформації про реагування на інциденти, але містять достатню інформацію для визначення того, що необхідно виконати для реалізації заходів, визначених у цих планах. Дії, що пов’язані з безпекою та приватністю, охоплюють, наприклад, оцінювання безпеки та приватності, перевірки й технічне обслуговування програмного забезпечення, управління виправленнями та тестуваннями плану забезпечення безперервної роботи й відновлення функціонування. Планування та координація мають охоплювати позаштатні ситуації (природного чи техногенного походження). Процес, визначений організаціями для планування й координації заходів, пов’язаних з безпекою та приватністю, за потреби може бути внесений у політики безпеки та приватності для систем чи інших документів.

Пов'язані заходи: AC-2, AC-6, AC-14, AC-17, AC-20, CA-2, CA-3, CA-7, CM-9, CM-13, CP-2, CP-4, IR-4, IR-8, MA-4, MA-5, MP-4, MP-5, PL-7, PL-8, PL-10, PL-11, PM-1, PM-7, PM-8, PM-9, PM-10, PM-11, RA-3, RA-8, RA-9, SA-5, SA-17, SA-22, SI-12, SR-2, SR-4.

Посилення заходів:

(1) ПЛАНИ ЗАХИСТУ ІНФОРМАЦІЇ ТА ПЕРСОНАЛЬНИХ ДАНИХ - КОНЦЕПЦІЯ ЕКСПЛУАТАЦІЇ

[Вилучено: включено до PL-7].

(2) ПЛАНИ ЗАХИСТУ ІНФОРМАЦІЇ ТА ПЕРСОНАЛЬНИХ ДАНИХ - ФУНКЦІОНАЛЬНА АРХІТЕКТУРА

[Вилучено: включено до PL-8].

(3) ПЛАНИ ЗАХИСТУ ІНФОРМАЦІЇ ТА ПЕРСОНАЛЬНИХ ДАНИХ - ПЛАНУВАННЯ ТА КООРДИНАЦІЯ З ІНШИМИ ОРГАНІЗАЦІЙНИМИ СТРУКТУРАМИ

[Вилучено: включено до PL-2].

Посилання: [OMB A-130], [SP 800-18], [SP 800-37], [SP 800-160-1], [SP 800-160-2].

## PL-3 ОНОВЛЕННЯ ПЛАНІВ ЗАХИСТУ ІНФОРМАЦІЇ ТА ПЕРСОНАЛЬНИХ ДАНИХ

[Вилучено: включено до PL-2].

## PL-4 ПРАВИЛА ПОВЕДІНКИ

Заходи захисту:

a. Створити та надати особам, що потребують доступу до інформаційної системи, правила, які описують їхні обов'язки й очікувану поведінку щодо інформації та використання інформаційної системи, безпеки та приватності.

b. Отримати документальне підтвердження від таких осіб про те, що вони прочитали, зрозуміли та погодилися дотримуватися правил поведінки, перш ніж дозволяти доступ до інформації та інформаційної системи.

c. Переглядати й оновлювати правила поведінки [*Призначення: з визначеною організацією частотою*].

d. Вимагати від осіб, які підписали попередню версію правил поведінки, перечитати та повторно підписати правила [*Вибір (один або декілька): [Призначення: з визначеною організацією частотою]; коли правила переглядаються чи оновлюються*].

Рекомендації з реалізації: Це вдосконалення стосується користувачів організації. Інші типи угод, за якими дозволяються надавати доступ, включають в себе угоди про нерозголошення, конфлікт інтересів, а також угоди про правила використання (див. PS-6). Організації розглядають правила поведінки, що базуються на окремих ролях і

обов'язках користувачів, розрізняючи правила для привілейованих і непривілейованих користувачів. Встановлення правил поведінки для деяких типів користувачів, що не є працівниками організації, включно з, наприклад, особами, які просто отримують дані чи інформацію з системи, часто не є можливим, враховуючи велику кількість таких користувачів та обмежений характер їхньої взаємодії із системами. Правила поведінки для користувачів організації також можуть бути встановлені в AC-8. У цьому розділі наведено список заходів захисту, які мають відношення правил поведінки в організації. Вимоги PL-4b можуть забезпечуватися навчанням щодо інформованості про безпеку та приватність, а також навчальними програмами з питань безпеки та приватності, що розробляються організаціями, якщо таке навчання містить правила поведінки. Документальним підтвердженням ознайомлення та погодження із правилами поведінки є електронний або фізичний підпис особи, а також прийняття електронної угоди розміщенням галочки у відповідному полі.

Пов'язані заходи: AC-2, AC-6, AC-8, AC-9, AC-17, AC-18, AC-19, AC-20, AT-2, AT-3, CM-11, IA-2, IA-4, IA-5, MP-7, PS-6, PS-8, SA-5, SI-12.

Посилення заходів:

(1) ПРАВИЛА ПОВЕДІНКИ - ОБМЕЖЕННЯ НА СОЦІАЛЬНІ МЕДІА ТА МЕРЕЖУ

Внести до правил поведінки обмеження щодо:

a) використання соціальних медіапорталів, вебсайтів, а також зовнішніх/сторонніх сайтів/додатків;

b) розміщення інформації, що належить організації, на загальнодоступних вебсайтах;

c) використання наданих організацією ідентифікаторів (наприклад, електронна пошта) та секретів автентифікації (наприклад, паролі) для створення акаунтів на зовнішніх/сторонніх вебсайтах/додатках.

Рекомендації з реалізації: Це вдосконалення стосується правил поведінки, пов'язаних з використанням соціальних медіа та мережевих вебсайтів, коли персонал організації використовує такі сайти для службових обов'язків, а також коли організаційна інформація залучається до соціальних медіа та мережевих транзакцій і коли персонал здійснює доступ до соціальних медіа та мережевих сайтів з систем організації. Організації також встановлюють конкретні правила, які не дають можливість стороннім організаціям отримувати недержавну організаційну інформацію із соціальних медіа та мережевих сайтів.

Пов'язані заходи: AC-22, AU-13.

Посилання: Немає.

## PL-5 ОЦІНЮВАННЯ ВПЛИВУ НА ПРИВАТНІСТЬ

[Вилучено: включено до RA-8].

## PL-6 ПЛАНУВАННЯ ДІЯЛЬНОСТІ, ПОВ'ЯЗАНОЇ З БЕЗПЕКОЮ

[Вилучено: включено до PL-2].

## PL-7 КОНЦЕПЦІЯ ЕКСПЛУАТАЦІЇ

Заходи захисту:

a. Розробити концепцію експлуатації інформаційної системи, яка описує, як організація має намір керувати системою з погляду забезпечення безпеки та приватності інформації.

b. Переглядати й оновлювати концепцію експлуатації [*Призначення: з визначеною організацією частотою*].

Рекомендації з реалізації: Концепція експлуатації — це документ, який призначений для користувача та містить інформацію про робочі характеристики системи з погляду користувача. На відміну від концепції функціонування, концепція експлуатації може містити один або декілька сценаріїв експлуатації системи. Концепція експлуатації розробляється перед початком розробки системи на стадії проєктування. Вона є основою для формування функціональних вимог до системи. Концепція експлуатації може бути внесена до плану захисту інформації та персональних даних або до інших документів життєвого циклу розробки систем. Зміни в концепції експлуатації мають відображатися в постійних оновленнях планів захисту інформації та персональних даних, архітектурі безпеки та приватності й інших відповідних документах, включно з, наприклад, документами щодо життєвого циклу розробки системи та специфікації.

Пов'язані заходи: PL-2, SA-2, SI-12.

Посилення заходів: Немає.

Посилання: [OMB A-130].

## PL-8 АРХІТЕКТУРА БЕЗПЕКИ ТА ПРИВАТНОСТІ

Заходи захисту:

a. Розробити архітектуру безпеки та приватності для інформаційної системи, яка:

   1. характеризує методологію, вимоги та підходи, які слід вживати для забезпечення конфіденційності, цілісності та доступності інформації, що циркулює в системі;

   2. характеризує методологію, вимоги та підхід до обробки персональних даних для мінімізації ризику їх втрати;

   3. характеризує, як архітектури безпеки та приватності інтегруються в архітектуру підприємства;

   4. характеризує будь-які припущення, що пов'язані з безпекою та приватністю, щодо зовнішніх служб і залежності від них.

b. Переглядати й оновлювати архітектуру безпеки та приватності [*Призначення:з визначеною організацією частотою*], щоб відображати оновлення в архітектурі підприємства.

c. Відображати заплановані зміни архітектури плану безпеки та приватності, концепції експлуатації інформаційної системи, аналізу критичності,

організаційних заходах, постачань та закупівель.

Рекомендації з реалізації: Цей захід безпеки стосується дій, що вживаються організаціями з проєктування та розробки систем. Архітектури безпеки та приватності на системному рівні мають відповідати й доповнювати організаційні архітектури безпеки та приватності, описані в PM-7, які є невіддільною частиною і розробляються як частина архітектури підприємства. Архітектури безпеки та приватності містять: опис архітектури, розміщення і розподіл функцій безпеки та приватності (включно із заходами захисту), інформацію про безпеку та приватність для зовнішніх інтерфейсів; інформацію, якою обмінюються через інтерфейси, та пов'язані механізми захисту з кожним інтерфейсом. Крім того, архітектури безпеки та приватності можуть містити іншу інформацію, наприклад: ролі користувачів і привілеї доступу, які присвоєні кожній ролі; унікальні вимоги безпеки та приватності; типи інформації, що обробляється, зберігається та передається системою; пріоритети відновлення інформаційних і послуг системи та будь-які інші конкретні потреби захисту.

У сучасних обчислювальних архітектурах організаціям стає все складніше контролювати всі інформаційні ресурси. Можуть бути наявними залежність від зовнішніх інформаційних послуг і постачальників послуг. Опис таких залежностей в архітектурах безпеки та приватності є важливим для розробки комплексної стратегії захисту місії. Створення, розробка, документування та підтримка конфігурації систем організації має вирішальне значення для впровадження й ефективної архітектури безпеки та приватності. Розробка архітектури безпеки та приватності має координуватися зі службою безпеки інформації для забезпечення визначення й ефективної реалізації заходів захисту, необхідних для забезпечення вимог безпеки та приватності.

PL-8 насамперед орієнтований на організації для того, щоб впевнитися, що архітектура системи інтегрована до архітектури організації або тісно з нею пов'язана. В той же час, SA-17 в першу чергу орієнтований на розробників та інтеграторів зовнішніх продуктів інформаційних технологій та систем. SA-17, який доповнює PL-8, обирається у випадках, коли організація передає розробку системи або її компонентів зовнішнім організаціям, а також у разі необхідності продемонструвати узгодженість архітектури заходів захисту та приватності корпоративній архітектурі організації.

Пов'язані заходи: CM-2, CM-6, PL-2, PL-7, PL-9, PM-5, PM-7, RA-9, SA-3, SA-5, SA-8, SA-17, SC-7.

Посилення заходів:

(1) АРХІТЕКТУРА БЕЗПЕКИ ТА ПРИВАТНОСТІ - «ГЛИБОКА ОБОРОНА»

Спроєктувати архітектуру безпеки та приватності для інформаційної системи, використовуючи підхід «глибокої оборони», що:

(a) призначає [*Призначення: визначені організацією заходи захисту*] для [*Призначення: визначених організацією місць та архітектурних рівнів*];

(b) забезпечує, щоб призначені заходи захисту діяли скоординовано та на взаємодоповнювальній основі.

Рекомендації з реалізації: Організації стратегічно розділяють елементи забезпечення безпеки та приватності у відповідних архітектурах, щоб

зловмисникам необхідно було подолати численні заходи захисту для досягнення своєї мети. Створення для зловмисників вищезазначених умов призводить до додаткових часових витрат, необхідних для атаки на інформаційні ресурси організації, що в свою чергу збільшує ймовірність виявлення такої атаки. Координація виділених елементів заходів захисту має важливе значення для у випадках, коли атака на один із таких елементів може призвести до некоректної роботи решти. Непередбачувані наслідки можуть включати блокування системи та каскадні сигнали тривоги. Розміщення заходів захисту в системах і організаціях є важливим процесом, який вимагає ретельного аналізу. Вартість активів організації є важливим фактором для впровадження додаткових рівнів захисту. Підхід до побудови архітектури «глибокої оборони» включає в себе принцип модульності та багаторівневості (див. SA-8 (3)), розділення функціональних можливостей користувача та системи (див. SC-2) та ізоляції функції безпеки (див. SC-3).

Пов'язані заходи: SC-2, SC-3, SC-29, SC-36.

(2) АРХІТЕКТУРА БЕЗПЕКИ ТА ПРИВАТНОСТІ - РІЗНОМАНІТНІСТЬ ПОСТАЧАЛЬНИКІВ

Забезпечити, щоб [*Призначення: визначені організацією заходи захисту*], призначені для [*Призначення: визначених організацією місць та архітектурних рівнів*], були отримані від різних постачальників.

Рекомендації з реалізації: Різні продукти інформаційних технологій мають різні сильні та слабкі сторони. Надання широкого спектру продуктів доповнює індивідуальні пропозиції. Наприклад, постачальники, що пропонують захист від зловмисного коду, зазвичай оновлюють свою продукцію в різний час, часто розробляючи рішення для відомих вірусів на основі їх пріоритетів та графіків розробки. Завдяки наявності різних продуктів у різних об'єктах захисту збільшується ймовірність, що принаймні один з них виявить зловмисний код. Що стосується приватності, постачальники можуть пропонувати продукти, які відслідковують особисту інформацію в системах, використовуючи різні методи відслідковування. Використання більшою кількості таких продуктів надасть більшу впевненість в тому, що персональні дані включені в реєстр.

Пов'язані заходи: SC-29, SR-3.

Посилання: [OMB A-130], [SP 800-160-1], [SP 800-160-2].

## PL-9 ЦЕНТРАЛІЗОВАНЕ УПРАВЛІННЯ

Заходи захисту:
Централізовано управляти [*Призначення: визначеними організацією організаційними заходами захисту та пов'язаними з ними процесами*].

Рекомендації з реалізації: Централізоване управління стосується управління в цілому в організації та впровадження вибраного заходу захисту, а також пов'язаних з цим процесів. Це охоплює: планування, впровадження, оцінювання, надання дозволу та моніторинг визначених організацією централізовано керованих заходів і процесів. Централізоване управління заходів захисту сприяє та полегшує стандартизацію впровадження й управління, а також розумне використання ресурсів організації. Оскільки централізоване управління заходами захисту пов'язане з концепцією спільних

(успадкованих) мір безпеки, таке управління сприяє та полегшує стандартизацію реалізації мір безпеки та управління, а також розумне використанні ресурсів організації. Заходи захисту та процеси, які підлягають централізованому управлінню, можуть виконувати вимоги незалежного оцінювання з метою забезпечення дотримання початкових та поточних дозволів для роботив рамках проведення постійного організаційного моніторингу. Автоматизовані інструменти (наприклад, інструменти управління захистом інформації та подіями, інструменти керування та моніторингу безпеки організації) можуть підвищити точність, послідовність і доступність інформації, пов'язаної з центральним управлінням заходами захисту і процесами. Автоматизація також може забезпечити можливість зведення та співвідношення даних, роботу механізмів оповіщення, створення інформаційних панелей для створення можливості прийняття рішень на основі ризиків в організації. В рамках процесу вибору заходів захисту організація визначає елементи управління, які можуть бути застосовані для центрального управління, виходячи із можливостей та ресурсів. Не завжди можливо організувати центральне управління кожного аспекту заходу захисту. У таких випадках заходи захисту можуть впроваджуватися та керуватися гібридно: централізовано або на системному рівні. Заходи захисту та заходи посилення, які можна використати для повного або часткового централізованого управління, включають, але не обмежуються: AC-2(1), AC-2(2), AC-2(3), AC-2(4), AC-4(all), AC-17(1), AC-17(2), AC-17(3), AC17(9), AC-18(1), AC-18(3), AC-18(4), AC-18(5), AC-19(4), AC-22, AC-23, AT-2(1), AT-2(2), AT-3(1), AT-3(2), AT-3(3), AT-4, AU-3, AU-6(1), AU-6(3), AU-6(5), AU-6(6), AU-6(9), AU-7(1), AU-11, AU-13, AU-16, CA-2(1), CA-2(2), CA-2(3), CA-3(1), CA-3(2), CA-3(3), CA-7(1), CA-9, CM-2(2), CM-3(1), CM-3(4), CM-4, CM-6, CM-6(1), CM-7(2), CM-7(4), CM-7(5), CM-8(all), CM-9(1), CM-10, CM-11, CP-7(all), CP-8(all), SC-43, SI-2, SI-3, SI-4(all), SI-7, SI-8.

Пов'язані заходи: PL-8, PM-9.

Посилення заходів: Немає.

Посилання: [OMB A-130], [SP 800-37].

## PL-10 ВИБІР БАЗОВОГО ПРОФІЛЮ БЕЗПЕКИ

Заходи захисту:
Вибрати базовий профіль безпеки для інформаційної системи.

Рекомендації з реалізації: Вибір базового профілю безпеки визначається потребами зацікавлених сторін. Потреби та проблеми зацікавлених сторін передбачають вимоги та завдання, що пов'язані з місією у рамках чинного законодавства. Базовий профіль безпеки являє собою відправну точку для забезпечення приватності, інформації та інформаційних систем із подальшим адаптуванням дій для управління ризиками відповідно до місії, бізнесу чи інших обмежень (див. PL-11). Організації вибирають один з базових профілів безпеки після: огляду типів інформації, яка обробляється, зберігається та передається в системах організації; аналізу можливого несприятливого впливу чи наслідків втрати або компрометації системи (інформації) щодо діяльності й активів організації, окремих людей, інших організацій; врахування результатів оцінювань ризику.

Пов'язані заходи: PL-2, PL-11, RA-2, RA-3, SA-8.

Посилення заходів: Немає.

Посилання: FIPS Publications 199, 200, [SP 800-30], [SP 800-37], [SP 800-39], [SP 800-53B], [SP 800- 60-1], [SP 800-60-2], [SP 800-160-1], [CNSSI 1253].

## PL-11 НАЛАШТУВАННЯ БАЗОВОГО ПРОФІЛЮ БЕЗПЕКИ

Заходи захисту:
Налаштувати вибраний базовий профіль безпеки, застосовуючи вказані дії для налаштування.

Рекомендації з реалізації: Налаштування базового профілю безпеки дозволяє організаціям налаштовувати набір заходів захисту. Це полегшує вибір заходів захисту та дозволяє організаціям розробляти плани захисту інформації та персональних даних, які: відображають їх конкретні місії (призначення), функції та завдання; середовища, у яких працюють їх системи; загрози та вразливості, що можуть вплинути на їхні системи. Налаштування базового профілю безпеки здійснюється шляхом: визначення та призначення загальних заходів захисту; міркувань щодо розміщення; вибору компенсаційних заходів захисту; призначення значень параметрам; доповнення базового профілю додатковими заходами захисту (за необхідності).

Пов’язані заходи: PL-10, RA-2, RA-3, RA-9, SA-8.

Посилення заходів: Немає.

Посилання: FIPS Publications 199, 200, [SP 800-30], [SP 800-37], [SP 800-39], [SP 800-53B], [SP 800- 60-1], [SP 800-60-2], [SP 800-160-1], [CNSSI 1253].

## 10.13 Клас заходів захисту PM — МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

### PM-1 ПРОГРАМА (КОНЦЕПЦІЯ) ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Заходи захисту:

a. Розробити та поширити на організаційному рівні план програми (концепцію) з інформаційної безпеки, яка:

   1. містить огляд вимог до програми (концепції) безпеки й описує заходи управління програмою інформаційної безпеки та загальних заходів безпеки, які використовуються або плануються для виконання цих вимог;

   2. містить визначення та розподіл ролей, обов'язків, відповідальності керівництва, заходи з координації діяльності організації і забезпечення відповідності вимогам законодавства та іншим нормативним документам;

   3. відображає координацію між організаційними елементами, що відповідають за інформаційну безпеку;

   4. затверджена вищою посадовою особою, що відповідає та підзвітна за управління ризиками, пов'язаними з організаційними операціями (включно з завданнями (місією), функціями, іміджем і репутацією організації), організаційні активи, фізичних осіб, інші організації та державу.

b. Переглядати та оновлювати загальноорганізаційний план програми (концепцію) інформаційної безпеки [*Призначення: з визначеною організацією частотою*] та у випадку [*Призначення: визначені організацією випадки*].

c. Забезпечити захист плану програми (концепції) інформаційної безпеки від несанкціонованого розкриття та зміни.

Рекомендації з реалізації: План програми (концепція) інформаційної безпеки являє собою формальний документ, в якому міститься огляд вимог безпеки для програми інформаційної безпеки в масштабах всієї організації та описує існуючі заходи захисту управління програмами та загальні заходи захисту в цілому, а також заплановані заходи захисту які будуть відповідати вищезазначеним вимогам. Залежно від складності організаційної архітектури, програма (концепція) інформаційної безпеки може бути представлена в одному документі або в декількох. Плани програм забезпечення приватності та плани управління ризиками ланцюга постачання розглядаються окремо в PM-18 та SR-2 відповдіно. На документальному рівні план програми відображає основні положення щодо забезпечення інформаційної безпеки та визначені організацією загальні заходи захисту. План надає вичерпну інформацію про заходи захисту (в тому числі специфікацію параметрів для операцій призначення та вибору, відображаючи таку інформацію в явному вигляді або за допомогою посилань) для забезпечення реалізації, яка однозначно відповідає меті плану, та визначення ризику, який виникне у разі впровадження такого плану. Оновлення планів програм інформаційної безпеки включають в себе організаційні зміни та проблеми, які були виявлені під час впровадження плану або отриманих в результаті контрольного оцінювання. Заходи захисту менеджменту інформаційної безпеки можуть бути реалізовані на рівні організації, місії, бізнес-процесу та є важливою складовою програми інформаційної безпеки організації. Заходи захисту менеджменту

інформаційної безпеки відрізняються від звичайних, специфічних для системи та гібридних заходів захисту, оскільки являються незалежними від будь-якої конкретної системи. Разом індивідуальні плани безпеки та план програми інформаційної безпеки організації забезпечують повне охоплення засобів заходів захисту, що використовуються в організації. Плани захисту для окремих систем і загальноорганізаційна програма інформаційної безпеки мають охоплювати всі заходи захисту, які застосовуються в організації. Загальні заходи захисту мають бути задокументовані в додатку до програми (концепції) інформаційної безпеки, якщо вони не внесені в окремі плани безпеки системи. Загальноорганізаційна програма інформаційної безпеки має містити посилання на окремі плани захисту, які містять описи загальних заходів захисту. Якщо програма (концепція) інформаційної безпеки складається з кількох документів, у кожному з них має бути зазначена посадова особа, відповідальна за розробку, реалізацію, оцінювання, надання дозволу та моніторинг відповідних загальних заходів безпеки.

Пов'язані заходи: PL-2, PM-18, PM-30, RA-9, SI-12, SR-2.

Посилення заходів: Немає.

Посилання: [FISMA], [OMB A-130], [SP 800-37], [SP 800-39].

## PM-2 РОЛІ ПРОГРАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Заходи захисту:

Призначити старшу посадову особу служби інформаційної безпеки, яка наділена відповідними завданнями та ресурсами для здійснення координації, розробки, впровадження та підтримки програми (концепції) інформаційної безпеки.

Рекомендації з реалізації: Старша особа служби інформаційної безпеки —посадова особа в організації. Для державних органів (відповідно до чинного законодавства) ця особа є посадовою особою інформаційної безпеки. Організації можуть також визначати цю посадову особу як старшу посадову особу з інформаційної безпеки.

Пов'язані заходи: Немає.

Посилення заходів: Немає.

Посилання: [OMB M-17-25], [SP 800-37], [SP 800-39], [SP 800-181].

## PM-3 РЕСУРСИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ПРИВАТНОСТІ

Заходи захисту:

a. Внести ресурси, необхідні для реалізації програми інформаційної безпеки та приватності, у процес планування капіталовкладень і запитів на інвестиції та задокументувати всі винятки з цієї вимоги.

b. Підготувати документацію, необхідну для розв'язання завдань програми інформаційної безпеки та приватності в процесі планування фінансування та запитів на інвестування відповідно до чинних законів, виконавчих наказів, директив, політик, правил, стандартів.

c. Забезпечити доступ до ресурсів, призначених для розв'язання завдань із захисту інформації та приватності.

Рекомендації з реалізації: Посадовим особам, відповідальним за питання інформаційної безпеки, мають бути виділені необхідні ресурси для їхньої діяльності. Організації можуть призначити та уповноважити раду з капіталовкладень або подібну групу для управління та надання контролю за аспектами інформаційної безпеки та приватності, пов'язаними з процесом планування капіталовкладень і управління інвестиціями.

Пов'язані заходи: PM-4, SA-2.

Посилення заходів: Немає.

Посилання: [OMB A-130].

## PM-4 ПЛАН ДІЙ ТА ЕТАПИ

Заходи захисту:

a. Запровадити процес для забезпечення того, щоб плани дій та етапи програм безпеки та приватності, програм управління ризиками ланцюга постачання і пов'язаних систем організації:

   1. розроблялися та підтримувалися;

   2. задокументовані корегувальні заходи захисту адекватно реагували на ризики для операцій організації і активів, фізичних осіб, інших організацій та держави;

   3. оприлюднювалися відповідно до встановлених вимог до звітності.

b. Переглядати плани дій та етапи для узгодженості з організаційною стратегією управління ризиками й організаційними пріоритетами щодо дій з реагування на ризики.

Рекомендації з реалізації: План дій (з виділеними основними етапами) є ключовим документом у програмах інформаційної безпеки та приватності. Плани дій та основні етапи мають бути розроблені на загальноорганізаційному рівні, визначаючи пріоритетність дій щодо реагування на ризики та забезпечуючи їх відповідність цілям і завданням організації . План дій та оновлення важливих етапів має базуватися на результатах контрольних оцінювань і постійних моніторингових заходів. Може бути кілька планів дій і етапів, що відповідають рівню інформаційної системи, місії/рівню процесу та організаційному рівню управління. У той час як для органів державної влади необхідні плани дій і основні етапи, інші організації можуть допомогти зменшити ризики шляхом документування та відстеження запланованих заходів із відновлення. Конкретні вказівки щодо планів дій і етапів на системному рівні надаються в CA-5.

Пов'язані заходи: CA-5, CA-7, PM-3, RA-7, SI-12.

Посилення заходів: Немає.

Посилання: [PRIVACT], [OMB A-130], [SP 800-37].

## PM-5 ІНВЕНТАРИЗАЦІЯ СИСТЕМИ

Заходи захисту: Розробити та оновити [*Завдання: частота, визначена організацією*] перелік систем організації.

Рекомендації з реалізації: [OMB A-130] надає вказівки щодо проведення інвентаризації систем і відповідних вимог до звітності. Системна інвентаризація стосується загальноорганізаційної інвентаризації систем, а не компонентів системи, як описано в CM-8.

Пов'язані заходи: Немає.

Посилення заходів:

(1) ІНВЕНТАРИЗАЦІЯ СИСТЕМИ - ІНВЕНТАРИЗАЦІЯ ПЕРСОНАЛЬНИХ ДАНИХ

Створення, підтримка та оновлення [*Призначення: частота, визначена організацією*] процедури інвентаризації всіх систем, програм і проектів, які обробляють персональні дані.

Рекомендації з реалізації: Інвентаризація систем, програм і проектів, які обробляють персональні дані, підтримує відображення дій із даними, надаючи особам повідомлення про конфіденційність, зберігаючи точні персональні дані та обмежуючи обробку таких даних, якщо така вони не потрібні для оперативних цілей. Організації використовують такі інструменти, щоб гарантувати, що системи обробляють персональні дані лише для авторизованих цілей і що ця обробка все ще актуальна та необхідна для визначеної мети в системі.

Повязані заходи: AC-3, CM-8, CM-12, CM-13, PL-8, PM-22, PT-3, PT-5, SI-12, SI-18.

Посилання: [OMB A-130], [IR 8062].

## PM-6 ПОКАЗНИКИ ПРОДУКТИВНОСТІ

Заходи захисту:
Розробити, відстежувати та звітувати про результати вимірювань показників продуктивності забезпечення безпеки інформації та приватності.

Рекомендації з реалізації: Показники продуктивності — це показники, які використовуються організацією для вимірювання ефективності програм інформаційної безпеки та конфіденційності, а також заходів захисту, що використовуються для підтримки програми. Щоб сприяти управлінню ризиками безпеки та приватності, організації розглядають узгодження показників ефективності з організаційною толерантністю до ризику, як визначено в стратегії управління ризиками.

Пов'язані заходи: CA-7, PM-9.

Посилення заходів: Немає.

Посилання: [OMB A-130], [SP 800-37], [SP 800-39], [SP 800-55], [SP 800-137].

## PM-7 АРХІТЕКТУРА ПІДПРИЄМСТВА

Заходи захисту:
Розробити корпоративну архітектуру з урахуванням вимог програми інформаційної безпеки та приватності, а також результатів оцінки ризику для операцій і активів організації, фізичних осіб, інших організацій та держави.

Рекомендації з реалізації: Інтеграція вимог і заходів захисту в архітектуру організації гарантує, що питання безпеки та приватності розв'язуються на початку життєвого циклу розробки системи й безпосередньо та явно пов'язані з місією і процесами організації та вбудовуються відповідно до стратегії управління ризиками організації. Для PM-7 архітектури безпеки та приватності розробляються на системному рівні всіх систем організації. Для PL-8 архітектури безпеки та приватності розробляються на рівні, який представляє окрему систему. Архітектури системного рівня узгоджуються з архітектурами безпеки та приватності, визначеними в організації. Вимоги до безпеки та приватності та інтеграції заходів захисту найефективніше досягаються шляхом суворого застосування Risk Management Framework [SP 800-37] і допоміжних стандартів безпеки та інструкцій.

Пов'язані заходи: AU-6, PL-2, PL-8, PM-11, RA-2, SA-3, SA-8, SA-17.

Посилення заходів:

(1) АРХІТЕКТУРА ПІДПРИЄМСТВА - РОЗВАНТАЖЕННЯ

Розвантажити [*Призначення: несуттєві функції або послуги, визначені організацією*] шляхом перенесення до інших систем, компонентів системи або передачі зовнішньому постачальнику.

Рекомендації з реалізації: Не кожна функція або послуга, яку надає система, є важливою для виконання цілей чи функцій організації. Друк або копіювання є прикладом несуттєвої, але допоміжної послуги для організації. Якщо це можливо, такі допоміжні, але несуттєві функції чи послуги не розміщуються разом із функціями чи послугами, які підтримують основні цілі чи функції організації. Підтримка таких функцій у тій самій системі чи системному компоненті збільшує поверхню атаки на основні функції або послуги організації. Переміщення допоміжних, але несуттєвих функцій до некритичної системи, системного компонента або зовнішнього постачальника також може підвищити ефективність основної системи, шляхом передачі таких функції або послуг під контроль окремих осіб або постачальників, які є експертами в галузі таких функцій або послуг.

Пов'язані заходи: SA-8.

Посилання: [OMB A-130], [SP 800-37], [SP 800-39], [SP 800-160-1], [SP 800-160-2].

## PM-8 ПЛАН ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Заходи захисту:
Визначити завдання інформаційної безпеки та приватності при розробці документуванні та оновленні плану захисту критичної інфраструктури та ключових ресурсів.

Рекомендації з реалізації: Стратегії захисту мають базуватися на визначенні пріоритетності критичних активів і ресурсів. Вимоги та рекомендації щодо визначення

критичної інфраструктури та основних ресурсів, а також підготовки відповідного плану захисту критичної інфраструктури містяться в чинному законодавстві.

Пов'язані заходи: CP-2, CP-4, PE-18, PL-2, PM-9, PM-11, PM-18, RA-3, SI-12.

Посилення заходів: Немає.

Посилання: [EO 13636], [OMB A-130], [HSPD 7], [DHS NIPP].

## PM-9 СТРАТЕГІЯ УПРАВЛІННЯ РИЗИКАМИ

Заходи захисту:

a. Розробити комплексну стратегію управління:

   1. ризиками безпеки для операцій та активів організації, фізичних осіб, інших організацій і держави, пов'язаних з експлуатацією та використанням систем організації;

   2. ризиками приватності для фізичних осіб, які можуть виникати внаслідок збирання, обміну, зберігання, передачі, використання та розпорядження персональними даними;

b. Реалізувати стратегію управління ризиками в масштабах організації.

c. Переглядати й оновлювати стратегію управління ризиками [*Призначення: з визначеною організацією частотою*] або, якщо потрібно, у разі змін в організації.

Рекомендації з реалізації: Загальноорганізаційна стратегія управління ризиками охоплює: прийнятні методики оцінювання ризику, стратегії зменшення ризику безпеки та приватності ланцюгів постачань, процес послідовного оцінювання ризику безпеки та приватності ланцюгів постачань по всій організації та підходи до моніторингу ризику. Старша посадова особа з управління ризиками має зіставляти процеси управління інформаційною безпекою з процесами стратегічного, оперативного та бюджетного планування. Функція управління ризиками, яку очолює старша посадова особа, відповідальна за управління ризиками, може сприяти послідовному застосуванню стратегії управління ризиками в усій організації. Стратегія управління ризиками може ґрунтуватися на вхідних даних, пов'язаних із ризиком безпеки та приватності, з інших джерел, як внутрішніх, так і зовнішніх для організації, щоб гарантувати, що стратегія є широкою та всеосяжною. Стратегія управління ризиками ланцюга постачання, описана в PM-30, також може надати корисні дані для загальної стратегії управління ризиками організації.

Пов'язані заходи: AC-1, AU-1, AT-1, CA-1, CA-2, CA-5, CA-6, CA-7, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PL-2, PM-2, PM-8, PM-18, PM-28, PM-30, PS-1, PT-1, PT-2, PT-3, RA-1, RA-3, RA-9, SA-1, SA-4, SC-38, SI-1, SI-12, SR-1, SR-2.

Посилення заходів: Немає.

Посилання: [OMB A-130], [SP 800-30], [SP 800-37], [SP 800-39], [SP 800-161], [IR 8023].

## PM-10 ПРОЦЕС АВТОРИЗАЦІЇ

Заходи захисту:

a. Управляти станом безпеки та приватності інформаційних систем організації та середовищ, у яких ці інформаційні системи експлуатуються через процедури авторизації

b. Призначити окремих осіб для виконання певних ролей і обов'язків у рамках організаційного процесу управління ризиками.

c. Інтегрувати процеси авторизації в загальноорганізаційну програму управління ризиками.

Рекомендації з реалізації: Процеси авторизації систем в організації і робочих середовищ вимагають впровадження: загальноорганізаційного процесу управління ризиками; структури управління ризиками та супутніх стандартів; рекомендацій щодо безпеки та приватності. Конкретні ролі для процесів управління ризиками включають відповідального керівника ризиків (функцію) та призначених посадових осіб для кожної системи в організації та основного постачальника засобів захисту. Процеси акредитації мають бути інтегровані з процесами постійного моніторингу для полегшення постійного розуміння та прийняття ризиків безпеки та приватності для операцій і активів організації, осіб та інших організацій і країни.

Пов'язані заходи: CA-6, CA-7, PL-2.

Посилення заходів: Немає.

Посилання: [SP 800-37], [SP 800-39], [SP 800-181].

## PM-11 ВИЗНАЧЕННЯ ЗАВДАНЬ І ПРОЦЕСІВ

Заходи захисту:

a. Визначити організаційні завдання та процеси з урахуванням інформаційної безпеки та приватності й ризиків, пов'язаних з організаційними операціями, організаційними активами, фізичними особами, іншими організаціями та державою.

b. Визначити потреби захисту інформації та персональних даних, які випливають із завданнь і процесів.

c. Переглядати й перевіряти завдання та процеси [*Призначення: з визначеною організацією частотою*].

Рекомендації з реалізації: Потреби в захисті — це незалежні від технології, необхідні можливості протидії загрозам через компрометацію інформації (тобто втрати конфіденційності, цілісності, доступності чи приватності). Необхідність захисту інформації та персональних даних при обробці інформації випливає з місії та ділових потреб, що визначаються зацікавленими сторонами в організаціях, місії та процесів, визначених для задоволення цих потреб, та стратегії управління організаційними ризиками. Захист інформації та потреби в обробці персональних даних визначають необхідні заходи захисту для організації та систем. Для визначення потреб у захисті та обробці персональних даних, невід'ємним є розуміння несприятливих наслідків, до яких може призвести компрометація або злам таких даних. Процес категоризації використовується для визначення такого потенційного впливу. Ризики приватності для осіб можуть виникати через компрометацію персональних даних або як ненавмисні

наслідки чи побічні ефекти їх обробки на будь-якій стадії життєвого циклу персональних даних. Оцінка ризиків приватності використовується для визначення пріоритетності ризиків, які створюються для осіб у результаті системної обробки песональних даних. Така оцінка дозволяє обрати необхідний захід захисту. Визначення місії та процесів і пов'язані з цим вимоги щодо захисту мають документуватися відповідно до організаційної політики та процедур.

Пов'язані заходи: CP-2, PL-2, PM-7, PM-8, RA-2, RA-3, RA-9, SA-2.

Посилення заходів: Немає.

Посилання: [OMB A-130], [FIPS 199],[SP 800-39], [SP 800-60-1], [SP 800-60-2], [SP 800-160-1].

## PM-12 ПРОГРАМА ІНСАЙДЕРСЬКОЇ ЗАГРОЗИ

Заходи захисту:
Впровадити програму інсайдерської (внутрішньої) загрози, яка передбачає наявність команди з обробки інцидентів, пов'язаних з внутрішньою дисципліною.

Рекомендації з реалізації: Відповідно до Указу 13587 [EO 13587] і Національної політики щодо внутрішніх загроз [ODNI NITP] організації, які обробляють секретну інформацію, зобов'язані створювати програми інсайдерських загроз. Стандарти та рекомендації, що застосовуються до програм інсайдерських загроз, також можуть ефективно застосовуватися для підвищення безпеки критичної інформації. Програми інсайдерської загрози містять заходи для виявлення та запобігання зловмисній інсайдерській діяльності за допомогою централізованої інтеграції та аналізу технічної і нетехнічної інформації для виявлення потенційних проблем щодо інсайдерської загрози. Старша посадова особа, призначена керівником, має забезпечувати та здійснювати контроль за програмою. Окрім централізованої інтеграції та аналізу, програми інсайдерських загроз вимагають від організацій підготувати політику та плани впровадження інсайдерських загроз для окремих підрозділів, здійснювати моніторинг дій окремих співробітників на робочих місцях, де, обробляється інформація з обмеженим доступом, проводити навчання зі співробітниками для поінформованості про інсайдерські загрози, отримувати доступ до інформації з окремих підрозділів для аналізу інсайдерської загрози та проводити самооцінку інсайдерських загроз в підрозділах.

Програми інсайдерських загроз можуть ініціювати створення груп, що займаються поводженням з інцидентами, які, можливо, уже наявні в організації, — таких як команди реагування на інциденти комп'ютерної безпеки. Записи стосовно кадрових ресурсів є особливо важливими (оскільки є переконливі докази, які свідчать про те, що деяким видам інсайдерських злочинів часто передує нетехнічна поведінка на робочому місці, включно з, наприклад, постійним незадоволенням і конфліктами з колегами). Однак використання записів стосовно поведінки кадрового складу може створювати значні ризики приватності. Має бути залучена юридична служба для забезпечення дотримання всіх вимог щодо приватності персональних даних.

Пов'язані заходи: AC-6, AT-2, AU-6, AU-7, AU-10, AU-12, AU-13, CA-7, IA-4, IR-4, MP-7, PE-2, PM-14, PM-16, PS-3, PS-4, PS-5, PS-7, PS-8, SC-7, SC-38, SI-4.

Посилення заходів: Немає.

Посилання: [EO 13587], [NITP12], [ODNI NITP].

## РМ-13 БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРАЦІВНИКІВ

Заходи захисту: Створити програму розвитку та вдосконалення спеціалістів з питань безпеки та приватності.

Рекомендації з реалізації: Програми розвитку та підвищення обізнаності спеціалістів з питань безпеки та приватності містять, наприклад, визначення знань, умінь і навичок, необхідних для виконання обов'язків і завдань безпеки та приватності, розробку навчальних програм на основі ролей для осіб, яким призначені ролі та обов'язки щодо безпеки та приватності, надання вказівок для вимірювання та побудови індивідуальних кваліфікацій для посадових осіб і кандидатів на посади, пов'язані з безпекою та приватністю. Програми заохочують організації наймати на посади з питань безпеки та приватності кваліфікованих працівників. Програми розвитку та підвищення обізнаності спеціалістів з питань безпеки та приватності доповнюють програми інформаційного забезпечення і навчання з питань безпеки та зосереджуються на інституціоналізації основних можливостей безпеки та приватності, підготовці персоналу щодо впровадження дій, необхідних для захисту операцій організації, активів і персональних даних.

Пов'язані заходи: AT-2, AT-3.

Посилення заходів: Немає.

Посилання: [OMB A-130], [SP 800-181].

## РМ-14 ТЕСТУВАННЯ, НАВЧАННЯ ТА МОНІТОРИНГ

Заходи захисту:

a. Впровадити процес забезпечення планів організації проведення тестування безпеки та приватності, навчання та моніторингу діяльності, пов'язаної з інформаційними системами організації, який:

    1. є розробленим та підтримується постійно;

    2. виконується своєчасно.

b. Перевіряти плани тестування, навчання та моніторингу для узгодженості з організаційною стратегією управління ризиками та загальноорганізаційними пріоритетами дій щодо реагування на ризик.

Рекомендації з реалізації: Цей захід захисту надає рекомендації щодо тестування безпеки та приватності, навчання та моніторингових заходів, що проводяться в масштабах усієї організації та допомагає гарантувати, що організації здійснюють нагляд за діяльністю з тестування, навчання та моніторингу, а також координують ці дії. Зі зростанням важливості програм постійного моніторингу, впровадження інформаційної безпеки та приватності на трьох рівнях ієрархії управління ризиками та широкого використання загальних заходів захисту, організації координують і консолідують заходи тестування та моніторингу, які регулярно проводяться як частина поточних оцінки, що підтримують різноманітні заходи захисту. Навчальні заходи з безпеки та приватності, які зосереджені на окремих системах і конкретних ролях, також потребують координації між усіма організаційними елементами. Плани та заходи

тестування, навчання та моніторингу базуються на поточних оцінках загроз і вразливості.

Пов'язані заходи: AT-2, AT-3, CA-7, CP-4, IR-3, PM-12, SI-4.

Посилення заходів: Немає.

Посилання: [OMB A-130], [SP 800-37], [SP 800-39], [SP 800-53A], [SP 800-115], [SP 800-137].

## PM-15 КОНТАКТИ З ГРУПАМИ ТА АСОЦІАЦІЯМИ З ПИТАНЬ БЕЗПЕКИ ІНФОРМАЦІЇ ТА ПРИВАТНОСТІ

Заходи захисту:
Створити та інституціоналізувати контакти між обраними групами та асоціаціями зі спільнотами безпеки та приватності для:

a. сприяння постійному навчанню та підготовці персоналу в галузі безпеки інформації та приватності;

b. підтримки ознайомленості з рекомендованими практиками безпеки інформації та приватності, техніками та технологіями;

c. розповсюдження поточної інформації про стан безпеки та приватності, включно із загрозами, вразливостями та інцидентами.

Рекомендації з реалізації: Постійний контакт з групами та асоціаціями з питань безпеки інформації та приватності має велике значення в умовах технологій і загроз, які швидко змінюються. До груп і асоціацій з питань безпеки інформації та приватності належать, наприклад, спеціальні групи за інтересами, професійні асоціації, форуми, новинарні групи та групи фахівців з безпеки інформації та приватності. Організації обирають групи та асоціації на основі місій і ділових функцій організації. Організації поділяють загрозу, вразливість та інформацію про інциденти, а також контекстуальні уявлення, методи дотримання та проблеми приватності, що відповідають чинним законам, наказам, директивам, політикам, правилам, стандартам та рекомендаціям.

Пов'язані заходи: SA-11, SI-5.

Посилення заходів: Немає.

Посилання: [OMB A-130].

## PM-16 ПРОГРАМА ІНФОРМУВАННЯ ПРО ЗАГРОЗИ

Заходи захисту:
Запровадити програму інформування про загрози, яка містить можливості спільного обміну інформацією між організаціями для аналізу загроз.

Рекомендації з реалізації: Через постійну мінливість і все більшу кваліфікацію порушників, шанси успішного порушення або компрометації систем, що належать організації різко зростають. Однією з найкращих методик для вирішення цієї проблеми є обмін інформацією про загрози, включаючи події загрози (тобто тактику, методики та процедури), які організації зазнали, пом'якшення, які організації виявили, та які

виявились ефективними проти певних видів загроз. Обмін інформацією про загрози може бути двостороннім або багатостороннім. Прикладами двостороннього обміну щодо загрози можуть бути державно-комерційні кооперативи та державно-урядові кооперативи. Прикладами багатостороннього обміну є організації, які беруть участь у консорціумах. Інформація про загрози може бути дуже чутливою (у такому разі необхідна наявність спеціальних угод між контрагентами щодо взаємного нерозголошення).

Пов'язані заходи: IR-4, PM-12.

Посилення заходів:

(1) ПРОГРАМА ІНФОРМУВАННЯ ПРО ЗАГРОЗИ - АВТОМАТИЗОВАНІ ЗАСОБИ ДЛЯ ОБМІНУ ІНФОРМАЦІЄЮ ПРО ЗАГРОЗИ

Використовувати автоматизовані засоби з метою максимізації ефективності обміну інформацією про виявлені загрози.

Рекомендації з реалізації: Для досягнення максимальної ефективності моніторингу важливо знати, яку загрозу та індикатори повинні шукати датчики. Використовуючи налагоджені сервіси та автоматизовані інструменти, організації значно покращують свою здатність швидко ділитися та передавати в засоби моніторингу виявлені загрози.

Пов'язані заходи: Немає.

Посилання: Немає.

## PM-17 ЗАХИСТ ПУБЛІЧНОЇ ІНФОРМАЦІЇ У ЗОВНІШНІХ СИСТЕМАХ

Заходи захисту:

a. Розробити політику та процедури для забезпечення того, щоб вимоги до захисту публічної (некласифікованої) інформації, яка обробляється, зберігається або передається у зовнішніх системах, здійснювалися відповідно до чинного законодавства.

b. Оновлювати політику та процедури [*Призначення: з визначеною організацією частотою*].

Рекомендації з реалізації: Контрольована некласифікована інформація визначається Національною адміністрацією архівів та записів разом із вимогами захисту та розповсюдження такої інформації та кодифікується в [32 CFR 2002], а спеціально для систем, зовнішніх для федеральної організації, 32 CFR 2002.14H. Політика прописує конкретне використання та умови, які повинні бути реалізовані відповідно до процедур організації, включаючи його договірні процеси.

Пов'язані заходи: CA-6, PM-10.

Посилення заходів: Немає.

Посилання: [32 CFR 2002], [SP 800-171], [SP 800-172], [NARA CUI].

## РМ-18 ПРОГРАМА (КОНЦЕПЦІЯ) ЗАБЕЗПЕЧЕННЯ ПРИВАТНОСТІ

Заходи захисту:

a. Розробити та поширити загальноорганізаційну програму (концепцію) забезпечення приватності, яка:

   1. містить опис структури програми забезпечення приватності та ресурсів, призначених для її реалізації;

   2. містить огляд вимог до забезпечення приватності й опис засобів управління програмою забезпечення приватності та загальних заходів захисту, встановлених або запланованих для задоволення цих вимог;

   3. визначає обов'язки посадової особи щодо приватності, а також визначає обов'язки інших посадових осіб і персоналу з питань забезпечення приватності;

   4. описує зобов'язання керівництва, стратегічні цілі та завдання програми забезпечення приватності;

   5. відображає координацію між організаційними структурами, відповідальними за різні аспекти приватності;

   6. затверджена високопосадовцем, який є відповідальним (та підзвітним) за: управління ризиками приватності, що виникають при здійсненні операцій організації (включно із завданнями, функціями, іміджем і репутацією); організаційними активами, фізичними особами, іншими організаціями та країнами.

b. Оновлювати програму [*Призначення: за визначеною організацією частотою*], а також в разі змін законодавства, змін в організації і виявлення проблем в ході реалізації програми або оцінювання заходів приватності.

Рекомендації з реалізації: Програма приватності — це документ, який описує: структуру програми приватності; ресурсів, присвячених програмі приватності; ролі старшої посадової особи щодо приватності, а також визначає обов'язки інших посадових осіб і персоналу з питань забезпечення приватності, стратегічні цілі та завдання програми приватності, управління програмами та загальний контроль, що існує або планується для задоволення чинних вимог приватності та управління ризиками приватності. Програма приватності може бути інтегрована з планами захисту інформації або може бути представлена самостійно.
Старша посадова особа з питань приватності несе відповідальність за загальні, специфічні та гібридні заходи захисту щодо забезпечення приватності в організації та управління програмами приватності. Програми приватності мають містити достатньо інформації щодо управління та загальних заходів захисту (включно зі специфікацією параметрів). Плани захисту персональних даних окремих систем та плани приватності для всієї організації разом мають повністю охоплювати всі заходи захисту, що застосовуються в організації для забезпечення конфіденційності.
Заходи захисту програми приватності, як правило, впроваджуються на рівні організації та є важливими для її керування в організації. Вони відрізняються від звичайних, специфічних та гібридних заходів захисту, оскільки не залежать від конкретної інформаційної системи. Разом плани приватності для окремих систем і план програми приватності для всієї організації забезпечують повне охоплення заходів захисту щодо

конфіденційності в організації.

Організації на власний розсуд вирішують, чи описувати загальні заходи захисту в одному документі, чи в декількох. Якщо програма приватності містить кілька документів, організація вказує в кожному документі організаційну посадову особу, відповідальну за розробку, реалізацію, оцінювання та моніторинг відповідних загальних заходів захисту.

Загальні заходи захисту мають бути задокументовані в додатку до програми приватності організації, якщо вони не внесені в окремий план. План програми приватності для всієї організації вказує, які окремі плани приватності містять опис заходів захисту для забезпечення конфіденційності.

Пов'язані заходи: PM-8, PM-9, PM-19.

Посилення заходів: Немає.

Посилання: [PRIVACT], [OMB A-130].

## PM-19 КЕРІВНІ РОЛІ ПРОГРАМИ ПРИВАТНОСТІ

Заходи захисту:
Призначити старшу посадову особу з питань забезпечення приватності з повноваженнями, завданням, підзвітністю і ресурсами для координації, розробки та реалізації відповідних вимог забезпечення приватності й управління ризиками приватності в рамках програми забезпечення приватності всієї організації.

Рекомендації з реалізації: Офіцер з питань приватності має бути штатним працівником організації. Для органів державної влади відповідно до законів, указів, директив, нормативних актів, стандартів та рекомендацій – ця особа призначається старшою посадовою особою органу з питань приватності. Організації також можуть називати цю посадову особу головним офіцером з питань приватності. Старша посадова особа органу з питань приватності також входить до складу комісії (ради) з управління даними (див. PM-23) та комісії (ради) з цілісності даних (див. PM-24).

Пов'язані заходи: PM-18, PM-20, PM-23, PM-24, PM-27.

Посилення заходів: Немає.

Посилання: [OMB A-130].

## PM-20 СИСТЕМА ЗАПИСІВ ПРОГРАМИ ПРИВАТНОСТІ

Заходи захисту: підтримувати центральну вебсторінку ресурсу на головному загальнодоступному вебсайті організації, яка слугує центральним джерелом інформації про програму приватності організації та яка:

a. забезпечує доступ громадськості до інформації про діяльність щодо забезпечення приватності в організації та можливість комунікації з уповноваженою посадовою особою з питань забезпечення приватності;

b. оприлюднює організаційну політику забезпечення приватності на вебсайті організації або іншим чином;

c. використовує публічні адреси електронної пошти та/або телефонні лінії, щоб дати можливість громадськості надавати відгуки та/або направляти запитання щодо програми приватності в організації.

Рекомендації з реалізації: Для органів державної влади вебсторінки мають розташовуватися на домені .gov.ua. Органи державної влади включають оцінку впливу на публічну приватність, систему сповіщень про записи, повідомлення та угоди, винятки та правила впровадження, звіти про конфіденційність, політику конфіденційності, інструкції для осіб, які надсилають запити на доступ або зміни, адреси електронної пошти для запитань/скарг, блоги, періодичні видання.

Пов'язані заходи: AC-3, PM-19, PT-5, PT-6, PT-7, RA-8.

Посилення заходів:

(1) СИСТЕМА ЗАПИСІВ ПРОГРАМИ ПРИВАТНОСТІ - ПОЛІТИКА ПРИВАТНОСТІ ВЕБСАЙТІВ, ДОДАТКІВ І ЦИФРОВИХ ПОСЛУГ

Розробити та опублікувати політику конфіденційності на всіх зовнішніх вебсайтах, у мобільних додатках та інших цифрових службах, яка:

a) написана простою мовою та організована так, щоб її було легко зрозуміти та впроваджувати;

b) надає інформацію, необхідну громадськості для прийняття обґрунтованого рішення про те, як взаємодіяти з організацією;

c) оновлюються щоразу, коли організація вносить суттєві зміни до політики, яку вона описує, і включає позначку часу/дати для інформування громадськості про дату останніх змін.

Рекомендації з реалізації: Організації публікують політику приватності на всіх зовнішніх вебсайтах, у мобільних додатках та інших цифрових службах. Організації розміщують посилання на відповідну політику приватності на будь-яких відомих основних точках входу на вебсайт, додатках чи цифрових сервісах. Крім того, організації надають посилання на політику приватності на будь-якій вебсторінці, яка збирає персональні дані. На організації можуть поширюватися відповідні закони, виконавчі накази, директиви, нормативні акти чи політики, які вимагають надання певної інформації громадськості. Персонал організації консультується зі старшим представником агентства з приватності та юрисконсультантом щодо таких вимог.

Пов'язані заходи: Немає.

Посилання: [PRIVACT], [OMB A-130], [OMB M-17-06].

## PM-21 ОБЛІК РОЗКРИТТЯ ПЕРСОНАЛЬНИХ ДАНИХ

Заходи захисту:

a. Забезпечити доступ громадськості до інформації із забезпечення приватності в організації та можливість комунікації з уповноваженою посадовою особою з питань забезпечення приватності щодо:

1. дати, характеру та мети кожного розкриття запису;

2. імені та адреси особи або організації, щодо яких було зроблено розкриття даних.

b. Обліковувати та зберігати випадки розкриття персональних даних протягом терміну дії запису або п’яти років після розкриття інформації.

c. Здійснювати облік випадків розкриття персональних даних, доступних особі, зазначеній у записі за запитом.

Рекомендації з реалізації: Облік випадків розкриття персональних даних полягає в тому, щоб дозволити особам дізнатися, кому були розкриті записи про них; створити основу для подальшого консультування одержувачів записів будь-яких виправлених або оскаржених записів; надати аудиту відомості для наступних перевірок відповідності організацій щодо виконання умов розкриття інформації. Для органів державної влади облік та зберігання випадків розкриття персональних даних є обов'язковим згідно з [PRIVACT]; організації повинні звернутися до старшою посадової особи з питань приватності та юрисконсультанта з таких питань і бути обізнаними з законодавчими винятками та дорученнями OMB, пов'язаними з цим положенням.
Організації можуть використовувати будь-яку систему для зберігання записів про випадки розкриття, якщо з неї можна скласти документ зі списком всіх випадків розкриття разом з іншою необхідною інформацією. Також можливе використання автоматизованих механізмів для визначення часу розкриття персональних даних, включаючи комерційні сервіси, які надають сповіщення та повідомлення. Облік випадків розкриття також може бути використаний для допомоги організаціям у перевірці дотримання вимог законодавства з питань приватності та політик щодо розкриття або поширення персональних даних та обмежень щодо їх розповсюдження.

Пов’язані заходи: AC-3, AU-2, PT-2.

Посилення заходів: Немає.

Посилання: Немає.

## PM-22 УПРАВЛІННЯ ЯКІСТЮ ПЕРСОНАЛЬНИХ ДАНИХ

Заходи захисту:
Розробити та задокументувати загальноорганізаційну політику та процедури, які довзолять:

a. Проводити огляд точності, актуальності, своєчасності та повноти персональних даних протягом їх життєвого циклу;

b. Коригувати або видаляти неточну або застарілу інформацію;

c. Інформувати осіб або інші відповідні організації про внесення змін або видалення персональної інформації;

d. Оскаржувати відмови на запити щодо коригування чи видалення.

Рекомендації з реалізації: Настанови щодо Управління якістю персональних даних містять обґрунтовані кроки, які організації вживають для підтвердження точності й актуальності персональних даних, що визначаються протягом її життєвого циклу. Життєвий цикл персональних даних містить: створення, збір, використання, обробку,

зберігання, обслуговування, розповсюдження, розкриття та розміщення персональних даних. Організаційні політики та процедури для управління якістю персональних даних є важливими, оскільки неточні або застарілі персональні дані, які зберігаються організаціями, можуть створювати проблеми для осіб. Організації розглядають якість персональних даних, які задіяні в бізнес-функціях, де неточна інформація може призвести до негативних рішень або відмови у послугах та пільгах, або розкриття такої інформації може призвести до негативних наслідків. У певних обставинах правильна інформація може створювати проблеми для особи, тому організації розглядають створення політик та процедур для видалення такої інформації.
Старша посадова особа з питань приватності забезпечує наявність практичних засобів та механізмів, які є доступними для осіб або їх уповноважених представників для звернення щодо виправлення або видалення персональних даних. Процеси виправлення або видалення даних чітко визначені та доступні для громадськості.
Організації використовують обгрунтований (дискреційний) підхід до визначення, чи слід видаляти або виправляти дані на основі обсягу запитів щодо запропонованих змін, та наслідків таких змін. Крім того, процеси включають надання відповідей особам щодо відмови у запитах на виправлення або видалення. У відповіді наводяться причини прийнятих рішень, забезпечується можливість реєстрації індивідуальних скарг на ці рішення та запитів на перегляд початкових визначень.
Для забезпечення прозорості та підтвердження виконаних дій, організації повідомляють осіб або їх уповноважених представників, коли персональна інформація цих осіб була виправлена або видалена.

Пов’язані заходи: PM-23, SI-18.

Посилання: [OMB A-130], [OMB M-19-15], [SP 800-188].

## PM-23 ОРГАН УПРАВЛІННЯ ПЕРСОНАЛЬНИМИ ДАНИМИ

Заходи захисту: створити орган управління персональними даними, на якого покладено [*Призначення: визначені організацією функції*] та виконання [*Призначення: визначені організацією обов’язки*].

Рекомендації з реалізації: Орган управління персональними даними може допомогти забезпечити наявність злагоджених політик у організації та можливість дотримання балансу між використанням даних та вимогами щодо забезпечення їх безпеки та приватності. Орган з управління персональними даними встановлює політики, процедури та стандарти, що сприяють управлінню даними таким чином, щоб персональні дані були ефективно контрольовані та зберігалися відповідно до чинного законодавства, виконавчих наказів, директив, політик, стандартів та рекомендацій. Обов'язки можуть включати розробку та впровадження рекомендацій, що підтримують моделювання даних, якість, цілісність та потреби у деідентифікації персональних даних на всіх етапах їх життєвого циклу, а також перегляд та затвердження заявок на надання даних за межі організації, архівування заявок, проведення моніторингу після надання даних для гарантування того, що прийняті рішення на підставі даних залишаються актуальними та обгрунтованими. До складу органу управління персональними даними входять керівник інформаційної служби, старша посадова особа з інформаційної безпеки та старша посадова особа з питань приватності. Органи державної влади повинні створити Орган з управління персональними даними з конкретними функціями та обовязками згідно з [EVIDACT] та політиками, встановленими згідно з [OMB M-19-23].

Пов’язані заходи: AT-2, AT-3, PM-19, PM-22, PM-24, PT-7, SI-4, SI-19.

Посилення заходів: Немає.

Посилання: [EVIDACT], [OMB A-130], [OMB M-19-23], [SP 800-188].

## PM-24 ОРГАН З ПИТАНЬ ЦІЛІСНОСТІ ДАНИХ

Заходи захисту:
Створити орган з питань цілісності даних для здійснення:

a. Розгляду пропозицій щодо проведення відповідної програми або участі у ній.

b. Проведення огляду усіх поточних програм, в яких бере участь організація.

Рекомендації з реалізації: Орган з питань цілісності даних – це орган, який складається зі старших посадових осіб, які призначені керівником органу державної влади і який відповідає за огляд пропозицій щодо проведення або участі у програмі відповідності та здійснення щорічного огляду всіх програм відповідності, в яких орган брав участь. Загалом, програма відповідності - це комп'ютерне порівняння записів з двох або більше автоматизованих систем записів [PRIVACT], які зберігаються не в органі державної влади (або його представника). Програма порівняння пов'язана з державними програмами соціальних вигод або державними записами про персонал та заробітну плату. Як мінімум, до складу органу з питань цілісності даних входять генеральний інспектор відповідного відомства та старша посадова особа з питань приватності.

Пов’язані заходи: AC-4, PM-19, PM-23, PT-2, PT-8.

Посилення заходів: Немає.

Посилання: [PRIVACT], [OMB A-130], [OMB A-108].

## PM-25 МІНІМІЗАЦІЯ КІЛЬКОСТІ ПЕРСОНАЛЬНИХ ДАНИХ, ЩО ВИКОРИСТОВУЮТЬСЯ ПІД ЧАС ТЕСТУВАННЯ, НАВЧАННЯ ТА ДОСЛІДЖЕНЬ

Заходи захисту:

a. Розробити та впровадити політики та процедури, спрямовані на врегулювання питань використання персональних даних для внутрішнього тестування, навчання та досліджень.

b. Вжити заходи щодо обмеження або зведення до мінімуму кількості персональних даних, які використовуються для внутрішнього тестування, навчання та досліджень.

c. Надавати дозвіл на використання персональних даних, коли така інформація вимагається для внутрішнього тестування, навчання і досліджень.

d. Здійснювати огляд та оновлення політик та процедур, спрямованих на врегулювання питань використання персональних даних для внутрішнього тестування, навчання та досліджень [*Призначення: з визначеною організацією частотою*].

Рекомендації з реалізації: Організації часто використовують персональні дані для тестування нових застосунків чи систем, для наукових цілей та навчання. Використання

персональних даних для тестування, досліджень і навчання збільшує ризик несанкціонованого розголошення або неправомірного використання таких даних. Організації мають консультуватися зі старшою посадовою особою з питань приватності та юридичним відділом, щоб переконатися, що використання персональних даних для тестування, навчання та досліджень є сумісним з початковою метою, для якої вони були зібрані. За можливості, організації використовують заповнювачі даних для уникнення розголошення персональних даних під час проведення тестування, навчання та досліджень.

Пов'язані заходи: PM-23, PT-3, SA-3, SA-8, SI-12.

Посилення заходів: Немає.

Посилання: [OMB A-130].

## PM-26 УПРАВЛІННЯ СКАРГАМИ

Заходи захисту:
Впровадити процес отримання та реагування на скарги, проблеми чи запитання від фізичних осіб щодо організаційної практики забезпечення приватності, який охоплює:

a. механізми, які легко використовувати та які є легкодоступними для громадськості;

b. усю інформацію, необхідну для успішного подання скарг;

c. механізми відстеження, що забезпечують отримання всіх скарг та їх вчасний і належний розгляд протягом [*Призначення: визначений організацією період часу*];

d. підтвердження отримання скарг, заявлених проблем чи запитань від фізичних осіб протягом [*Призначення: визначений організацією період часу*];

e. надання відповідей на отримані скарги, заявлені проблеми чи запитання від фізичних осіб протягом [*Призначення: визначений організацією період часу*].

Рекомендації з реалізації: Скарги та запити фізичних осіб можуть слугувати цінним джерелом зворотнього зв'язку для організації, що дозволяє поліпшити операційні моделі, використання технологій, практики збору даних, а також контроль приватності й безпеки. До механізмів, які можуть бути використані для зворотного зв'язку, належать: електронна пошта, телефонна гаряча лінія або вебформи.

Пов'язані заходи: IR-7, IR-9, PM-22, SI-18.

Посилення заходів: Немає.

Посилання: [OMB A-130].

## PM-27 ЗВІТНІСТЬ З ПИТАНЬ ЗАБЕЗПЕЧЕННЯ ПРИВАТНОСТІ

Заходи захисту:

a. Розробити [*Призначення: визначені організацією звіти з питань забезпечення приватності*] та надати:

1. [*Завдання: наглядові органи, визначені організацією*] для перевірки дотримання вимог законодавства, а також визначених регуляторними актами та нормативними документами, розробленими відповідно до політики конфіденційності;

2. [*Призначення: посадові особи, визначені організацією*] та інший персонал, відповідальний за моніторинг дотримання програми приватності.

b. Переглядати і оновлювати звіти з питань забезпечення приватності [*Призначення: частота, визначена організацією*].

Рекомендації з реалізації: Внутрішня та зовнішня звітність з питань забезпечення приватності допомагає організаціям забезпечувати відповідальність та прозорість в операціях з персональними даними. Надання звітності також може допомогти організаціям визначити прогрес у виконанні вимог щодо забезпечення приватності та контролю, порівнювати результати з іншими урядовими органами, виявляти вразливості, ідентифікувати недоліки в політиці та її реалізації, а також виявляти ефективні моделі забезпечення приватності. Для органів державної влади звіти з питань забезпечення приватності включають щорічні звіти старшої посадової особи агентства з питань приватності до OMB, звіти до Конгресу, які вимагаються регулюючими документами Закону про комісію 9/11 та інші публічні звіти, які вимагаються законом, регулюванням або політикою, включаючи внутрішні політики організації. Старша посадова особа агентства з питань приватності консультується з юрисконсультантами, за необхідності, щоб забезпечити дотримання всіх відповідних вимог щодо звітності про забезпечення приватності

Пов'язані заходи: IR-9, PM-19.

Посилення заходів: Немає.

Посилання: [FISMA], [OMB A-130], [OMB A-108].

## PM-28 ОЦІНКА РИЗИКІВ

Заходи захисту:

a. Визначити та задокументувати:

1. припущення, що впливають на оцінку ризиків, реагування на ризики та моніторинг ризиків;

2. обмеження, що впливають на оцінку ризиків, реагування на ризики та моніторинг ризиків;

3. пріоритети та компроміси, які розглядаються організацією для здійснення управління ризиками;

4. стійкість організації до ризиків.

b. Поінформувати [*Призначення: визначений організацією персонал*] про результати визначення ризиків.

c. Переглядати та оновлювати підходи щодо визначення ризиків [*Призначення: з визначеною організацією частотою*].

Рекомендації з реалізації: Оцінка ризиків є найбільш ефективною, коли проводиться на рівні організації з консультацією зацікавлених сторін всієї організації, включаючи організаторів місії, бізнесу та систем. Оцінка ризиків, відповідь на ризики та моніторинг ризиків ґрунтуються на стратегії управління ризиками, яка формується на основі припущень, обмежень, рівня прийняття ризику, пріоритетів та компромісів, визначених у процесі оцінки ризиків. Результати оцінки ризиків передаються персоналу організації, включаючи власників(організаторів) місії та бізнесу, власників інформації, систем, уповноважених посадових осіб, старшої посадової особи з питань приватності, старшоїпосадової особи з питань управління ризиками.

Пов'язані заходи: CA-7, PM-9, RA-3, RA-7.

Посилення заходів: Немає.

Посилання: [OMB A-130], [SP 800-39].

## PM-29 РОЛІ КЕРІВНИКІВ ПРОГРАМИ УПРАВЛІННЯ РИЗИКАМИ

Заходи захисту:

a. Призначити старшу посадову особу, відповідальну за управління ризиками, для узгодження процесів управління організації інформаційною безпекою та приваністю, включаючи процеси планування стратегії, фінансування, діяльності організації;

b. Створити посаду відповідального за управління ризиками (або покласти відповідні обов'язки на посадову особу організації) з метою розгляду та аналізу ризиків з точки зору всієї організації та забезпечення узгодженого управління ризиками в межах всієї організації.

Рекомендації з реалізації: Відповідальна старша посадова особа з питань управління ризиками очолює виконавчу (функціональну) службу з питань управління ризиками в організації.

Пов'язані заходи: PM-2, PM-19.

Посилення заходів: Немає.

Посилання: [SP 800-37], [SP 800-181].

## PM-30 ПЛАН УПРАВЛІННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ

Заходи захисту:

a. Розробити план управління ризиками ланцюга постачання, пов'язаного з розробкою, придбанням, обслуговуванням та утилізацією систем, компонентів системи та послуг для системи.

b. Реалізувати план управління ризиками ланцюга постачання послідовно та наскрізно по всій організації.

c. Переглядати й оновлювати план управління ризиками ланцюга постачання [*Призначення: з визначеною організацією частотою*] або, якщо потрібно, у разі змін в організації.

Рекомендації з реалізації: План управління ризиками ланцюга постачання на рівні організації включає чітке визначення інтересів та стійкості щодо ризиків ланцюга постачання для організації, прийнятні стратегії або контроль за ризиками ланцюга постачання, процес постійної оцінки та моніторингу ризиків ланцюга постачання, підходи до впровадження та комунікації стратегії управління ризиками ланцюга постачання, а також пов'язані з цим ролі та відповідальності. Управління ризиками ланцюга постачання включає врахування ризиків безпеки та приватності, пов'язаних з розробкою, придбанням, підтримкою та видаленням систем, компонентів систем та послуг для системи. План управління ризиками ланцюга постачання можна включити до загального плану управління ризиками організації та використовувати його для керування та надання інформації щодо політик управління ризиками ланцюга постачання та планів управління ризиками ланцюга на рівні системи. Крім того, використання послуг спеціаліста з ризик-менеджменту може допомогти забезпечити послідовне, широкомасштабне застосування стратегії управління ризиками в ланцюгу постачання на рівні організації. План управління ризиками ланцюга постачання впроваджується на рівні організації, а також місії/бізнесу, тоді як план управління ризиками ланцюга постачання (див. SR-2) впроваджується на рівні системи.

Пов’язані заходи: CM-10, PM-9, SR-1, SR-2, SR-3, SR-4, SR-5, SR-6, SR-7, SR-8, SR-9, SR-11.

Посилення заходів:

(1) ПЛАН УПРАВЛІННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ – ПОСТАЧАННЯ КРИТИЧНОВАЖЛИВИХ ТОВАРІВ АБО ТОВАРІВ, ЩО МАЮТЬ ВАЖЛИВЕ ЗНАЧЕННЯ ДЛЯ ДІЯЛЬНОСТІ ОРГАНІЗАЦІЇ

Виявляти, визначати пріоритети та оцінювати постачальників критичноважливих технологій, продуктів та послуг, в тому числі тих, які мають важливе значення для діяльності організації.

Рекомендації з реалізації: Визначення та пріоритезація постачальників критичних або невідкладних технологій, продуктів та послуг є надзвичайно важливим для успіху місії/бізнесу організації. Оцінка постачальників проводиться за допомогою оглядів постачальників (див. SR-6) та процесів оцінки ризиків ланцюга постачання (див. RA-3(1)). Аналіз ризиків ланцюга постачання може допомогти організації визначити системи або компоненти, для яких потрібні додаткові засоби мінімізації ризиків ланцюга постачання.

Пов’язані заходи: RA-3, RA-6.

Посилання: [PRIVACT], [FASC18], [EO 13873], [41 CFR 201], [OMB A-130], [OMB M-17-06] [CNSSD 505], [ISO 27036], [ISO 20243], [SP 800-161], [IR 8272].

## PM-31 ПЛАН БЕЗПЕРЕРВНОГО МОНІТОРИНГУ

Заходи захисту:

Розробити план безперервного моніторингу в масштабах всієї організації та впровадити програми безперервного моніторингу, які включають:

a. Встановити відповідні показників для моніторингу в масштабах всієї організації

[*Призначення: визначені організацією показники*];

b. Встановити [*Призначення: частота, визначеної організацією*] для здійснення моніторингу та [*Призначення: періодичність, визначена організацією*] проведення оцінки ефективності контролю;

c. Постійний моніторинг визначених організацією показників відповідно до стратегії безперервного моніторингу;

d. Співставлення та аналіз інформації, отриманої в результаті здійснення моніторингу, та контрольних оцінок;

e. Заходи реагування на результати аналізу оцінок контролю та моніторингових даних;

f. Звітування про стан безпеки та приватності систем організації перед [*Призначення: визначеним організацією персоналом чи посадовою особою*] [*Призначення: з визначеною організацією періодичністю*].

Рекомендації з реалізації: Постійний моніторинг на рівні організації сприяє постійній увазі до стану безпеки та приватності в організації для підтримки ризик-менеджменту та прийняття рішень організації. Термін "постійний" означає, що організації оцінюють та моніторять свої заходи захисту та ризики з достатньою частотою для підтримки прийняття рішень на основі ризику. Різні типи заходів захисту можуть вимагати різної частоти моніторингу. Постійний моніторинг дозволяє організаціям керувати ризиками та реагувати на них, використовуючи результати моніторингу. Програми постійного моніторингу дозволяють організаціям підтримувати авторизацію систем та загальних заходів захисту в динамічних середовищах експлуатації з мінливими умовами щодо потреб місії та бізнесу, загроз, вразливостей та технологій. Можливість отримання постійного доступу до інформації, пов'язаної з безпекою та приватністю, через звіти та інформаційні панелі дає посадовим особам організації змогу приймати ефективні, своєчасні та обґрунтовані рішення щодо управління ризиками, включаючи постійну авторизацію. Для подальшого сприяння управлінню ризиками безпеки та приватності, організації розглядають можливість вирівнювання організаційно визначених метрик моніторингу з організаційною стійкістю до ризиків, визначеною планом управління ризиками. Вимоги до моніторингу, включаючи необхідність проведення самого моніторингу, можуть бути згадані в інших заходах захисту та їх посиленнях, таких як: AC-2g, AC-2(7), AC-2(12)(a), AC-2(7)(b), AC-2(7)(c), AC-17(1), AT-4a, AU-13, AU-13(1), AU-13(2), CA-7, CM-3f, CM-6d, CM-11c, IR-5, MA-2b, MA-3a, MA-4a, PE-3d, PE-6, PE-14b, PE-16, PE-20, PM-6, PM-23, PS-7e, SA-9c, SC-5(3)(b), SC-7a, SC-7(24)(b), SC-18b, SC-43b, SI-4.

Пов’язані заходи: AC-2, AC-6, AC-17, AT-4, AU-6, AU-13, CA-2, CA-5, CA-6, CA-7, CM-3, CM-4, CM-6, CM-11, IA-5, IR-5, MA-2, MA-3, MA-4, PE-3, PE-6, PE-14, PE-16, PE-20, PL-2, PM-4, PM-6, PM-9, PM-10, PM-12, PM-14, PM-23, PM-28, PS-7, PT-7, RA-3, RA-5, RA-7, SA-9, SA-11, SC-5, SC7, SC-18, SC-38, SC-43, SI-3, SI-4, SI-12, SR-2, SR-4.

Посилення заходів: Немає.

Посилання: [SP 800-37], [SP 800-39], [SP 800-137], [SP 800-137A].

## PM-32 ПРИЗНАЧЕННЯ

Заходи захисту:

Аналізувати [*Призначення: визначені організацією системи чи системні компоненти*], які підтримують важливі для місії послуги чи функції, щоб гарантувати, що інформаційні ресурси використовуються відповідно до їх призначення.

Рекомендації з реалізації: Системи призначені для підтримки конкретної місії або бізнес-функції. Однак з часом системи та компоненти систем можуть використовуватися для підтримки послуг та функцій, які виходять за межі передбаченого місією чи бізнес-функцією. Таке використання може спричинити ризики витоку інформації у небажані середовища, що значно збільшить загрозу безпеці. При цьому системи стають більш вразливими до компрометації, що може вплинути на послуги та функції, для яких вони призначені. Це особливо впливає на послуги та функції, що є невідкладними для виконання місії. Шляхом аналізу використання ресурсів, організації можуть виявити такі можливі вразливості.

Пов'язані заходи: CA-7, PL-2, RA-3, RA-9.

Посилення заходів: Немає.

Посилання: [SP 800-160-1], [SP 800-160-2]

## 10.14 Клас заходів захисту PS — КАДРОВА БЕЗПЕКА

### PS-1 ПОЛІТИКА ТА ПРОЦЕДУРИ КАДРОВОЇ БЕЗПЕКИ

Заходи захисту:

a. Розробити, задокументувати та поширити серед [*Призначення: визначених організацією персоналу або ролей*]:

   1. [*Впровадити (одну або декілька): на рівні організації, на рівні місії/бізнес процесу, на рівні системи*] політику кадрової безпеки, яка:

      (a) містить мету, сферу застосування, ролі, обов'язки, відповідальність керівництва, координацію між організаційними підрозділами та систему контролю відповідності (complaince);

      (b) відповідає чинному законодавству, виконавчим наказам, директивам, нормам, політикам, стандартам та рекомендаціям.

   2. Процедури, що сприяють здійсненню політики кадрової безпеки та пов'язаних з ними заходів кадрової безпеки.

b. Призначити [*Призначення: визначену організацією посадову особу*] для управління розробкою, документуванням та впровадженням політики та процедур кадрової безпеки.

c. Переглядати та оновлювати:

   1. Поточну політику кадрової безпеки [*Призначення: з визначеною організацією частотою*] та подальші заходи, визначені організацію.

   2. Поточні процедури кадрової безпеки [*Призначення: з визначеною організацією частотою*] та подальші заходи, визначені організацію.

Рекомендації з реалізації: Цей захід захисту стосується встановлення політики та процедур для ефективного здійснення заходів і їх посилень у класі PS. Стратегія управління ризиками є важливим фактором у встановленні політики та процедур. Комплексна політика та процедури допомагають забезпечити безпеку та приватність. За наявності політики, а також планів захисту інформації та персональних даних на рівні організації, конкретні системні політики та процедури можуть бути не потрібні. Політика може бути внесена до складу загальної політики безпеки та приватності або може бути представлена кількома політиками (у випадках складної архітектури). Процедури описують, як має реалізуватися політика чи заходи захисту та як вони можуть бути спрямовані на персонал або роль, яка є об'єктом процедури. Процедури можуть бути задокументовані в планах захисту інформації та персональних даних (як один або декілька документів). Події, що можуть послужити приводом для оновлення політики та процедур з персональної безпеки, включають, але не обмежуються оціночними або висновками аудиту, інцидентами або порушеннями безпеки, змінами відповідних законів, указів, директив, нормативних актів, політик, стандартів та рекомендацій. Просте повторення заходів захисту не вважається організаційною політикою чи процедурою

Пов'язані заходи: PM-9, PS-8, SI-12.

Посилення заходів: Немає.

Посилання: [SP 800-12], [SP 800-30], [SP 800-39], [SP 800-100].

## PS-2 ВИЗНАЧЕННЯ ПОСАДОВОГО РИЗИКУ

Заходи захисту:

a. Визначити ризики для всіх посад організації.

b. Встановити критерії відбору осіб, які заміщують ці посади.

c. Переглядати та оновлювати посадові ризики [*Призначення: з визначеною організацією частотою*].

Рекомендації з реалізації: Класифікації ризику посад відображають політику та рекомендації Офісу з питань управління персоналом (OPM). Правильна класифікація посад є основою ефективної та послідовної оцінки придатності персоналу та програми забезпечення його безпеки. Система класифікації посад (PDS) оцінює обов'язки та відповідальність посади для визначення ступеня потенційної шкоди ефективності або цілісності служби, що може бути завдана через невірні дії посадової особи, та встановлює рівень ризику для цієї посади. Оцінка PDS також визначає, чи можуть обов'язки та відповідальність посади створити потенційний негативний вплив на національну безпеку та встановлює рівень чутливості такої посади. Результати оцінки визначають, який рівень перевірки проводиться для посади. Класифікації ризику можуть впливати на типи дозволів, які отримують особи під час доступу до інформаційних ресурсів та систем організації. Критерії відбору посад включають вимоги щодо призначення явних ролей із захисту інформації. Частини 1400 та 731 Загального кодексу федеральних регуляцій, Заголовок 5, встановлюють вимоги для організацій щодо оцінки відповідальних посад на відповідність рівню чутливості та ризику відповідно до їх обов'язків і відповідальності.

Пов’язані заходи: AC-5, AT-3, PE-2, PE-3, PL-2, PS-3, PS-6, SA-5, SA-21, SI-12.

Посилення заходів: Немає.

Посилання: [5 CFR 731], [SP 800-181].

## PS-3 ПЕРЕВІРКА ПЕРСОНАЛУ

Заходи захисту:

a. Перевіряти окремих осіб перед дозволом на доступ до інформаційної системи.

b. Переглядати окремих осіб відповідно до [*Призначення: визначених організацією умов, що вимагають перегляду, та якщо це визначено необхідною частотою повторного перегляду*].

Рекомендації з реалізації: Діяльність щодо перевірки персоналу має проводитися з урахуванням чинного законодавства, а також конкретних критеріїв, встановлених для визначення посадового ризику призначених на посади осіб. Організації можуть визначати різні умови доступу персоналу до систем на основі типів інформації, що обробляються, зберігаються або передаються системами. Прикладами перевірки персоналу є виявлення наявності судимостей та перевірки відповідних відомостей у відповідних органах. Організації можуть встановлювати різні умови та частоту

повторної перевірки персоналу, який отримує доступ до систем, в залежності від типів інформації, яку обробляють, зберігають або передають ці системи.

Пов'язані заходи: AC-2, IA-4, MA-5, PE-2, PM-12, PS-2, PS-6, PS-7, SA-21.

Посилення заходів:

(1) ПЕРЕВІРКА ПЕРСОНАЛУ - ІНФОРМАЦІЯ З ОБМЕЖЕНИМ ДОСТУПОМ

Переконатися, що особи, які мають доступ до інформаційної системи, що обробляє, зберігає або передає інформацію з обмеженим доступом, є перевіреними та уповноваженими на доступ до найвищої категорії критичності інформації, до якої вони мають доступ в інформаційній системі.

Рекомендації з реалізації: Інформація з обмеженим доступом є найбільш чутливою інформацією, яку органи державної влади обробляють, зберігають або передають. Необхідно мати відповідний рівень допуску та доступу до системи, що обробляє інформацію з обмеженим доступом, перед тим, як мати доступ до такої інформації. Дозволи на доступ забезпечуються заходом захисту з питань забезпечення доступу до систем (див. AC-3) та управління інформаційними потоками (див. AC-4).

Пов'язані заходи: AC-3, AC-4.

(2) ПЕРЕВІРКА ПЕРСОНАЛУ - ІНСТРУКТАЖ

Переконатися, що особи, яким передбачається надати доступ до системи, де обробляється, зберігається або передається інформація з обмеженим доступом, пройшли відповідний офіційний інструктаж про всі відповідні типи інформації, до якої вони отримають доступ в системі.

Рекомендації з реалізації: До типів інформації, для доступу до якої необхідне проходження спеціального інструктажу, належить будь-яка інформація з обмеженим доступом (персональні дані, критична інформація, таємна інформація).

Пов'язані заходи: AC-3, AC-4.

(3) ПЕРЕВІРКА ПЕРСОНАЛУ - ІНФОРМАЦІЯ, ЩО ПОТРЕБУЄ ДОДАТКОВИХ ЗАХОДІВ ЗАХИСТУ

Переконатися, що особи, які звертаються до ІС та які зберігають, обробляють або передають інформацію, що потребує додаткових заходів захисту:

(a) мають чинний дозвіл на доступ, який відповідає законам, наказам, настановам, директивам тощо;

(b) задовольняють [*Призначення: визначені організацією додаткові критерії відбору персоналу*].

Рекомендації з реалізації: До інформації, яка потребує додаткових заходів захисту, належить критична інформація, персональні дані та таємна інформація. Критерії забезпечення безпеки персоналу включають перевірку відповідності кваліфікаційних вимог персоналу до рівня чутливості посади

Пов’язані заходи: Немає.

(4) ПЕРЕВІРКА ПЕРСОНАЛУ - ВИМОГИ ДО ГРОМАДЯНСТВА

Переконатися, що особи, які звертаються до системи обробки, зберігання або передачі [*Призначення: визначених організацією типів інформації*], задовольняють [*Призначення: визначені організацією вимоги до громадянства*].

Рекомендації з реалізації: Немає.

Пов’язані заходи: Немає.

Посилання: FIPS Publications 199, 201, [EO 13526], [EO 13587], [SP 800-60-1], [SP 800-60-2], [SP 800-73-4], [SP 800-76-2], [SP 800-78-4].

## PS-4 ЗВІЛЬНЕННЯ ПЕРСОНАЛУ

Заходи захисту:

При припиненні особою індивідуального трудового договору в організації необхідно:

a. відключити доступ до системи протягом [*Призначення: визначеного організацією періоду часу*];

b. завершити або скасувати всі засоби автентифікації та облікові дані, пов’язані з цією особою;

c. провести співбесіди при звільненні, які містять обговорення [*Призначення: визначених організацією тем інформаційної безпеки*];

d. отримати все майно, пов’язане із заходами безпеки під час користування системою організації;

e. зберігати доступ до інформації та систем організації, які раніше контролювала звільнена особа.

Рекомендації з реалізації: До властивості системи належать: токени автентифікації, технічні посібники адміністрації системи, ключі, ідентифікаційні картки та інші дані. Вихідні співбесіди можуть гарантувати, що особи, які завершують трудову діяльність, розуміють обмеження безпеки, які накладені на колишніх працівників. Під час вихідних бесід можуть порушуватися такі теми: нагадування про угоди щодо нерозголошення; можливі обмеження щодо майбутньої роботи та інші. У певних ситуаціях має бути проведена деактивація облікових записів системи.

Пов’язані заходи: AC-2, IA-4, PE-2, PM-12, PS-6, PS-7.

Посилення заходів:

(1) ЗВІЛЬНЕННЯ ПЕРСОНАЛУ - ВИМОГИ ПІСЛЯ ЗАКІНЧЕННЯ ТРУДОВОЇ ДІЯЛЬНОСТІ

(a) Повідомити звільненх особ про чинні, юридично обов’язкові вимоги, що діють після закінчення трудової діяльності й що стосуються захисту інформації, яка стала їм відома під час виконання службових обов’язків.

(b) Вимагати від звільнених осіб підписати підтвердження вимог після закінчення трудової діяльності в рамках процесу звільнення.

Рекомендації з реалізації: Організації можуть консультуватися з юридичними відділами щодо вимог після закінчення трудової діяльності.

Пов'язані заходи: Немає.

(2) ЗВІЛЬНЕННЯ ПЕРСОНАЛУ - АВТОМАТИЗОВАНЕ СПОВІЩЕННЯ

Впровадити автоматизовані механізми для повідомлення [*Призначення: визначеного організацією персоналу або ролей*] після звільнення особи.

Рекомендації з реалізації: В організаціях з великою кількістю співробітників не весь персонал, який повинен знати про дії звільнення, отримує відповідні сповіщення або отримує їх невчасно. Автоматизовані механізми можуть використовуватися для надсилання автоматичних сповіщень персоналу організації або конкретній ролі після припинення трудової діяльності. Такі автоматизовані сповіщення можуть передаватися різними способами, включно з, наприклад, телефоном, електронною поштою, текстовим повідомленням. Автоматизовані механізми також можна використовувати для швидкого й повного блокування доступу до ресурсів системи після звільнення працівника.

Пов'язані заходи: Немає.

Посилання: Немає.

## PS-5 ПЕРЕВЕДЕННЯ ПЕРСОНАЛУ

Заходи захисту:

a. Переглядати та підтверджувати поточну оперативну потребу в поточних дозволах логічного та фізичного доступу до систем і об'єктів, коли особи перепризначаються або переводяться на інші посади в організації.

b. Ініціювати [*Призначення: визначені організацією дії щодо переведення або перепризначення*] в межах [*Призначення: визначеного організацією часового періоду після формальної дії переказу*].

c. Змінювати повноваження доступу, якщо це необхідно, щоб відповідати будь-яким змінам операційної потреби через перепризначення або переведення.

d. Повідомляти про переведення персоналу [*Призначення: визначений організацією персонал або посадові особи*] в рамках [*Призначення: визначений організацією період часу*].

Рекомендації з реалізації: Цей захід захисту застосовується у випадках, коли в організації перепризначення чи передача повноважень відбувається постійно. Дії, які можуть знадобитися для переведення персоналу в межах організації, охоплюють, наприклад, повернення старих та видачу нових ключів, ідентифікаційних карток і пропусків, закриття старих облікових записів системи та створення нових , зміну авторизацій доступу до системи (тобто привілеїв).

Пов'язані заходи: AC-2, IA-4, PE-2, PM-12, PS-4, PS-7.

Посилення заходів: Немає.

Посилання: Немає.

## PS-6 УГОДИ ПРО ДОСТУП

Заходи захисту:

a. Розробити та оформити угоди про доступ до інформаційних систем організації.

b. Переглядати та оновлювати угоди про доступ [*Призначення: з визначеною організацією частотою*].

c. Переконатися, що особи, які потребують доступу до організаційної інформації та систем:

   1. підписали відповідні угоди про доступ перед тим, як отримати доступ;

   2. повторно підписали угоди про доступ для підтримки доступу до інформаційних систем організації, коли угоди про доступ були оновлені або [*Призначення: з визначеною організацією частотою*].

Рекомендації з реалізації: До угод про доступ належать угоди про нерозголошення, правила поведінки та угоди про конфлікт інтересів. Підписані угоди про доступ містять підтвердження того, що люди прочитали, зрозуміли та погоджуються дотримуватися обмежень, пов'язаних з організаційними системами, до яких їм дозволений доступ. Організації можуть використовувати електронні підписи для підтвердження угод про доступ, якщо це не заборонено організаційною політикою.

Пов'язані заходи: AC-17, PE-2, PL-4, PS-2, PS-3, PS-6, PS-7, PS-8, SA-21, SI-12.

Посилення заходів:

(1) УГОДИ ПРО ДОСТУП - ІНФОРМАЦІЯ, ЩО ВИМАГАЄ СПЕЦІАЛЬНОГО ЗАХИСТУ

[Виключено: включено до PS-3].

(2) УГОДИ ПРО ДОСТУП - ІНФОРМАЦІЯ З ОБМЕЖЕНИМ ДОСТУПОМ, ЩО ВИМАГАЄ СПЕЦІАЛЬНОГО ЗАХИСТУ

Переконатися, що доступ до інформації з обмеженим доступом, який вимагає спеціального захисту, надається лише особам, які:

(a) мають чинний дозвіл на доступ, що відповідає вимогам чинного законодавства;

(b) задовільняють відповідним критеріям безпеки щодо персоналу;

(c) прочитали, зрозуміли й підписали угоду про нерозголошення.

Рекомендації з реалізації: Секретна інформація, яка потребує особливого захисту, включає додаткову інформацію, інформацію Програми спеціального доступу (SAP) і конфіденційну інформацію з розділами (SCI). До інформації з обмеженим доступом, яка потребує спеціального захисту, належать персональні дані, критична інформація, таємна інформація. Критерії безпеки персоналу відображають чинні закони, накази, директиви, положення, політику, стандарти та настанови.

Пов’язані заходи: Немає.

(3) УГОДИ ПРО ДОСТУП - ВИМОГИ ПІСЛЯ ЗАКІНЧЕННЯ ТРУДОВОЇ ДІЯЛЬНОСТІ

(a) Повідомити особам про чинні, юридично обов’язкові вимоги після закінчення трудової діяльності щодо захисту організаційної інформації.

(b) Вимагати від осіб підписання підтвердження вимог, якщо це необхідно, як частину надання першого доступу до інформації.

Рекомендації з реалізації: Організації можуть консультуватися з юридичним відділом щодо питань, пов’язаних з вимогами після закінчення трудових відносин.

Пов’язані заходи: PS-4.

Посилання: Немає.

## PS-7 БЕЗПЕКА ЗОВНІШНЬОГО ПЕРСОНАЛУ

Заходи захисту:

a. Встановити вимоги щодо безпеки персоналу, включно з ролями й обов’язками щодо безпеки для зовнішніх постачальників послуг.

b. Вимагати від зовнішніх постачальників дотримання правил і процедур кадрової безпеки, встановлених організацією.

c. Вимагати безпечного ставлення персоналу до документів.

d. Вимагати від зовнішніх постачальників повідомляти [*Призначення: визначені організацією персонал або ролі*] щодо будь-яких переведень або звільнення зовнішнього персоналу, який володіє організаційними повноваженнями або має системні привілеї в межах [*Призначення: визначеного організацією строку*].

e. Контролювати відповідності постачальника визначеним вимогам щодо безпеки інформації.

Рекомендації з реалізації: До зовнішніх постачальників належать: провайдери послуг; підрядники й інші організації, що надають послуги з розробки системи, послуги з впровадження інформаційних технологій; аутсорсингові послуги; послуги тестування/оцінювання та управління мережею і безпекою. Організації прямо вносять вимоги безпеки персоналу в документи, що пов’язані з придбанням. Зовнішні провайдери можуть мати персонал, який працює в установах організації з обліковими даними або системними привілеями, наданими організаціями. Повідомлення про зміни зовнішнього персоналу мають забезпечувати належне припинення привілеїв та повноважень. Організації визначають передачу та припинення привілеїв, про які можна звітувати, за характеристиками, пов’язаними з безпекою, які включають функції, ролі та характер облікових даних або привілеїв, пов’язаних з особами, яким їх було передано або припинено.

Пов’язані заходи: AT-2, AT-3, MA-5, PE-3, PS-2, PS-3, PS-4, PS-5, PS-6, SA-5, SA-9, SA-21.

Посилення заходів: Немає.

Посилання: [SP 800-35], [SP 800-63-3].

## PS-8 КАДРОВІ САНКЦІЇ

Заходи захисту:

a. Використовувати формальний процес санкцій для осіб, які не дотримуються встановлених правил і процедур інформаційної безпеки.

b. Повідомляти [*Призначення: визначений організацією персонал або ролі*] в межах [*Призначення: визначеного організацією періоду часу*], коли починається офіційний процес накладання санкцій працівникам, визначаючи особу та причину санкції.

Рекомендації з реалізації: Кадрові санкції мають відповідати чинному законодавству, наказам, директивам, положенням, політикам, стандартам і рекомендаціям. Кадрові санкції мають бути описані в угодах про доступ і можуть бути внесені як частина загальної кадрової політики та процедур організацій. Організації можуть консультуватися з юридичним відділом щодо питань кадрових санкцій.

Пов'язані заходи: All XX-1 Controls, PL-4, PM-12, PS-6, PT-1.

Посилення заходів: Немає.

Посилання: Немає.

## PS-9 ОПИС ПОЗИЦІЙ

Заходи захисту: Включіть ролі й обов'язки з безпеки та приватності в опис посади в організації.

Рекомендації з реалізації: Специфікація ролей у сфері безпеки та приватності в описі посад окремих організацій сприяє ясності розуміння таких обов'язків, а також вимог щодо рольової підготовки з безпеки та приватності.

Посилення заходів: Немає.

Посилання: [SP 800-181].

## 10.15 Клас заходів захисту PT — ПОВНОВАЖЕННЯ НА ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ

### PT-1 ПОЛІТИКА ТА ПРОЦЕДУРИ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

Заходи захисту:

a. Розробіть, задокументуйте та поширте [*Призначення: персонал або ролі, визначені організацією*]:

1. [*Вибір (один або декілька): Рівень організації; Рівень місії/бізнес-процесу; рівень системи*], обробки персональних даних та політики прозорості, який:

a) розглядає мету, сферу діяльності, ролі, відповідальність, зобов'язання керівництва, координацію між організаційними підрозділами та відповідність;

b) відповідає чинним законам, розпорядженням, директивам, положенням, політикам, стандартам і рекомендаціям.

2. Процедури для реалізації політики обробки та прозорості персональних даних, а також пов'язані засоби контролю;

b. Призначте [*Призначення: посадову особу, визначену організацією*] для керування розробкою, документуванням і розповсюдженням політики й процедур щодо обробки персональних даних та прозорості;

c. Перегляньте та оновіть поточні процедури обробки та прозорість персональних даних:

1. Політика [*Призначення: частота, визначена організацією*] і наступні [*Призначення: події, визначені організацією*];

2. Процедури [*Призначення: частота, визначена організацією*] та наступні [*Призначення: подія, визначена організацією*].

Рекомендації з реалізації: Політика й процедури щодо обробки персональних даних та прозорості стосуються елементів керування класу заходів захисту PT, які реалізують в системах і організаціях. Стратегія управління ризиками є важливим фактором у встановленні такої політики та процедур. Політики та процедури сприяють забезпеченню безпеки та конфіденційності. Тому важливо, щоб програми, які забезпечують безпеку та конфіденційність взаємодіяли при розробці політики й процедур щодо обробки персональних даних та прозорості. Програмні політики, процедури безпеки та конфіденційності на рівні організації є кращим рішенням, яке може усунути потребу в політиках і процедурах, що стосуються місії чи окремої системи. Політика може бути включена як частина загальної політики безпеки та конфіденційності або представлена декількома політиками, які відображають складний характер організацій. За потреби можна встановити процедури для програм безпеки та конфіденційності, для місії чи бізнес-процесів, а також для окремих систем. Процедури описують, як реалізуються політики або засоби контролю, і можуть бути спрямовані на особу або роль, які є об'єктом процедури. Процедури можуть бути задокументовані в системі безпеки та плані конфіденційності або в одному чи кількох окремих документах. Події, які можуть спричинити оновлення політики й процедур прозорості

обробки персональних даних, включають висновки оцінки або аудиту, злами систем або зміни в чинних законах, виконавчих наказах, директивах, положеннях, політиках, стандартах і вказівках. Просте повторне встановлення засобів контролю не є організаційною політикою чи процедурою.

Пов'язані заходи: Немає.

Посилення заходів: Немає.

Посилання: [OMB A-130].

## PT-2 ПОВНОВАЖЕННЯ НА ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ

Заходи захисту:

a. визначити та задокументувати [*Призначення: повноваження, визначені організацією]*, які дозволяють [*Призначення: обробку, визначену організацією*] персональної інформації;

b. обмежити [*Призначення: обробку, визначену організацією*] персональної інформації лише таким чином, яким дозволено (тільки до того, що дозволено)

Рекомендації з реалізації: Обробка персональних даних — це операція або набір операцій, які інформаційна система чи організація виконує щодо персональних даних протягом життєвого циклу інформації. Обробка включає, але не обмежується створенням, збором, використанням, обробкою, зберіганням, підтримкою, розповсюдженням, розкриттям та видаленням інформації. Операції обробки також включають журналювання, генерацію та перетворення, а також методи аналізу даних.

На організації можуть поширюватися закони, виконавчі накази, директиви, нормативні акти чи політики, які встановлюють повноваження організації та, таким чином, обмежують певні типи обробки персональних даних або встановлюють інші вимоги, пов'язані з їх обробкою. Персонал організації консультується з консультантом з конфіденційності та юрисконсультантом щодо таких повноважень, особливо якщо організація підпадає під кілька юрисдикцій або джерел повноважень. Для організацій, обробка яких не визначена юридичними повноваженнями, політика організації та визначення, як вони обробляють персональні дані. Хоча обробка персональних даних може бути дозволена законом, ризики конфіденційності все одно можуть виникнути. Оцінка ризиків конфіденційності може виявити ризики, пов'язані з авторизованою обробкою персональних даних і підтримати рішення для управління такими ризиками.

Організації враховують відповідні вимоги та організаційну політику, щоб визначити, як документувати ці повноваження. Для органів державної влади повноваження на обробку персональних даних задокументовано в політиках конфіденційності та повідомленнях, повідомленнях про систему записів, оцінці впливу на конфіденційність, заявах], угодах і повідомленнях про комп'ютерні угоди, контрактах, угодах про обмін інформацією, меморандумах про взаєморозуміння та іншій документації.

Організації вживають заходів для забезпечення того, щоб персональні дані оброблялися лише для авторизованих цілей, включаючи навчання організаційного персоналу авторизованій обробці персональних даних, її моніторинг та аудит використання в організації.

Пов'язані заходи: AC-2, AC-3, CM-13, IR-9, PM-9, PM-24, PT-1, PT-3, PT-5, PT-6, RA-3, RA-8, SI-12, SI-18.

Посилення заходів:

(1) ПОВНОВАЖЕННЯ НА ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ - ТЕГУВАННЯ ДАНИХ

Додавання тегів даних, що містять [*Призначення: авторизована обробка, визначена організацією*], до [*Призначення: визначені організацією елементи персональних даних*].

Рекомендації з реалізації: Теги даних підтримують відстеження та примусове виконання авторизованої обробки, передаючи типи авторизованої обробки разом із відповідними елементами персональних даних в усій системі. Теги даних також можуть підтримувати використання автоматизованих інструментів.

(2) ПОВНОВАЖЕННЯ НА ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ - АВТОМАТИЗАЦІЯ

Керування примусовою обробкою персональних даних за допомогою [*Призначення: автоматизовані механізми, визначені організацією*].

Рекомендації з реалізації: Автоматизовані механізми доповнюють перевірку того, що відбувається лише авторизована обробка інформації.

Пов'язані заходи: CA-6, CM-12, PM-5, PM-22, PT-4, SC-16, SC-43, SI-10, SI-15, SI-19.

Посилання: [PRIVACT], [OMB A-130], [IR 8112].

## PT-3 ЦІЛІ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

Заходи захисту:

a. визначити та задокументувати [*Призначення: цілі, визначені організацією*] для обробки персональних даних;

b. описати мету (цілі) у публічних повідомленнях про конфіденційність і політиках організації;

c. обмежити [*Призначення: обробку, визначену організацією*] персональних даних лише тією, яка сумісна з визначеною ціллю(ями);

d. відстежувати зміни в обробці персональних даних та впроваджувати [*Завдання: визначені організацією механізми*], щоб гарантувати, що будь-які зміни вносяться відповідно до [*Завдання: визначені організацією вимоги*].

Рекомендації з реалізації: Визначення та документування мети обробки дає організаціям основу для розуміння того, для чого бробляються персональні дані Термін «процес» включає кожен етап життєвого циклу інформації як створення, збір, використання, обробку, зберігання, обслуговування, розповсюдження, розкриття та видалення. Визначення та документування мети обробки є необхідною умовою для того, щоб власники та оператори системи та особи, чия інформація обробляється системою, могли зрозуміти, як саме ця інформація буде оброблятися. Це дає змогу людям приймати обґрунтовані рішення щодо їх взаємодії з інформаційними системами та організаціями та керувати своїми інтересами конфіденційності. Після визначення конкретної мети обробки ця мета описується в повідомленнях про конфіденційність,

політиках організації та будь-якій пов'язаній документації щодо відповідності конфіденційності, включаючи оцінки впливу на конфіденційність, повідомлення про систему записів, заяви [PRIVACT], повідомлення про комп'ютерні угоди та інші відповідні Повідомлення Федерального реєстру.

Організації вживають заходів для забезпечення того, щоб персональні дані оброблялися лише для визначених цілей, включаючи навчання персоналу організації, моніторинг та аудит обробки персональних даних в організації.

Організації відстежують зміни в обробці персональних даних. Персонал організації консультується зі старшим представником агентства з питань конфіденційності та юрисконсультантом, щоб переконатися, що будь-які нові цілі, які виникають у результаті змін в обробці, сумісні з метою, для якої було зібрано дані, або, якщо нова мета несумісна, запровадити механізми відповідно із визначеними вимогами, щоб дозволити нову обробку, якщо це необхідно. Механізми можуть включати отримання згоди від окремих осіб, перегляд політики конфіденційності або інші заходи для управління ризиками конфіденційності, які виникають через зміни в цілях обробки персональних даних.

Пов'язані заходи: AC-2, AC-3, AT-3, CM-13, IR-9, PM-9, PM-25, PT-2, PT-5, PT-6, PT-7, RA-8, SC-43, SI-12, SI-18.

Посилення заходів:

(1) ЦІЛІ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ - ТЕГУВАННЯ ДАНИХ

Додайте теги даних із такими цілями до [*Призначення: визначені організацією елементи персональної інформації*]: [*Призначення: визначені організацією цілі обробки*].

Рекомендації з реалізації: Теги даних підтримують відстеження цілей обробки, передаючи цілі разом із відповідними елементами персональних даних по всій системі. Передаючи цілі обробки в тег даних разом із персональними даними під час проходження інформації через систему, власник або оператор системи може визначити, чи буде зміна в обробці сумісна з ідентифікованою та документально підтверджені цілі. Теги даних також можуть підтримувати використання автоматизованих інструментів.

Пов'язані заходи: CA-6, CM-12, PM-5, PM-22, SC-16, SC-43, SI-10, SI-15, SI-19.

(2) ЦІЛІ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ - АВТОМАТИЗАЦІЯ

Відстежуйте цілі обробки персональних даних за допомогою [*Призначення: автоматизовані механізми, визначені організацією*].

Рекомендації з реалізації: Автоматизовані механізми доповнюють відстеження цілей обробки.

Пов'язані заходи: CA-6, CM-12, PM-5, PM-22, SC-16, SC-43, SI-10, SI-15, SI-19.

Посилання: [PRIVACT], [OMB A-130], [IR 8112].

## PT-4 ЗГОДА НА ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ

Заходи захисту: Впроваджувати [*Призначення: інструменти або механізми, визначені організацією*], щоб окремі особи давали згоду на обробку їх персональних даних до її

збору, що полегшить прийняття обґрунтованих рішень особами.

Рекомендації з реалізації: Згода дозволяє особам брати участь у прийнятті рішень щодо обробки їх персональних даних та передає частину ризику, який виникає внаслідок обробки персональних даних, від організації до окремої особи. Згода може вимагатися згідно з чинними законами, розпорядженнями, директивами, правилами, політиками, стандартами чи рекомендаціями. В іншому випадку, обираючи згоду як засіб контролю, організації розглядають, чи можна обґрунтовано очікувати, що особи розумітимуть і приймуть ризики конфіденційності, які виникають через їх авторизацію. Організації розглядають, які засоби контролю можуть ефективніше зменшити ризик конфіденційності окремо чи за згодою. Організації також враховують будь-які демографічні чи контекстуальні фактори, які можуть вплинути на розуміння або поведінку осіб щодо обробки їх даних, що виконується системою чи організацією. Запитуючи згоду від окремих осіб, організації розглядають відповідний механізм для отримання згоди, включаючи тип згоди (наприклад, згода, відмова), як правильно автентифікувати та підтвердити особу і як отримати згоду за допомогою електронних засобів. Крім того, організації розглядають можливість надання особам механізму відкликання згоди після її надання. Нарешті, організації враховують фактори зручності використання, щоб допомогти особам зрозуміти ризики, прийняті під час надання згоди, включаючи використання простої мови.

Пов'язані заходи: AC-16, PT-2, PT-5.

Посилення заходів:

(1) ЗГОДА НА ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ - ІНДИВІДУАЛЬНА ЗГОДА НА ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ

Надайте [*Призначення: механізми, визначені організацією*], щоб дозволити особам пристосовувати дозволи на обробку до вибраних елементів персональних даних.

Рекомендації з реалізації: Хоча певна обробка може бути необхідною для базової функціональності продукту чи послуги, інша обробка може бути необхідна. За таких обставин організації дозволяють окремим особам вибирати, як обробляти конкретні ідентифікаційні елементи інформації. Індивідуальна згода може допомогти зменшити ризик конфіденційності, підвищити задоволеність послугою та уникнути відмови від продукту чи послуги.

Пов'язані заходи: PT-2.

(2) ЗГОДА НА ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ - СВОЄЧАСНА ЗГОДА НА ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ

Представляти [*Завдання: визначені організацією механізми отримання згоди*] особам із [*Завдання: визначена організацією частота*] та в поєднанні з [*Завдання: визначена організацією обробка персональної інформації*].

Рекомендації з реалізації: Своєчасна згода дозволяє особам брати участь у тому, як обробляються їх персональні дані в той час або в поєднанні з певними типами обробки даних, коли така участь може бути найбільш корисною для особи. Індивідуальні припущення щодо того, як обробляється персональні дані, можуть бути неточними чи ненадійними, якщо минув час з моменту останньої згоди особи або тип обробки створює значний ризик конфіденційності. Організації на

власний розсуд визначають, коли використовувати своєчасну згоду, і можуть використовувати допоміжну інформацію про демографічні показники, фокус-групи чи опитування, щоб дізнатися більше про інтереси та проблеми конфіденційності окремих осіб.

Пов'язані заходи: PT-2.

(3) ЗГОДА НА ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ - ВІДКЛИКАННЯ

Впровадити [*Призначення: інструменти або механізми, визначені організацією*] для відкликання згоди осіб на обробку їх персональних даних.

Рекомендації з реалізації: Відкликання згоди дозволяє особам контролювати своє початкове рішення щодо згоди, коли обставини змінюються. Організації враховують фактори зручності використання та забезпечують просту у використанні можливість відкликання.

Пов'язані заходи: PT-2.

Посилання: [PRIVACT], [OMB A-130], [SP 800-63-3].

## PT-5 ПОВІДОМЛЕННЯ ПРО КОНФІДЕНЦІЙНІСТЬ

Заходи захисту: Впровадити повідомлення про конфіденційність особам, чиї персональні дані обробляються в системі, які:

a. доступні окремим особам під час першої взаємодії з організацією, та згодом [*Призначення: частота, визначена організацією*];

b. виражені простою мовою;

c. визначають орган, який надає дозвіл на обробку персональних даних;

d. визначають цілі, для яких мають оброблятися персональні дані;

e. включають [*Призначення: інформація, визначена організацією*].

Рекомендації з реалізації: Повідомлення про конфіденційність допомагають інформувати людей про те, як система чи організація обробляє їх персональні дані. Організації використовують повідомлення про конфіденційність, щоб інформувати осіб про те, як та з якими повноваженнями і метою обробляються їх персональні дані, а також інша інформація, щодо вибору такої обробки та інших сторін, яким інформація надається. Закони, розпорядження, директиви, нормативні акти чи політики можуть вимагати, щоб повідомлення про конфіденційність включали певні елементи або надавалися в певних форматах. Персонал органу держаної влади консультується зі старшим представником агентства з конфіденційності та юрисконсультантом стосовно того, коли та як надавати такі повідомлення, а також щодо елементів, які слід включати в повідомлення про конфіденційність, і необхідних форматів таких повідомлень. За обставин, коли закони чи загальнодержавні політики не вимагають повідомлень про конфіденційність, організаційні політики та визначення можуть вимагати повідомлень про конфіденційність і можуть служити джерелом елементів для включення до повідомлень про конфіденційність.

Оцінка ризиків конфіденційності визначає ризики конфіденційності, пов'язані з обробкою персональних даних, і може допомогти організаціям визначити відповідні елементи для включення в повідомлення про конфіденційність для управління такими

ризиками. Щоб допомогти людям зрозуміти, як обробляється їх персональні дані, організації пишуть матеріали простою мовою та уникають технічного жаргону.

Пов'язані заходи: PM-20, PM-22, PT-2, PT-3, PT-4, PT-7, RA-3, SC-42, SI-18.

Посилення заходів:

(1) ПОВІДОМЛЕННЯ ПРО КОНФІДЕНЦІЙНІСТЬ - СВОЄЧАСНЕ ПОВІДОМЛЕННЯ ПРО КОНФІДЕНЦІЙНІСТЬ

Повідомляти особам про обробку персональних даних в той час і в місці, де особа її надає, або під час дій з даними, або [*Призначення: частота, визначена організацією*].

Рекомендації з реалізації: Своєчасні повідомлення інформують людей про те, як організації обробляють їх персональні дані в час, коли такі повідомлення можуть бути найбільш корисними для людей. Індивідуальні припущення щодо того, як будуть оброблятися персональні дані, можуть бути неточними або ненадійними, якщо минув час з моменту останнього наданого повідомлення або змінилися обставини, за яких особі було надано останнє повідомлення. Своєчасне повідомлення може прояснити дії з даними, які організації визначили як такі, що потенційно можуть створити більший ризик для конфіденційності окремих осіб. Організації можуть використовувати своєчасне повідомлення, щоб оновлювати або нагадувати особам про певні дії з даними, коли вони відбуваються, або висвітлювати конкретні зміни, які відбулися з часу останнього повідомлення. Своєчасне повідомлення можна використовувати разом із своєчасною згодою, щоб пояснити, що станеться, якщо згоду буде відхилено. Організації на власний розсуд визначають, коли використовувати своєчасні повідомлення, і можуть використовувати допоміжну інформацію про демографічні показники користувачів, фокус-групи чи опитування, щоб дізнатися про інтереси та проблеми щодо конфіденційності користувачів.

Пов'язані заходи: PM-21.

(2) ПОВІДОМЛЕННЯ ПРО КОНФІДЕНЦІЙНІСТЬ - ЗАЯВИ ПРО КОНФІДЕНЦІЙНІСТЬ

Включіть заяви про конфіденційність у форми, які збирають інформацію, що зберігатиметься в системі записів Закону про конфіденційність, або надайте заяви про конфіденційність у формах, які можуть зберігатися особами.

Рекомендації з реалізації: Якщо орган державної влади просить окремих осіб надати персональні дані, які стануть частиною системи записів, він має надати заяву [PRIVACT] у формі, яка використовується для збору таких даних, або в окремій формі, яку особа може зберігати для себе. За таких обставин орган державної влади надає заяву [PRIVAC] незалежно від того, чи збиратимуться дані в паперовій чи електронній формі, на вебсайті, у мобільному додатку, по телефону чи іншим способом. Ця вимога гарантує, що особі надається достатньо інформації про запит на персональні дані, щоб прийняти обґрунтоване рішення щодо відповіді.
[PRIVACT] заяви надають офіційне повідомлення особам про орган, який уповноважує вимагати персональні дані; про обов'язковість чи добровільність надання таких даних; основну мету (цілі), для якої дані будуть використовуватися; способи використання та публікації, яким підлягають дані;

вплив на особу, якщо такий є, ненадання всієї або будь-якої частини запитувани інформації; відповідне посилання та посилання на відповідну систему записів. Співробітники органу державної влади консультуються зі старшим представником агентства з питань конфіденційності та юрисконсультантом щодо положень про повідомлення [PRIVACT].

Пов'язані заходи: PT-6.

Посилення заходів: Немає.

Посилання: [PRIVACT], [OMB A-130], [OMB A-108].

## PT-6 СИСТЕМА ЗАПИСІВ ПОВІДОМЛЕНЬ ПРО КОНФІДЕНЦІЙНІСТЬ

Заходи захисту: для систем, які обробляють інформацію, яка зберігатиметься в системі записів Закону про конфіденційність:

a. розробити проект системи повідомлень про записи відповідно до вказівок OMB і подати нову та суттєво змінену систему повідомлень про записи до OMB та відповідних комітетів Конгресу для попереднього розгляду;

b. опублікувати систему записів повідомлень у Державному реєстрі;

c. зберігайте повідомлення системи записів точними, оновленими та в обсязі відповідно до впровадженої політики.

Рекомендації з реалізації: [PRIVACT] вимагає, щоб органи державної влади публікували повідомлення про систему записів у Державному реєстрі після створення та/або зміни системи [PRIVACT] записів. Як правило, система повідомлень про записи потрібна, коли орган державної влади зберігає групу будь-яких записів під своїм контролем, з яких інформація витягується за іменем особи або певним ідентифікаційним номером, символом чи іншим ідентифікатором. Повідомлення описує існування та характер системи та ідентифікує систему записів, мету системи, повноваження для ведення записів, категорії записів, які зберігаються в системі, категорії осіб, щодо яких ведуться записи, використання записів, і додаткові відомості про систему, як описано в [OMB A-108].

Пов'язані заходи: AC-3, PM-20, PT-2, PT-3, PT-5.

Посилення заходів:

(1) СИСТЕМА ЗАПИСІВ ПОВІДОМЛЕНЬ ПРО КОНФІДЕНЦІЙНІСТЬ - ЗВИЧАЙНЕ ВИКОРИСТАННЯ

Перегляньте всі звичайні випадки використання, опубліковані в повідомленні системи записів [*Призначення: частота, визначена організацією*], щоб забезпечити постійну точність і сумісність звичайних видів використання з метою, для якої була зібрана інформація.

Рекомендації з реалізації: Звичайне використання [PRIVACT] — це особливий вид розкриття запису за межами органу державної влади, який підтримує систему записів. Звичайне використання є винятком із заборони [PRIVACT] на розкриття запису в системі записів без попередньої письмової згоди особи, до якої відноситься запис. Щоб кваліфікувати використання як звичайне, розголошення має бути сумісне з метою, для якої дані були зібрані спочатку. [PRIVAC] вимагає

від установ описувати кожне звичайне використання записів, які зберігаються в системі записів, включаючи категорії користувачів записів і мету використання. Органи державної влади можуть встановлювати звичайне використання лише шляхом явної публікації у відповідній системі записів.

Пов'язані заходи: Немає.

(2) СИСТЕМА ЗАПИСІВ ПОВІДОМЛЕНЬ ПРО КОНФІДЕНЦІЙНІСТЬ - ПРАВИЛА ЗВІЛЬНЕННЯ

Переглядайте всі винятки із Закону про конфіденційність, заявлені для системи записів [*Призначення: частота, визначена організацією*], щоб переконатися, що вони залишаються доцільними та необхідними відповідно до закону, що вони були оприлюднені відповідно до законодавства та що вони точно описані в системі повідомлення про записи.

Рекомендації з реалізації: [PRIVAC] містить два набори положень, які дозволяють органам державної влади вимагати звільнення від певних вимог статуту. За певних обставин ці положення дозволяють органам державної влади оприлюднити правила, щоб звільнити систему записів від певних положень [PRIVACT]. Положення про звільнення [PRIVACT] організацій включають конкретні назви будь-яких систем записів, які будуть звільнені, конкретні положення [PRIVACT], для яких система(и) записів буде звільнена, причини звільнення та пояснення того, чому звільнення є необхідним і доречним.

Пов'язані заходи: Немає.

Посилання: [PRIVACT], [OMB A-108].

## PT-7 СПЕЦІАЛЬНІ КАТЕГОРІЇ ПЕРСОНАЛЬНИХ ДАНИХ

Заходи захисту: Застосувати [*Призначення: умови обробки, визначені організацією*] для певних категорій персональних даних.

Рекомендації з реалізації: Організації застосовують будь-які умови або засоби захисту, які можуть бути необхідними для певних категорій персональних даних. Ці умови можуть вимагатися законами, виконавчими розпорядженнями, директивами, правилами, політиками, стандартами чи рекомендаціями. Вимоги також можуть випливати з результатів оцінки ризиків конфіденційності, які враховують контекстуальні зміни, що можуть призвести до того, що організація може визначити, що певна категорія персональних даних є особливо чутливою або створює певні ризики конфіденційності. Організації консультуються зі старшим представником агентства з конфіденційності та юрисконсультантом щодо будь-яких заходів захисту, які можуть бути необхідними для таких категорій даних.

Пов'язані заходи: IR-9, PT-2, PT-3, RA-3.

Посилення заходів:

(1) СПЕЦІАЛЬНІ КАТЕГОРІЇ ПЕРСОНАЛЬНИХ ДАНИХ - НОМЕРИ СОЦІАЛЬНОГО СТРАХУВАННЯ

Коли система обробляє номери соціального страхування:

а) усуньте непотрібне збирання, обслуговування та використання номерів

соціального страхування та досліджуйте інші альтернативні персональні ідентифікатори замість них;

b) не відмовляйте жодній особі в будь-яких правах, пільгах чи привілеях, передбачених законом, через відмову такої особи розкрити свій номер соціального страхування;

c) інформуйте будь-яку особу, яку просять розкрити свій номер соціального страхування, чи є це розкриття обов'язковим чи добровільним, який законодавчий чи інший орган вимагає такий номер і як він буде використаний.

Рекомендації з реалізації: Федеральний закон і політика встановлюють особливі вимоги до обробки номерів соціального страхування організаціями. Організації вживають заходів для усунення непотрібного використання номерів соціального страхування та іншої конфіденційної інформації та дотримуються будь-яких особливих вимог, які застосовуються для обробки номерів соціального страхування.

Пов'язані заходи: IA-4.

(2) СПЕЦІАЛЬНІ КАТЕГОРІЇ ПЕРСОНАЛЬНИХ ДАНИХ - ІНФОРМАЦІЯ ПРО ПЕРШУ ПОПРАВКУ

Заборонити обробку інформації, що описує, як будь-яка особа реалізує права, гарантовані Першою поправкою, за винятком випадків, коли це прямо дозволено законом або особою, або якщо вона не стосується та входить до сфери санкціонованої діяльності правоохоронних органів.

Рекомендації з реалізації: [PRIVACT] обмежує можливості організацій обробляти інформацію, яка описує, як особи користуються правами, гарантованими Першою поправкою. Організації консультуються зі консультантом з конфіденційності та юрисконсультантом щодо таких вимог.

Пов'язані заходи: Немає.

Посилання: [PRIVACT], [OMB A-130], [OMB A-108], [NARA CUI].

## PT-8 ВИМОГИ ДО ВІДПОВІДНОСТІ

Заходи захисту: Коли система чи організація обробляє інформацію з метою проведення програми відповідності необхідно:

a. отримати схвалення Ради з цілісності даних для проведення програми відповідності;

b. розробити та укласти договір комп'ютерної відповідності;

c. незалежним чином перевіряти інформацію, надану програмою відповідності, перш ніж вживати негативних заходів проти особи;

d. повідомляти осіб і надати їм можливість оскаржити висновки, перш ніж вживати проти них негативних заходів.

Рекомендації з реалізації: [PRIVACT] встановлює вимоги до державних і недержавних організацій, якщо вони беруть участь у програмі відповідності. Загалом, програма

відповідності — це комп’ютеризоване порівняння записів із двох або більше автоматизованих [PRIVACT] систем записів або автоматизованої системи записів і автоматизованих записів, що ведуться недержавних організацій (або його агентом). Програма відповідності стосується або державних програм пільг, або державних кадрових чи облікових записів про заробітну плату. Порівняння державних пільг проводиться для визначення або перевірки права на отримання виплат за державними програмами пільг або для відшкодування виплат чи прострочених боргів за державними програмами пільг. Програма встановлення відповідності передбачає не лише саму діяльність зі встановлення відповідності, але й подальше розслідування та кінцеві дії, якщо такі є.

Пов’язані заходи: PM-24.

Посилення заходів: Немає.

Посилання: [PRIVACT], [CMPPA], [OMB A-130], [OMB A-108].

## 10.16 Клас заходів захисту RA — ОЦІНЮВАННЯ РИЗИКУ

### RA-1 ПОЛІТИКА ТА ПРОЦЕДУРИ ОЦІНЮВАННЯ РИЗИКУ

Заходи захисту:

a. Розробити, задокументувати та поширити серед [*Призначення: визначеного організацією персоналу або посадових осіб*]:

   1. Політику оцінювання ризику, яка:

      (a) містить мету, сферу застосування, ролі, обов'язки, відповідальність керівництва, координацію між організаційними підрозділами та систему контролю відповідності (complaince);

      (b) відповідає чинному законодавству, виконавчим наказам, директивам, нормам, політикам, стандартам і керівним принципам.

   2. Процедури, що сприяють здійсненню політики оцінювання ризику та пов'язаних з ними заходів оцінювання ризику.

b. Призначити [*Призначення: визначена організацією посадову особу*] для управління політикою та процедурами оцінювання ризику.

c. Переглядати й оновлювати:

   1. Поточну політику оцінювання ризику [*Призначення: з визначеною організацією частотою*].

   2. Поточні процедури оцінювання ризику [*Призначення: з визначеною організацією частотою*].

Рекомендації з реалізації: Цей захід захисту стосується встановлення політики та процедур для ефективного здійснення заходів і їх посилень у класі RA, які впроваджуються в системах та організаціях. Стратегія управління ризиками є важливим фактором у встановленні політики та процедур. Комплексна політика та процедури допомагають забезпечити безпеку та приватність. Тому, важливо доясягти взаємодії роботи програм безпеки та приватності при розробці політик та процедур оцінки ризиків. За наявності політики, а також планів захисту інформації та персональних даних на рівні організації, конкретні системні політики та процедури можуть бути не потрібні. Політика може бути внесена до складу загальної політики безпеки та приватності або може бути представлена кількома політиками (у випадках складної архітектури). Процедури оцінки ризиків можуть бути передбачені для програм забезпечення безпеки та приватності для процесів місії/бізнесу, а також, за потреби, всієї системи. Процедури описують, як має реалізуватися політика чи заходи захисту та як вони можуть бути спрямовані на персонал або роль, яка є об'єктом процедури. Процедури можуть бути задокументовані в планах захисту інформації та персональних даних (як один або декілька документів). Події, які можуть призвести до необхідності оновлення політики та процедур оцінки ризиків, включають результати оцінки та аудиту, випадки порушення безпеки або внесення змін до законів, наказів, директив, положеннях, політиках, стандартах та рекомендаціях.

Пов'язані заходи: PM-9, PS-8, SI-12.

Посилення заходів: Немає.

Посилання: [OMB A-130], [SP 800-12], [SP 800-30], [SP 800-39], [SP 800-100].

## RA-2 КАТЕГОРІЮВАННЯ БЕЗПЕКИ

Заходи захисту:

a. Здійснити категоріювання інформаційної системи й інформації, яку вона обробляє, зберігає та передає.

b. Задокументувати результати категоріювання безпеки, включно з обґрунтуванням, у плані захисту інформаційної системи.

c. Підтвердити, що посадова особа або уповноважений офіційний представник переглядає та затверджує рішення про категоріювання безпеки.

Рекомендації з реалізації: Категорії безпеки описують можливі несприятливі наслідки для операцій організації, активів організації і осіб, якщо інформація та системи будуть скомпрометовані через втрату конфіденційності, цілісності чи доступності. Категоризація безпеки є одним з типів характеризації втрат активів в процесах інженерії систем безпеки, який проводиться на протязі життєвого циклу розробки системи. Організації можуть використовувати процедури оцінки ризиків конфіденційності або оцінки впливу на приватність для кращого розуміння можливих негативних наслідків для фізичних осіб. [CNSSI 1253] надає додаткові рекомендації з категоризації для систем національної безпеки.
Організації проводять процес категоризації безпеки як загальноорганізаційну діяльність із залученням керівників інформаційних служб, старших посадових осіб з інформаційної безпеки відомства, старших посадових осіб відомства з питань конфіденційності, власників систем, місій і підприємств, а також власників або розпорядників інформації. При цьому, враховуються потенційні негативні наслідки для інших організацій, а також, відповідно до указів Президента з питань національної безпеки та [USA PATRIOT], для держави в цілому.
Процеси категоризації безпеки сприяють розробці інвентаризації інформаційних активів і, разом з CM-8, визначення відповідності компонентів системи категоріям безпеки в залежності від того, де обробляється, зберігається або передається інформація. Процес категоризації безпеки переглядається на протязі життєвого циклу розробки системи з метою забезпечення точності та актуальності категорій безпеки.

Пов'язані заходи: CM-8, MP-4, PL-2, PL-10, PL-11, PM-7, RA-3, RA-5, RA-7, RA-8, SC-7, SC-38, SI-12.

Посилення заходів:

(1) КАТЕГОРІЮВАННЯ БЕЗПЕКИ - КАТЕГОРІЮВАННЯ ДРУГОГО РІВНЯ

Провести категоріювання другого рівня для інформаційних систем організації з метою отримання додаткової деталізації рівнів критичності інформаційної системи.

Рекомендації з реалізації: У результаті такої класифікації системи можуть отримати позначки «низький», «середній» або «високий» рівень критичності. Організації, які бажають додаткової деталізації в системах позначень критичності, можуть надалі розподілити системи на підкатегорії. Наприклад,

категоріювання другого рівня в системі з помірним рівнем може створити три нові підкатегорії: низько-середній, помірно-середній і високо-середній. Це вторинне категоріювання та отримані підкатегорії безпеки системи дають організаціям можливість вибрати пріоритет фінансування, пов’язаний з вибором заходів захисту й адаптацією цільових профілів безпеки. Категоріювання другого рівня може також використовуватися для визначення тих систем, які є винятково важливими для завдань і процесів організації.
Оцінка рівня впливу може також використовуватися для визначення тих систем, які можуть бути особливо цікавими або цінними для зловмисників, а також представляти критичну втрату для державної установи, іноді називаються об'єктами критичної важливості. У випадку таких об'єктів критичної важливості організації можуть більше зосередитися на складності, агрегації та обміні інформацією. У разі об'єктів критичної важливості організації зазвичай виявляють більш складну структуру та взаємозв'язок між її складовими. Це може відображатися на архітектурі та топології мережі, що потребує більш ретельного аналізу, планування та керування. Крім того, у таких системах може бути велика кількість даних з різних джерел, що потребує їх агрегації та аналізу для забезпечення цілісної картини безпеки. Інформаційний обмін між різними складовими системи також може створювати додаткові завдання для забезпечення безпеки. Організації можуть використовувати різноманітні техніки та підходи для керування цими вразливостями, такі як збір та обробка даних для розуміння потенційних загроз, розробка політик та процедур для ефективного обміну інформацією та регулярний аудит для забезпечення відповідності заходам безпеки. Системи об’єктів критичної важливості можуть бути відокремлені від інших систем шляхом розділення систем з високим впливом на системи з низько-високим, помірно-високим та надзвичайно-високим рівнями впливу. Організації можуть також використовувати рекомендації, викладені в [CNSSI 1253] для категоризації безпеки.

Пов’язані заходи: Немає.

Посилення заходів: Немає.

Посилання: FIPS Publications 199, 200, [SP 800-30], [SP 800-37], [SP 800-39], [SP 800-60-1], [SP 800- 60-2], [SP 800-160-1], [CNSSI 1253], [NARA CUI].

## RA-3 ОЦІНЮВАННЯ РИЗИКУ

Заходи захисту:

a. Проводити оцінювання ризику, включно з вірогідністю й величиною шкоди від:

   1. несанкціонованого доступу, використання, розголошення, руйнування, модифікації або знищення інформаційної системи, інформації, яку вона обробляє, зберігає та передає; а також будь-якої пов’язаної інформації;

   2. проблем, пов’язаних з приватністю фізичних осіб, що виникають у результаті обробки персональних даних.

b. Інтегрувати результати оцінювання ризику та рішення з управління ризиками на рівні організації та завдань/процесів з оцінюванням ризиків на рівні інформаційної системи.

c. Задокументувати результати оцінювання ризику до [*Вибір: планів безпеки та приватності; звіту про оцінювання ризику;* [*Призначення: визначеного організацією документа*]].

d. Переглядати результати оцінювання ризиків [*Призначення: з визначеною організацією частотою*].

e. Поширити результати оцінювання ризику серед [*Призначення: визначеного організацією персоналу або посадових осіб*].

f. Оновлювати оцінювання ризику [*Призначення: з визначеною організацією частотою*] або коли є суттєві зміни в інформаційній системі, її робочому середовищі чи інших умовах, які можуть вплинути на стан безпеки або приватність інформаційної системи.

Рекомендації з реалізації: Оцінка ризиків враховує загрози, вразливості, ймовірність та вплив на діяльність та активи організації, окремих осіб, інші організації та державу. Оцінювання ризиків має враховувати загрози, вразливості, імовірність і вплив на організаційні операції та активи, осіб, інші організації на основі функціювання та використання систем. Оцінювання ризиків також враховує ризик зовнішніх сторін, включно з: особами, які мають доступ до систем організації; підрядниками, що працюють у системі від імені організації; постачальниками послуг; суб'єктами аутсорсингу. Організації можуть проводити оцінювання ризиків на всіх трьох рівнях ієрархії управління ризиками (тобто рівень організації, рівень процесів, рівень системи) і на будь-якій фазі життєвого циклу розробки системи та на будь-якому етапі життєвого циклу розробки системи. Оцінювання ризиків також може проводитися на різних етапах системи управління ризиками, включаючи підготовку, категоризацію, вибір засобів захисту, впровадження заходів захисту, оцінку заходів захисту, дозвіл на їх застосування та моніторинг. Оцінка ризиків є неперервним процесом, що проводиться на протязі усього життєвого циклу розробки системи.
Оцінки ризиків можуть включати інформацію про систему, включаючи проект системи, призначення використання, результати тестування та артефакти, що пов'язані з ланцюгом постачання. У цьому випадку, артефакти можуть включати документацію, код програмного забезпечення, аудити безпеки та інші матеріали, що можуть служити джерелом інформації для процесу оцінки ризиків. Оцінки ризиків можуть відігравати важливу роль у процесах вибору заходів захисту, зокрема під час застосування рекомендацій щодо налаштування та в ранніх стадіях визначення можливостей.

Пов'язані заходи: CA-3, CP-6, CP-7, CM-4, CM-13, CP-6, IA-8, MA-5, PE-3, PE-8, PE-18, PL-2, PL-10, PL-11, PM-8, PM-9, PM-28, PM-32, PT-2, PT-7, RA-2, RA-5, RA-7, SA-8, SC-38, SI-12.

Посилення заходів:

(1) ОЦІНЮВАННЯ РИЗИКУ - ОЦІНЮВАННЯ РИЗИКУ ЛАНЦЮГА ПОСТАЧАННЯ

(a) Оцінити ризики ланцюга постачання, пов'язані з [*Призначення: визначеними організацією системами, компонентами системи та системними службами*];

(b) Оновлювати оцінювання ризику ланцюга постачання [*Призначення: з визначеною організацією частотою*], коли відбуваються значні зміни у відповідному ланцюгу постачання, або коли зміни в інформаційній системі, робочому середовищі чи інших умовах можуть вимагати змін у ланцюгу постачання.

Рекомендації з реалізації: Події, пов'язані з ланцюгом постачання, охоплюють, наприклад, зриви постачання,крадіжки, використання несправних компонентів, використання підробок, зловмисні розробки, неправильну доставку та введення шкідливого коду. Ці події можуть мати істотний вплив на конфіденційність, цілісність або доступність системи та її інформації, а отже також можуть негативно впливати на організаційні операції (включно з місією, функціями, іміджем чи репутацією), організаційні активи, осіб та інші організації. Події, пов'язані з ланцюгом постачання, можуть бути ненавмисними або зловмисними і можуть виникати в будь-якій точці життєвого циклу системи. Аналіз ризиків ланцюга постачання може допомогти організації визначити системи або компоненти, для яких необхідні додаткові заходи захисту.

Пов'язані заходи: RA-2, RA-9, PM-17, PM-30, SR-2.

(2) ОЦІНЮВАННЯ РИЗИКУ - ВИКОРИСТАННЯ ІНФОРМАЦІЇ З УСІХ ДОСТУПНИХ ДЖЕРЕЛ

Використовуйте інформацію з усіх доступних джерел для аналізу ризиків.

Рекомендації з реалізації: Організації використовують дані з усіх джерел, щоб інформувати про інженерні рішення, рішення щодо придбання та управління ризиками. Розвідка з усіх джерел складається з інформації, отриманої з усіх доступних джерел, включаючи загальнодоступну інформацію або інформацію з відкритих джерел, дані про вимірювання та сигнатури, людський інтелект, дані про сигнали та дані про зображення. Інтелектуальні дані з усіх джерел використовуються для аналізу ризику вразливості (як навмисної, так і ненавмисної) від процесів розробки, виробництва та доставки, людей і середовищ. Аналіз ризиків можна проводити для постачальників на кількох рівнях ланцюга постачання, достатніх для управління ризиками. Організації можуть укладати угоди з іншими організаціями щодо обміну розвідувальною інформацією всіх джерел або прийнятих рішень, якщо це відповідає вимогам. З метою управління ризиками може бути проведений щодо постачальників на декількох рівнях ланцюга постачання. За необхідності, організації можуть укладати договори про обмін інформацією з розвідувальних джерел або про прийняття рішень, що базуються на такій інформації, з іншими організаціями.

Пов'язані заходи: Немає.

(3) ОЦІНЮВАННЯ РИЗИКУ - УСВІДОМЛЕННЯ ДИНАМІЧНИХ ЗАГРОЗ

Визначити поточне середовище кіберзагроз на постійній основі за допомогою [*Призначення: засоби, визначені організацією*].

Рекомендації з реалізації: Зібрана інформація про потенційні загрози передається до відділу інформаційної безпеки з метою адаптації та оновлення процедур до мінливого середовища загроз. Наприклад, при підвищенні рівня загроз організації можуть змінювати порогові значення привілеїв або аутентифікації, необхідні для виконання конкретних операцій.

Пов’язані заходи: AT-2.

(4) ОЦІНЮВАННЯ РИЗИКУ - ПРОГНОСТИЧНА КІБЕРАНАЛІТИКА

Використовуйте наведені нижче розширені можливості автоматизації та аналітики, щоб передбачати та ідентифікувати ризики для [*Призначення: визначені організацією системи або компоненти системи*]: [*Призначення: визначені організацією розширені можливості автоматизації та аналітики*].

Рекомендації з реалізації: Оперативний центр безпеки (ОЦБ) або група реагування на комп’ютерні інциденти (CIRT) з належним ресурсом можуть бути перевантажені обсягом інформації, створеної завдяки поширенню інструментів і пристроїв безпеки, якщо вони не використовують розширену автоматизацію та аналітику для аналізу даних. Розширені можливості автоматизації та аналітики зазвичай підтримуються концепціями штучного інтелекту, включно з машинним навчанням. Прикладами є автоматичне виявлення та реагування на загрози (що включає широке збирання, аналіз на основі контексту та можливості адаптивного реагування), автоматизовані операції робочого процесу та машинні інструменти прийняття рішень. Однак, досвідчені зловмисники можуть отримувати інформацію, пов’язану з аналітичними параметрами, і переналаштовувати машинне навчання, щоб класифікувати зловмисну діяльність як доброякісну. Відповідно, машинне навчання доповнюється моніторингом людини, щоб переконатися, що досвідчені супротивники не зможуть приховати свою діяльність. Це дозволяє звести до мінімуму ймовірність того, що досвідчені зловмисники не зможуть приховувати свої дії.

Пов’язані заходи: Немає.

Посилання: [OMB A-130], [SP 800-30], [SP 800-39], [SP 800-161], [IR 8023], [IR 8062], [IR 8272].

## RA-4 ОНОВЛЕННЯ ОЦІНЮВАННЯ РИЗИКУ

[Вилучено: включено до RA-3].

## RA-5 СКАНУВАННЯ ВРАЗЛИВОСТЕЙ

Заходи захисту:

a. Сканувати на наявність вразливостей в інформаційній системі та інстальованих застосунках [*Призначення: з визначеною організацією частотою та/або випадково відповідно до визначеного організацією процесу*] і коли виявляються нові вразливості, які потенційно впливають на інформаційну систему.

b. Використовувати інструменти та методи сканування вразливості, які полегшують сумісність між інструментами та автоматизують частини процесу управління вразливостями, використовуючи стандарти для:

   1. обліку платформ, недоліків програмного забезпечення та неправильних конфігурацій;

   2. форматування контрольних списків і процедур тестування;

   3. вимірювання впливу вразливості.

c. Аналізувати звіти про сканування вразливості та результати контрольних оцінювань.

d. Виправити наявні вразливості [*Призначення: визначений організацією час відгуку*] відповідно до організаційної оцінки ризику.

e. Ділитися інформацією, отриманою в процесі сканування вразливостей та контрольного оцінювання серед [*Призначення: визначеного організацією персоналу або ролей*], щоб допомогти усунути подібні вразливі місця в інших системах.

f. Використовувати інструменти сканування вразливості, які містять можливість легко оновлювати вразливості, що були просканові.

Рекомендації з реалізації: Категоріювання безпеки інформації та систем проводиться на основі сканування вразливостей. Щоб не пропустити потенційні джерела вразливостей, таких як компоненти інфраструктури (наприклад, комутатори, маршрутизатори, захисники, датчики), мережеві принтери, сканери та копіювальні пристрої, організації визначають необхідний рівень моніторингу вразливостей для компонентів системи. Швидке оновлення засобів моніторингу вразливостей у випадку виявлення та анонсування нових вразливостей, а також при розробці нових методів сканування, допомагає забезпечити ефективне виявлення нових вразливостей, що можуть залишитися непоміченими засобами моніторингу вразливостей, що вже використовуються. Щоб якомога швидше виявляти та усувати потенційні вразливості системи, важливо підтримувати постійний процес оновлення засобів моніторингу вразливостей. Для моніторингу та аналізу вразливостей спеціалізованого програмного забезпечення можуть застосовуватися різні підходи, такі як:

статичний аналіз – передбачає аналіз вихідного коду програми без його запуску. Застосовується для виявлення можливих проблем у програмному коді, таких як помилки в синтаксисі, можливі вразливості безпеки, недостатньо оптимізований код тощо;

динамічний аналіз – передбачає аналіз програми при її виконанні. Застосовується для виявлення потенційних помилок в програмі, таких як вразливості безпеки, падіння програми, невірний вихід програми тощо. Цей метод дозволяє отримати більш точну інформацію про поведінку програми за час її виконання;

бінарний аналіз – метод аналізу файлів, що виконуються. Це дозволяє виявляти потенційні вразливості та помилки в програмах, не маючи доступу до вихідного коду. Такий метод може використовуватися для аналізу програм, які вже розгорнуті в середовищі виробництва або для виявлення вразливостей у сторонньому програмному забезпеченні;

гібридний підхід, який комбінує у собі ці три підходи.

Організації можуть використовувати ці методи аналізу під час огляду вихідного коду та в різних інструментах, включаючи вебпрограми для сканування додатків, статичні засоби аналізу та бінарні аналізатори.

Моніторинг вразливостей включає сканування рівня оновлення заходів безпеки, сканування функцій, портів, протоколів та служб, до яких не повинен мати доступ користувач або пристрій, а також сканування механізмів керування потоками, які неправильно налаштовані або працюють некоректно. Можливість постійного аналізу компонентів (різноманітних програмних модулів, бібліотек, оперативних систем,

мережевих пристроїв, баз даних, сервісів, веб-додатків, аплікацій, протоколів та інших складових системи) за допомогою інструментів постійного моніторингу вразливостей також може бути включена в процес моніторингу вразливостей. Інструментальні засоби можуть покращити точність виявлення вразливостей та застосовуватися в усій організації без необхідності їхнього сканування. Інструменти моніторингу вразливостей, які сприяють інтероперабельності, повинні бути підтверджені протоколом автоматизованого забезпечення безпеки (Security Content Automated Protocol, SCAP). Таким чином, організації розглядають можливість використання інструментів сканування, які вказують на вразливості відповідно до умовних назв вразливостей (Common Vulnerabilities and Exposures (CVE) та використовують мову Open Vulnerability Assessment Language (OVAL) для визначення наявності вразливостей. Для отримання інформації про вразливості використовуються такі джерела, як перелік Common Weakness Enumeration (CWE) та Національна база даних вразливостей (NVD). Оцінки контролю, такі як заходи «червоної команди», надають додаткові джерела потенційних вразливостей, які необхідно сканувати. У цьому контексті "червона команда" - це термін, який використовується для позначення групи людей, які намагаються знайти вразливості в системі або мережі, використовуючи техніки та інструменти, що можуть використовувати зловмисники. Отже, контрольні оцінки, які проводить "червона команда", можуть виявляти потенційні вразливості, які не були виявлені засобами моніторингу вразливостей, і ці вразливості також потрібно сканувати. Організації також розглядають можливість використання інструментів сканування, які вказують на наслідки вразливостей за допомогою системи оцінювання вразливостей (Common Vulnerability Scoring System (CVSS).

Моніторинг вразливості включає канал та процес отримання повідомлень про вразливості безпеки від широкої громадськості. Надання повідомлень про вразливості може бути дуже простим - наприклад, опублікувати адресу електронної пошти або створити веб-форму, яка моніторить та приймає повідомлення. Ці повідомлення можуть стосуватися заявок на добровільне тестування системи на вразливість або про повідомлення про проблеми з безпекою, що були виявлені. Організації зазвичай припускають, що дослідження, спрямовані на пошук вразливостей в їхніх системах, відбуваються з чи без їх згоди. Щоб забезпечити більш високу ймовірність того, що про вразливості буде повідомлено безпосередньо організацію для їх подальшого усунення, організації можуть використовувати публічні канали для сповіщення про такі вразливості.

Організації також можуть використовувати фінансові стимули (також відомі як "винагороди за виправлення помилок"), щоб додатково заохочувати зовнішніх дослідників безпеки повідомляти про виявлені вразливості. Програми винагород за виправлення помилок можуть бути адаптовані під потреби організації. Винагороди можуть надаватися на постійній основі або протягом певного періоду часу і бути запропоновані як широкому загалу, так і підібраним групам осіб. Організації можуть одночасно запускати публічні та приватні програми винагород ("bug bounty") і вибирати певних учасників, яким можуть надавати частковий доступ з високопривілейованих точок, щоб оцінити вразливості з точок зору привілейованого користувача.

Пов’язані заходи: CA-2, CA-7, CA-8, CM-2, CM-4, CM-6, CM-8, RA-2, RA-3, SA-11, SA-12, SA-15, SC-38, SI-2, SI-3, SI-4, SI-7, SR-11.

Посилення заходів:

(1) СКАНУВАННЯ ВРАЗЛИВОСТЕЙ - МОЖЛИВІСТЬ ОНОВЛЕННЯ ІНСТРУМЕНТІВ

[Вилучено: включено до RA-5].

(2) СКАНУВАННЯ ВРАЗЛИВОСТЕЙ - ОНОВЛЕННЯ ЗА ЧАСТОТОЮ, ПЕРЕД НОВИМ СКАНУВАННЯМ АБО ПРИ ІДЕНТИФІКАЦІЇ

Оновлювати перелік вразливостей системи, що були просканові [*Вибір: один або більше*]; [*Призначення: з визначеною організацією частотою*; *перед новим скануванням; коли виявлені та зареєстровані нові вразливості*].

Рекомендації з реалізації: Через складність сучасного програмного забезпечення, систем та інших компонентів, нові вразливості до атак виникають постійно. Тому, важливо включати будь-які нові виявлені вразливості до списку вразливостей для перевірки, щоб організація могла негайно вжити заходів для зниження ризиків, пов'язаних з цими вразливостями.

Пов’язані заходи: SI-5.

(3) СКАНУВАННЯ ВРАЗЛИВОСТЕЙ - ШИРОТА ТА ГЛИБИНА ПОКРИТТЯ

Запровадити процедури сканування вразливостей, які дозволять визначити широту й глибину покриття.

Рекомендації з реалізації: Широту охоплення сканування вразливостей можна виразити у відсотках компонентів в межах системи, за конкретними типами систем, за критичністю систем або за кількістю вразливостей, які необхідно перевірити. Глибина охоплення сканування на вразливість може бути виражена як рівень системи, що підлягає моніторингу організацією (наприклад, компонент, модуль, підсистема, елемент). Організації можуть визначити, наскільки детально потрібно сканувати систему на вразливості, враховуючи власну готовність приймати ризики та інші фактори, які можуть впливати на безпеку їхньої системи. Інструменти сканування та їх конфігурація можуть впливати на рівень деталізації та охоплення. Для досягнення бажаного рівня деталізації та охоплення можуть знадобитись кілька інструментів сканування. [SP 800-53A] надає додаткову інформацію про ширину та глибину охоплення.

Пов’язані заходи: Немає.

(4) СКАНУВАННЯ ВРАЗЛИВОСТЕЙ - ВИЯВНА ІНФОРМАЦІЯ

Визначити непередбачено-виявну інформацію про інформаційну систему та застосувати [*Призначення: визначені організацією коригувальні дії*].

Рекомендації з реалізації: Доступна інформація - це інформація, яку можуть отримати зловмисники, не використовуючи для цього шкідливі методи, такі як спроби несанкціонованого доступу до системи, де зберігається ця інформація. Замість цього вони можуть використовувати інші методи, такі як збір відкритої інформації або високо-розумні пошукові запити. До заходів з протидії можуть входити оповіщення персоналу організації, видалення позначеної інформації, внесення змін до системи, щоб ускладнити доступ зловмисника до позначеної інформації. Це вдосконалення не враховує умисно доступну інформацію, яка може бути включена в можливість встановлення пасток (наприклад, honeypots, honeynets, deception nets), що були розгорнуті організацією.

Пов’язані заходи: AU-13, SC-26.

(5) СКАНУВАННЯ ВРАЗЛИВОСТЕЙ - ПРИВІЛЕЙОВАНИЙ ДОСТУП

Реалізувати авторизацію привілейованого доступу до [*Призначення: визначених організацією компонентів системи*] для [*Призначення: визначеної організацією діяльності з виявлення вразливостей*].

Рекомендації з реалізації: У певних випадках сканування на вразливості може бути більш інтенсивним, або компонент системи, що є об'єктом сканування, може містити інформацію з обмеженим доступом або персональні дані. Надання привілейованого доступу до певних компонентів системи дозволяє проводити більш детальне сканування на вразливості та забезпечує захист конфіденційності такого сканування.

Пов’язані заходи: Немає.

(6) СКАНУВАННЯ ВРАЗЛИВОСТЕЙ - АВТОМАТИЗОВАНИЙ АНАЛІЗ ТЕНДЕНЦІЙ

Впровадити автоматизовані механізми для порівняння результатів сканування вразливостей з часом, щоб визначити тенденції вразливості системи.

Рекомендації з реалізації: Використання автоматизованих механізмів для аналізу кількох сканувань на вразливості з часом може допомогти виявити тенденції у вразливості системи та встановити схеми атак.

Пов’язані заходи: Немає.

(7) СКАНУВАННЯ ВРАЗЛИВОСТЕЙ - АВТОМАТИЗОВАНЕ ВИЯВЛЕННЯ ТА СПОВІЩЕННЯ ПРО НЕАВТОРИЗОВАНІ КОМПОНЕНТИ

[Вилучено: включено до CM-8].

(8) СКАНУВАННЯ ВРАЗЛИВОСТЕЙ - ОГЛЯД ЖУРНАЛІВ АУДИТУ ЗА МИНУЛІ ПЕРІОДИ

Переглядати журнали аудиту за минулі періоди, щоб визначити, чи була вразливість, яка виявлена в [*Призначення: системі, визначеній організацією*], була використана до її виявлення протягом [*Призначення: визначеного організацією періоду часу*].

Рекомендації з реалізації: Перевірка історичних аудит-логів може бути корисною для проведення дослідження, оскільки вона дозволяє встановити, чи була нещодавно виявлена вразливість в системі використана зловмисником у минулому. Це може надати важливу інформацію для аналізу подій та подальшого покращення захисту системи. Такий аналіз може допомогти визначити, наприклад, масштаб попереднього кібератаки, методику, використану під час атаки, викрадену або змінену інформацію, що належить організації, підірвані можливості місії або бізнесу та тривалість атаки.

Пов’язані заходи: AU-6, AU-11.

(9) СКАНУВАННЯ ВРАЗЛИВОСТЕЙ - ТЕСТУВАННЯ ТА АНАЛІЗ ПРОНИКНЕННЯ

[Вилучено: включено до CA-8].

(10) СКАНУВАННЯ ВРАЗЛИВОСТЕЙ - ЗІСТАВЛЕННЯ ІНФОРМАЦІЇ ПРО СКАНУВАННЯ

Порівнювати результати сканування вразливостей для визначення наявності численних вразливостей на множинних векторів атак.

Рекомендації з реалізації: Вектор атаки — це шлях або засіб, за допомогою якого зловмисник може отримати доступ до системи, щоб доставити шкідливий код або викрасти інформацію. Організації можуть використовувати дерева атак, щоб показати, як ворожі дії супротивників взаємодіють і поєднуються, щоб спричинити несприятливий вплив або негативні наслідки для систем і організацій. Така інформація, разом із корельованими даними з інструментів сканування вразливостей, може забезпечити більшу ясність щодо векторів атак із кількома вразливими місцями та кількома переходами. Кореляція інформації про сканування вразливостей особливо важлива, коли організації переходять від старих технологій до новіших (наприклад, переходять від мережевих протоколів IPv4 до IPv6). Під час таких переходів деякі системні компоненти можуть ненавмисно залишитися некерованими, що створює можливості для використання зловмисниками.

Пов'язані заходи: Немає.

(11) СКАНУВАННЯ ВРАЗЛИВОСТЕЙ - ПРОГРАМА ПУБЛІЧНОГО ОПРИЛЮДНЕННЯ

Встановіть публічний канал для отримання повідомлень про вразливості в системах організації і компонентах системи.

Рекомендації з реалізації: Канал повідомлень є загальнодоступним і містить чіткі формулювання, які дозволяють добросовісно дослідити та розкрити вразливості організації. Організація не обумовлює свій дозвіл очікуванням безстрокового нерозголошення суб'єктом, що звітує, але може вимагати певний період часу для належного усунення вразливості.

Пов'язані заходи: Немає

Посилання: [ISO 29147], [SP 800-40], [SP 800-53A], [SP 800-70], [SP 800-115], [SP 800-126], [IR 7788], [IR 8011-4], [IR 8023].

## RA-6 ЗАХОДИ ПРОТИДІЇ ТЕХНІЧНІЙ РОЗВІДЦІ

Заходи захисту:
Використовувати заходи ПДТР за [*Призначення: визначені організацією місця*] [*Вибір (один або кілька): [Призначення: з визначеною організацією частотою]; [Призначення: за визначеними організацією подіями або показниками*]].

Рекомендації з реалізації: Заходи ПДТР мають впроваджуватися кваліфікованим персоналом. Організації використовують заходи ПДТР для виявлення наявності приладів технічного спостереження, а також для виявлення недоліків технічного захисту інформації. Крім того, заходи ПДТР забезпечують оцінювання стану технічного захисту інформації та об'єктів і охоплюють ретельну візуальну, електронну та фізичну перевірку об'єктів, що обстежуються. Аналіз заходів ПДТР надає інформацію для оцінювання ризиків і критичної інформації організації щодо впливу на організацію потенційних порушників.

Пов’язані заходи: Немає.

Посилення заходів: Немає.

Посилання: Немає.

## RA-7 РЕАГУВАННЯ НА РИЗИК

Заходи захисту:
Реагувати на результати оцінювання, моніторингу й аудиту безпеки та приватності.

Рекомендації з реалізації: До варіантів реагування на ризик належать: зменшення ризику шляхом впровадження нових заходів захисту або посилення наявних заходів; прийняття ризику з відповідним обґрунтуванням; обмін, перенесення ризику або відхилення ризику. Організаційна толерантність до ризику впливає на рішення та дії щодо реагування на ризик. Цей захід захисту визначає необхідність проведення відповідного реагування на ризик до того, як буде сформовано план дій. Наприклад, може бути ухвалене рішення про прийняття ризику або відхилення ризику, або про можливість негайно пом’якшити ризик. Тому план дій і введення важливих етапів не потрібні. Однак якщо реакція на ризик є пом’якшення ризику, а пом’якшення не може бути завершено негайно, формується план дій та вказівки про основні його етапи.

Пов’язані заходи: CA-5, IR-9, PM-4, PM-28, PM-32, RA-2, RA-3, SR-2.

Посилення заходів: Немає.

Посилання: FIPS Publications 199, 200, [SP 800-30], [SP 800-37], [SP 800-39], [SP 800-160-1].

## RA-8 ОЦІНЮВАННЯ ВПЛИВУ НА ПРИВАТНІСТЬ

Заходи захисту:
Проводити оцінювання впливу на приватність інформаційних систем, програм або інших заходів, які становлять ризик приватності перед тим, як:

a. розробити або закупити інформаційні технології, які збирають, підтримують чи поширюють критичну інформацію;

b. ініціювати створення нових архівів інформації, яка:

   1. буде зібрана, збережена чи розповсюджена за допомогою інформаційних технологій;

   2. містить персональні дані, які дозволяють встановити фізичне або онлайн-з’єднання з конкретною особою.

Рекомендації з реалізації: Оцінювання впливу на приватність — це аналіз того, яким чином відбувається управління інформацією для забезпечення: відповідності такого управління чинним законодавчим і регуляторним вимогам щодо приватності; визначення супутніх ризиків приватності та наслідків збору, використання, обробки, зберігання, поширення персональних даних; визначення та оцінювання механізмів захисту й альтернативних процесів управління інформацією для зменшення

потенційних проблем приватності. Оцінювання впливу на приватність подається у вигляді офіційного документа, який містить деталізацію процесу та результати аналізу. Для проведення аналізу організації використовують процеси оцінювання ризиків.

Організації проводять та розробляють оцінку впливу на приватність з достатньою ясністю та конкретністю, щоб продемонструвати, що організація повністю врахувала вимоги щодо забезпечення приватності та включила відповідні заходи забезпечення приватності від початкових етапів діяльності організації та протягом життєвого циклу інформації. Для здійснення ефективної оцінки впливу на приватність, вища посадова особа з питань приватності організації співпрацює з менеджерами програм, власниками систем, фахівцями з інформаційних технологій, представниками служби безпеки, юристами та іншими працівниками організації, які мають відповідну компетенцію. Крім того, оцінка впливу на приватність не є обмеженою в часі діяльністю, яка обмежена певним етапом життєвого циклу інформаційної системи або персональних даних. Натомість, аналіз приватності продовжується протягом життєвого циклу інформаційної системи та персональних даних. Тому, оцінка впливу на приватність є живим документом, який організації оновлюють кожного разу, коли змінюються інформаційні технології, практики організації або інші фактори, які змінюють ризики приватності, пов'язані з використанням таких інформаційних технологій. Для проведення оцінки впливу на приватність організації можуть використовувати оцінювання ризиків з питань безпеки та приватності. Організації також можуть використовувати інші відповідні процеси з різними назвами, включаючи аналіз ризиків приватності. Публікація результатів оцінки впливу на приватність може бути засобом інформування громадськості про практики організації щодо захисту приватності. Хоча проведення та публікація оцінки впливу на приватність можуть бути вимогами законодавства, організації можуть також створювати такі політики для внутрішнього використання, незалежно від наявності відповідних вимог законодавства. Для державних установ оцінка впливу на приватність може бути обов'язковою згідно з [EGOV]. Установи повинні отримати консультації від своєї старшої посадової особи з питань приватності та юрисконсультанта щодо необхідності проведення оцінки впливу на приватність відповідно до вимог [EGOV]. Крім того, вони мають мати на увазі статутні виключення та рекомендації OMB щодо надання такої оцінки.

Пов’язані заходи: CM-4, CM-9, CM-13, PT-2, PT-3, PT-5, RA-1, RA-3, RA-7.

Посилення заходів: Немає.

Посилання: [EGOV], [OMB A-130], [OMB M-03-22].

## RA-9 АНАЛІЗ КРИТИЧНОСТІ

Заходи захисту:
Визначити критичні компоненти інформаційної системи та функції, виконавши аналіз критичності для [*Призначення: визначених організацією систем, компонентів системи або послуг для системи*] в [*Призначення: визначенні організацією точки ухвалення рішень у життєвому циклі розробки системи*].

Рекомендації з реалізації: Не всі системні компоненти, функції чи служби обов’язково потребують посиленого захисту. Аналіз критичності є ключовим принципом управління ризиками в ланцюгах постачання та надає інформацію про пріоритетність заходів захисту. Визначення критичних компонентів і функцій системи має враховувати чинні норми, директиви, політики, стандарти та вказівки, вимоги щодо функціональності системи, інтерфейсів систем і компонентів, а також залежностей систем і компонентів. Системні інженери мають проводити комплексну функціональну

декомпозицію системи для виявлення важливих для місії функцій і компонентів. Функціональна декомпозиція містить визначення основних місій організації, що підтримуються системою, декомпозицію на конкретні функції для виконання цих місій, а також відстеження компонентів апаратного та програмного забезпечення. Це означає, що проводиться аналіз місій, які система повинна виконувати, щоб ідентифікувати конкретні функції, необхідні для досягнення цих місій. Також проводяться пошуки зв'язків між цими функціями та компонентами обладнання, програмного та апаратного забезпечення, які забезпечують виконання цих функцій. Це також охоплює випадки, коли декілька компонентів, які належать до однієї системи, взаємодіють для виконання певних функцій. Критичність системи або її компонентів може залежати від їхнього операційного середовища, зокрема від зв'язків та залежностей від інших кіберфізичних систем, пристроїв та послуг IT, що можуть бути підключені до системи, а також залежностей від інших систем, з якими вона може взаємодіяти. Компоненти системи, які дають безпосередній доступ до критичних компонентів або функцій системи, є критичними через внутрішні вразливості, які вони створюють. Оцінка критичності компонентів та функцій ґрунтується на тому, як відмова компонентів або функцій може вплинути на виконання місій, які підтримує система, що містить ці компоненти та функції.

Аналіз критичності виконується під час розробки, модифікації або оновлення архітектури чи проекту. Якщо провести аналіз критичності на ранніх етапах життєвого циклу розробки системи, організації можуть внести зміни до проекту системи з метою зменшення критичності окремих компонентів та функцій, наприклад, шляхом додавання резервних елементів або альтернативних шляхів при проектуванні системи системи. Аналіз критичності також може впливати на заходи захисту, необхідні розробникам-підрядникам. Крім того, важливим аспектом є проведення аналізу критичності інформації, нарівні з аналізом критичності систем, її компонентів та сервісів. Такий аналіз проводиться в рамках категоризації безпеки в RA-2.

Пов’язані заходи: CP-2, PL-2, PL-8, PL-11, PM-1, PM-11, RA-2, SA-8, SA-12, SA-15, SA-20, SR-5.

Посилення заходів: Немає.

Посилання: [IR 8179].

## RA-10 АКТИВНИЙ ПОШУК ЗАГРОЗ

Заходи захисту:

a. Створити та підтримувати можливості активного пошуку кіберзагроз:

    1. пошук індикаторів компроментації в системах організації;

    2. виявлення, відстеження та знищення загроз, які можуть обходити існуючі засоби контролю безпеки.

b. використовуйте можливості активного пошуку загроз *[Призначення: частота, визначена організацією*].

Рекомендації з реалізації: Активний пошук загроз – це засіб кіберзахисту, який відмінний від традиційних заходів захисту, таких як брандмауери, системи виявлення та запобігання вторгненням, карантин шкідливого коду в пісочницях, а також технології та системи керування інформацією про безпеку та подіями. Активний пошук

кіберзагроз передбачає проактивний пошук систем організації, мереж та інфраструктури на наявність складних загроз. Мета полягає в тому, щоб відслідковувати та перешкоджати кіберзлочинцям якомога раніше в послідовності атак і відчутно підвищити швидкість і точність реагування організацій на них. Ознаками компрометації є незвичайний мережевий трафік, незвичні зміни файлів і наявність шкідливого коду. Команди пошуку загроз використовують наявні дані про загрози та можуть створювати нові дані про загрози, які надають іншим організаціям обміну та аналізу інформації (ISAO), центрам обміну та аналізу інформації (ISAC), а також відповідним урядовим департаментам і установам.

Пов’язані заходи: CA-2, CA-7, CA-8, RA-3, RA-5, RA-6, SI-4.

Посилення заходів: Немає.

Посилання: [SP 800-30].

## 10.17 Клас заходів захисту SA — ПРИДБАННЯ СИСТЕМИ ТА ПОСЛУГ

### SA-1 ПОЛІТИКА ТА ПРОЦЕДУРИ ПРИДБАННЯ СИСТЕМИ ТА ПОСЛУГ

Заходи захисту:

a. Розробити, задокументувати та поширити серед [*Призначення: визначеного організацією персоналу або ролей*]:

   1. [*Вибір (один або декілька): рівень організації; рівень місії/бізнес-процесу; рівень системи*] політики придбання систем і послуг, яка:

      (a) містить мету, сферу застосування, ролі, обов'язки, відповідальність керівництва, координацію між організаційними підрозділами та систему контролю (complaince);

      (b) відповідає чинному законодавству, виконавчим наказам, директивам, нормам, політикам, стандартам і рекомендаціям.

   2. Процедури, що полегшують впровадження політики та заходів придбання систем і послуг.

b. Призначити [*Призначення: визначену організацією посадову особу*] для управління політикою та процедурами придбання системи та послуг.

c. Переглядати й оновлювати поточні політику та процедури придбання систем та послуг:

   1. Поточну політику придбання системи та послуг [*Призначення: з визначеною організацією частотою*].

   2. Поточні процедури придбання системи та послуг [*Призначення: з визначеною організацією частотою*] та наступні [*Призначення: події, визначені організацією*].

Рекомендації з реалізації: Цей захід захисту стосується встановлення політики та процедур для ефективного здійснення заходів і їх посилень у класі SA. Стратегія управління ризиками є важливим фактором у встановленні політики та процедур. Комплексна політика та процедури допомагають забезпечити безпеку та приватність. За наявності політики, а також планів захисту інформації та персональних даних на рівні організації, конкретні системні політики та процедури можуть бути не потрібні. Політика може бути внесена до складу загальної політики безпеки та приватності або може бути представлена кількома політиками (у випадках складної архітектури). За потреби можна встановити процедури для програм безпеки та приватності, для місії чи бізнес-процесів, а також для систем. Процедури описують, як має реалізуватися політика чи заходи захисту та як вони можуть бути спрямовані на персонал або роль, що є об'єктом процедури. Процедури можуть бути задокументовані в планах захисту інформації та персональних даних (як один або декілька документів). Події, які можуть спричинити оновлення політики та процедур придбання систем та послуг, включають висновки оцінювання або аудиту, інциденти чи порушення безпеки або зміни в законах, розпорядженнях, директивах, положеннях, політиках, стандартах і рекомендаціях. Просте повторне встановлення заходів захисту не є організаційною політикою чи процедурою.

Пов’язані заходи: PM-9, PS-8, SA-8, SI-12.

Посилення заходів: Немає.

Посилання: [OMB A-130], [SP 800-12], [SP 800-30], [SP 800-39], [SP 800-100], [SP 800-160-1].

## SA-2 РОЗПОДІЛ РЕСУРСІВ

Заходи захисту:

a. Визначити вимоги щодо інформаційної безпеки та приватності для систем або послуг для системи при плануванні завдань та процесів.

b. Визначити, задокументувати та розподілити ресурси, які необхідні для захисту систем або послуг для системи у рамках процесу фінансового планування в організації та управління інвестиціями.

c. Створити окрему позицію бюджету для фінансування заходів із забезпечення інформаційної безпеки та приватності.

Рекомендації з реалізації: Розподіл ресурсів для інформаційної безпеки та приватності стосується фінансування для придбання систем та послуг, фінансування обслуговування та забезпечення ланцюга постачання протягом усього життєвого циклу системи.

Пов’язані заходи: PL-7, PM-3, PM-11, SA-9, SR-3, SR -5.

Посилення заходів: Немає.

Посилання: [OMB A-130], [SP 800-37], [SP 800-160-1].

## SA-3 ЖИТТЄВИЙ ЦИКЛ РОЗРОБКИ СИСТЕМИ

Заходи захисту:

a. Придбати, розробити та керувати системою, використовуючи [*Призначення: визначений організацією життєвий цикл розробки*], який охоплює питання захисту інформації та приватності.

b. Визначити та задокументувати роль і обов’язки із забезпечення безпеки та приватності інформації протягом усього життєвого циклу розробки системи.

c. Визначити осіб, які мають повноваження та обов’язки в області інформаційної безпеки та приватності.

d. Інтегрувати процес управління інформаційною безпекою та приватністю в процеси життєвого циклу розробки системи.

Рекомендації з реалізації: Процес життєвого циклу розробки системи надає основу для успішного розвитку, впровадження та функціонування систем. Для застосування необхідних заходів захисту протягом усього життєвого циклу розробки системи потрібне базове розуміння інформаційної безпеки та приватності, загроз, уразливостей,

несприятливих наслідків і ризиків для критичних місій та функцій. Принципи, які описані в SA-8, допомагають правильно розробляти, кодувати й тестувати системи та компоненти системи. До процесів життєвого циклу розробки системи мають бути залучені кваліфіковані працівники служби безпеки інформації, а також інші посадові особи, які мають відношення до питань проєктування та розгортання систем. За необхідності може проводитися додаткове навчання на базі ролей. Ефективна інтеграція вимог безпеки та приватності в архітектурі організації також допомагає гарантувати, що важливі питання безпеки та приватності враховуються протягом життєвого циклу системи та що ці міркування безпосередньо пов'язані з місією організації та бізнес-процесами. Цей процес також полегшує інтеграцію архітектур інформаційної безпеки та приватності в архітектурі організації відповідно до плану (стратегії) управління ризиками організації. Оскільки життєвий цикл розробки системи охоплює безліч організацій, включно з, наприклад, зовнішніми постачальниками, розробниками та постачальниками послуг, важливо усвідомити, що функції управління (та управління ризиками) в ланцюгах постачання та контролю відіграють значну роль у загальній ефективності управління системою протягом цього життєвого циклу розробки.

Пов'язані заходи: AT-3, PL-8, PM-7, SA-4, SA-5, SA-8, SA-11, SA-15, SA-17, SA-22, SR-3, SR-4, SR -5, SR-9.

Посилення заходів:

(1) ЖИТТЄВИЙ ЦИКЛ РОЗРОБКИ СИСТЕМИ - УПРАВЛІННЯ СЕРЕДОВИЩЕМ РОЗРОБКИ

Забезпечити захист середовища розробки системи, відповідно до ризиків протягом усього життєвого циклу розробки системи для системи, компонентів системи або служб.

Рекомендації з реалізації: Передвиробниче середовище включає середовища розробки, тестування та інтеграції. Аналіз критичності та застосування заходів захисту розробниками також сприяють створенню безпечнішого середовища розробки системи.

Пов'язані заходи: CM-2, CM-4, RA-3, RA-9, SA-4.

(2) ЖИТТЄВИЙ ЦИКЛ РОЗРОБКИ СИСТЕМИ - ВИКОРИСТАННЯ РЕАЛЬНИХ ДАНИХ

(a) Затвердити, задокументувати та контролювати використання реальних даних у середовищах розробки, тестування та інтеграції системи, компонента системи або послуг для системи.

(b) Захистити середовище розробки для системи, системного компонента або системної служби на тому ж рівні впливу або класифікації, що й будь-які реальні дані, що використовуються в середовищі розробки.

Рекомендації з реалізації: Реальні дані також називаються оперативними даними. Використання реальних даних у виробничих середовищах може призвести до значного ризику для організацій. Крім того, використання персональних даних під час тестування, досліджень і навчання підвищує ризик несанкціонованого розголошення або неправомірного використання таких даних. Тому для організації важливо керувати будь-якими додатковими ризиками, які можуть виникнути в результаті використання поточних або

оперативних даних. Організації можуть мінімізувати такий ризик, використовуючи тестові дані під час проєктування, розробки й тестування систем, компонентів системи та сервісів. Методи оцінки ризику можуть бути використані, щоб визначити, чи є ризик використання реальних чи оперативних даних прийнятним.

Пов'язані заходи: PM-25, RA-3.

(3) ЖИТТЄВИЙ ЦИКЛ РОЗРОБКИ СИСТЕМИ - ОНОВЛЕННЯ ТЕХНОЛОГІЙ

Планувати та впровадити графік оновлення технологій для підтримки системи протягом усього життєвого циклу розробки системи.

Рекомендації з реалізації: Планування оновлення технологій може охоплювати апаратне та програмне забезпечення, процеси, персонал, постачальників послуг і обладнання. Використання застарілої технології може збільшити ризики безпеки та приватності, пов'язані з: непідтримуваними компонентами; підробленими або перепрофільованими компонентами, компонентами, які не відповідають вимогам безпеки чи приватності, повільними або непрацездатними компонентами, компонентами з ненадійних джерел, випадковою помилкою персоналу або підвищеною складність. Технологічні оновлення зазвичай відбуваються на стадії експлуатації та обслуговування життєвого циклу розробки системи.

Пов'язані заходи: MA-6.

Посилання: [OMB A-130], [SP 800-30], [SP 800-37], [SP 800-160-1], [SP 800-171], [SP 800-172].

## SA-4 ПРОЦЕС ЗАКУПІВЕЛЬ

Заходи захисту: Включіть такі вимоги, описи та критерії, явно або за допомогою посилання, використовуючи [*Вибір (один або більше): стандартні пункти контракту; [Призначення: пункти контракту, визначені організацією]]* в контракті про придбання системи, системного компонента або системної послуги:

a. функціональні вимоги безпеки та приватності;

b. вимоги до стійкості механізму;

c. вимоги до забезпечення безпеки та приватності;

d. заходи захисту для забезпечення вимог безпеки та приватності;

e. вимоги до захисту документації з безпеки та приватності;

f. опис середовища розробки системи та середовища, у якому система призначена для роботи;

g. розподіл відповідальності або визначення сторін, відповідальних за управління інформаційною безпекою, приватністю та управлінням ланцюгами постачання;

h. критерії прийнятності.

Рекомендації з реалізації: Функціональні вимоги безпеки та приватності зазвичай

випливають із вимог високого рівня безпеки та приватності, описаних у SA-2. Похідні вимоги включають можливості безпеки та приватності, функції та механізми. Вимоги до міцності, пов'язані з такими можливостями, функціями та механізмами, включають ступінь правильності, повноти, стійкість до втручання або обходу та стійкість до прямої атаки. Вимоги до гарантії включають процеси розробки, процедури та методології, а також докази діяльності з розробки та оцінки, які дають підстави для впевненості в тому, що необхідна функціональність реалізована та має необхідну силу механізму. [SP 800-160-1] описує процес розробки вимог як частину життєвого циклу розробки системи.

Заходи захисту можна розглядати як опис засобів захисту та можливостей захисту, відповідних для досягнення конкретних цілей безпеки та приватності організації та для відображення вимог зацікавлених сторін до безпеки та приватності. Заходи захисту вибираються та впроваджуються, щоб задовольнити системні вимоги та включати обов'язки розробника та організації. Заходи захисту можуть включати технічні, адміністративні та фізичні аспекти. У деяких випадках вибір і впровадження заходів захисту може вимагати додаткової специфікації з боку організації у формі похідних вимог або інстанційованих значень параметрів таких заходів. Похідні вимоги та значення параметрів заходів захисту можуть бути необхідними для забезпечення відповідного рівня деталізації їх впровадження протягом життєвого циклу розробки системи.

Вимоги щодо документації безпеки та приватності охоплюють усі етапи життєвого циклу розробки системи. Документація містить вказівки для користувачів і адміністраторів щодо впровадження та роботи заходів захисту. Рівень деталізації, необхідний у такій документації, базується на категоризації безпеки або рівні класифікації системи та ступені, до якого організації залежать від можливостей, функцій або механізмів, щоб відповідати очікуванням реагування на ризики. Вимоги можуть містити обов'язкові параметри конфігурації, які визначають дозволені функції, порти, протоколи та служби. Критерії прийнятності для систем, компонентів системи і послуг для системи визначаються так само, як критерії для будь-якого організаційного придбання або закупівлі.

Пов'язані заходи: CM-6, CM-8, PS-7, SA-3, SA-5, SA-8, SA-11, SA-15, SA-16, SA-17, SA-21, SR-3, SR -5.

Посилення заходів:

(1) ПРОЦЕС ЗАКУПІВЕЛЬ - ФУНКЦІОНАЛЬНІ ВЛАСТИВОСТІ ЗАХОДІВ

Вимагати від розробника системи, компонента системи або системної служби надати опис функціональних властивостей заходів захисту, які повинні бути реалізовані.

Рекомендації з реалізації: Функціональні властивості засобів безпеки та приватності описують функціональні можливості (тобто безпеку чи приватність, функції чи механізми), заходи захисту інтерфейсів, а також стосуються функціональності та структури даних.

Пов'язані заходи: Немає.

(2) ПРОЦЕС ЗАКУПІВЕЛЬ - РОЗРОБКА ТА ВПРОВАДЖЕННЯ ІНФОРМАЦІЇ ДЛЯ ЗАХОДІВ

Вимагати від розробника системи, компонента системи або системної служби надати інформацію про розробку та реалізацію для вибраних заходів, яка містить: [*Вибір (один або більше): пов'язані з безпекою зовнішні системні інтерфейси; архітектуру (проєкт) високого рівня; архітектури (проєкт) низького рівня; вихідний код або апаратні схеми;* [*Призначення: визначена організацією інформація щодо розробки та впровадження*]] на [*Призначення: визначений організацією рівень деталізації*].

Рекомендації з реалізації: Залежно від складності організації може вимагатися різний рівень деталізації документації з розробки та впровадження заходів, вимог до надійності та стійкості, а також вимог до аналізу й тестування. Система може бути розділена на кілька підсистем, кожна підсистема своєю чергою може містити один або кілька модулів. Проектування високого рівня для системи виражається в термінах підсистем та інтерфейсів між підсистемами, що забезпечують функціональність, важливу для безпеки. Низькорівневе проектування системи виражається в термінах модулів та інтерфейсів між модулями, що забезпечують функціональність, важливу для безпеки. Документація щодо розробки та впровадження може містити виробника, версію, серійний номер, геш-підпис перевірки, бібліотеки програмного забезпечення, що використовуються, дату придбання або завантаження, а також постачальника або джерело завантаження. Вихідний код і апаратні схеми називаються представленням реалізації системи.

Пов'язані заходи: Немає.

(3) ПРОЦЕС ЗАКУПІВЕЛЬ - МЕТОДИ, ТЕХНІКИ ТА ПРАКТИКИ РОЗРОБКИ

Вимагати від розробника системи, системного компонента або системної служби продемонструвати використання процесу життєвого циклу розробки системи, що містить у собі:

a) [*Призначення: визначені організацією методи проєктування (інженерії) систем*];

b) [*Вибір (один або більше): методи проєктування безпеки систем; методи проєктування приватності; проєктування (інженерії) систем*];

c) [*Призначення: визначені організацією методи розробки програмного забезпечення; методи тестування, оцінювання, перевірки та підтвердження; та процеси контролю якості*].

Рекомендації з реалізації: Використання сучасних методів, технік і практик розробки програмного забезпечення, методів системної інженерії, а також процесів контролю якості протягом життєвого циклу розробки системи допомагає зменшити кількість прихованих помилок у системах, компонентах системи та в послугах для системи. Зменшення кількості та серйозності таких помилок зменшує кількість вразливостей у цих системах, компонентах і службах. Прозорість у методах і техніках, які розробники обирають і впроваджують для проектування систем, безпеки систем і приватності, розробки програмного забезпечення, оцінки компонентів і систем, а також процесів контролю якості, забезпечує підвищений рівень впевненості в надійності системи, системного компонента або придбання системної послуги.

Пов'язані заходи: Немає.

(4) ПРОЦЕС ЗАКУПІВЕЛЬ - ВІДНЕСЕННЯ КОМПОНЕНТІВ ДО СИСТЕМ

[Вилучено: включено до CM-8 (9)].

(5) ПРОЦЕС ЗАКУПІВЕЛЬ - КОНФІГУРАЦІЇ СИСТЕМИ, КОМПОНЕНТА ТА СИСТЕМНОЇ СЛУЖБИ

Вимагати від розробника системи, компонента системи або системної служби:

(a) встановити систему, компонент або системну службу за допомогою [*Призначення: визначених організацією конфігурацій безпеки*];

(b) використовувати ці конфігураційні налаштування за замовчуванням для будь-якої наступної переінсталяції або оновлення системи, компонента чи послуги.

Рекомендації з реалізації: Конфігурації безпеки містять, наприклад, затверджені базові профілі безпеки та будь-які обмеження щодо функцій, портів, протоколів і служб. До характеристик безпеки належать, наприклад, необхідність зміни паролів за замовчуванням.

Пов’язані заходи: Немає.

(6) ПРОЦЕС ЗАКУПІВЕЛЬ - ВИКОРИСТАННЯ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ

(a) Використовувати засоби захисту інформації, які пройшли державну експертизу або сертифікацію, створені для технічного та криптографічного захисту інформації.

(b) Переконатися, що ці засоби захисту мають позитивний експертний висновок або сертифікат відповідності, а також відповідні дозволи для використання для захисту критичної інформації.

Рекомендації з реалізації: Для використання схваленого NSA керування ключами можуть знадобитися комерційні стандартні IA або продукти інформаційної технології з підтримкою IA, які використовуються для захисту секретної інформації за допомогою криптографічних засобів. Див. [NSA CSFC].

Пов’язані заходи: SC-8, SC-12, SC-13.

(7) ПРОЦЕС ЗАКУПІВЕЛЬ - ЗАТВЕРДЖЕНІ ПРОФІЛІ ЗАХИЩЕНОСТІ

(a) Обмежити використання комерційної готової до використання технічної продукції, створеної для захисту інформації та з функцією підтримки забезпечення безпеки інформації, до тих продуктів, які були успішно оцінені відповідно до профілю захищеності для конкретного типу технології, затвердженого уповноваженим державним органом, якщо такий профіль наявний.

(b) У разі, якщо немає профілю захищеності для певного типу технологій, затвердженого уповноваженим органом, але забезпечення політики безпеки продукту, що надається на комерційній основі, залежить від криптографічних функцій, — вимагати, щоб криптографічний модуль пройшов державну експертизу, мав позитивний експертний висновок і був рекомендований до використання уповноваженим органом.

Рекомендації з реалізації: Немає.

Пов’язані заходи: IA-7, SC-12, SC-13.

(8) ПРОЦЕС ЗАКУПІВЕЛЬ - ПЛАН БЕЗПЕРЕРВНОГО МОНІТОРИНГУ ЗАХОДІВ БЕЗПЕКИ

Вимагати від розробника системи, системного компонента або системної служби створити план безперервного моніторингу ефективності заходів безпеки та приватності, який узгоджується з відповідним планом постійного моніторингу організації.

Рекомендації з реалізації: План безперервного моніторингу визначає, чи реалізований у системі повний набір запланованих і необхідних систем безпеки та заходів приватності. Такі плани мають бути розроблені з достатнім рівнем деталізації.

Пов’язані заходи: CA-7.

(9) ПРОЦЕС ЗАКУПІВЕЛЬ - ФУНКЦІЇ, ПОРТИ, ПРОТОКОЛИ ТА ПОСЛУГИ, ЩО ВИКОРИСТОВУЮТЬСЯ

Вимагати від розробника системи, компонента системи або системної служби визначити функції, порти, протоколи та послуги, призначені для використання організацією.

Рекомендації з реалізації: Ідентифікація функцій, портів, протоколів і послуг на ранніх стадіях життєвого циклу розробки системи (наприклад, під час початкових етапів визначення вимог і проектування) дозволяє організаціям впливати на архітектуру системи, компонента системи чи служби. Це допомагає уникати або мінімізувати використання функцій, портів, протоколів або служб, що створюють зайві ризики, а також розуміти компроміси, пов’язані з блокуванням конкретних портів, протоколів або служб. Рання ідентифікація функцій, портів, протоколів і служб дозволяє уникнути дорогої модернізації заходів захисту після впровадження системи, компонента або системної служби. SA-9 описує вимоги до зовнішніх послуг для системи. Організації визначають, які функції, порти, протоколи та послуги надаються із зовнішніх джерел.

Пов’язані заходи: CM-7, SA-9.

(10) ПРОЦЕС ЗАКУПІВЕЛЬ - ВИКОРИСТАННЯ ЗАТВЕРДЖЕНИХ ПРОДУКТІВ ПІДТВЕРДЖЕННЯ ОСОБИСТОСТІ (PIV)

Використовувати лише ту інформаційно-технічну продукцію, що перебуває в списку продуктів схвалених FIPS 201, затверджених уповноваженим органом, для можливостей підтвердження особистості (PIV), реалізованих в системах організації.

Рекомендації з реалізації: Продукти зі списку продуктів, затверджених FIPS 201, відповідають вимогам NIST щодо підтвердження особи (PIV) федеральних службовців і підрядників. Картки PIV використовуються для багатофакторної автентифікації в системах і організаціях.

Пов’язані заходи: IA-2, IA-8, PM-9.

(11) ПРОЦЕС ЗАКУПІВЕЛЬ – СИСТЕМА ЗАПИСІВ

Включіть [*Призначення: визначені організацією вимоги Закону про конфіденційність*] у договір про придбання для експлуатації системи записів від імені організації для виконання місії або функції організації.

Рекомендації з реалізації: Якщо згідно з договором організація передбачає функціонування системи записів для виконання організаційної місії або функції, організація відповідно до своїх повноважень забезпечує застосування вимог [PRIVACT] до системи записів.

Пов'язані заходи: PT-6.

(12) ПРОЦЕС ЗАКУПІВЕЛЬ – ПРАВО ВЛАСНОСТІ НА ДАНІ

a) включіть вимоги щодо володіння даними організації в договір на придбання;

b) вимагати видалення всіх даних із системи підрядника та повернення в організацію протягом [*Завдання: часові рамки, визначені організацією*].

Рекомендації з реалізації: Підрядники, які керують системою, що містить дані, які належать організації, що ініціювала контракт, мають політику та процедури для видалення даних зі своїх систем та/або повернення даних у часові рамки, визначені контрактом.

Пов'язані заходи: Немає.

Посилання: [PRIVACT], [OMB A-130], [ISO 15408-1], [ISO 15408-2], [ISO 15408-3], [ISO 29148], [FIPS 140-3], [FIPS 201-2], [SP 800-35], [SP 800-37], [SP 800-70], [SP 800-73-4], [SP 800-137], [SP 800-160-1], [SP 800-161], [IR 7539], [IR 7622], [IR 7676], [IR 7870], [IR 8062], [NIAP CCEVS], [NSA CSFC].

## SA-5 СИСТЕМНА ДОКУМЕНТАЦІЯ

Заходи захисту:

a. Отримати або розробити документацію адміністратора для системи, системного компонента або системної служби, яка описує:

1. безпечне налаштування, установку та роботу системи, компонента або служби;

2. ефективне використання, підтримку функцій та механізмів безпеки та приватності;

3. відомі вразливості щодо конфігурації та використання адміністративних або привілейованих функцій.

b. Отримати або розробити документацію користувача для системи, системного компонента або системної служби, яка описує:

1. функції та механізми безпеки та приватності та способи ефективного використання цих функцій і механізмів;

2. методи взаємодії з користувачем, що дозволяють окремим особам використовувати систему, компонент або службу безпечнішим чином та захищати індивідуальну приватність;

3. обов'язки користувача щодо забезпечення безпеки системи, компонента або служби та приватності окремих осіб.

c. Документувати спроби отримати доступ до документації системи, системного компонента чи системної служби, коли така документація недоступна або ж відсутня, і вжити [*Призначення: визначені організацією заходи*] у відповідь.

d. Поширити документацію серед [*Призначення: визначеного організацією персоналу або посадових осіб*].

Рекомендації з реалізації: Цей захід допомагає організаційному персоналу зрозуміти впровадженнґ та роботу заходів захисту. Організації розглядають можливість встановлення конкретних заходів захисту для визначення якості та повноти наданого контенту. Системна документація може використовуватися, наприклад, для підтримки управління ризиками ланцюга постачань, реагування на інциденти та інших функцій. До посадових осіб або ролей, що потребують документації, можуть належати власники системи, посадові особи служби безпеки, системні адміністратори. До спроб отримати документацію можуть належати прямий контакт з виробниками чи постачальниками та вебпошук. Неможливість отримати необхідну документацію може виникнути, наприклад, через вік системи чи компонента або відсутність підтримки розробників і підрядників. У таких ситуаціях організаціям може знадобитися відтворити цю документацію. Рівень захисту, що надається для документації, має бути співмірним з категорією безпеки або класифікацією системи. Документація, що стосується вразливостей системи, може вимагати підвищеного рівня захисту. Захищена робота системи включає початковий запуск системи та відновлення безпечної роботи системи після перерви в роботі системи.

Пов'язані заходи: CM-4, CM-6, CM-7, CM-8, PL-2, PL-4, PL-8, PS-2, SA-3, SA-4, SA-8, SA-9, SA-10, SA-11, SA-15, SA-16, SA-17, SI-12, SR-3.

Посилення заходів:

(1) СИСТЕМНА ДОКУМЕНТАЦІЯ - ФУНКЦІОНАЛЬНІ ВЛАСТИВОСТІ ЗАХОДІВ БЕЗПЕКИ

[Вилучено: включено до SA-4 (1)].

(2) СИСТЕМНА ДОКУМЕНТАЦІЯ - ЗОВНІШНІ СИСТЕМНІ ІНТЕРФЕЙСИ, ЩО СТОСУЮТЬСЯ БЕЗПЕКИ

[Вилучено: включено до SA-4 (2)].

(3) СИСТЕМНА ДОКУМЕНТАЦІЯ - АРХІТЕКТУРА (ПРОЄКТ) ВИСОКОГО РІВНЯ

[Вилучено: включено до SA-4 (2)].

(4) СИСТЕМНА ДОКУМЕНТАЦІЯ - АРХІТЕКТУРА (ПРОЄКТ) НИЗЬКОГО РІВНЯ

[Вилучено: включено до SA-4 (2)].

(5) СИСТЕМНА ДОКУМЕНТАЦІЯ - ВИХІДНИЙ КОД

[Вилучено: включено до SA-4 (2)].

Посилання: [SP 800-160-1].

## SA-6 ОБМЕЖЕННЯ ЩОДО ВИКОРИСТАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

[Вилучено: Включено до CM-10 та SI-7].

## SA-7 ВСТАНОВЛЕНЕ КОРИСТУВАЧЕМ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

[Вилучено: Включено до CM-11 та SI-7].

## SA-8 БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ

Заходи захисту:
Застосовувати [*Призначення: визначені організацією принципи інжинірингу безпеки та конфіденційності системи*] в специфікації, проєктуванні, розробці, впровадженні та зміні системи й компонентів системи.

Рекомендації з реалізації: Принципи безпечного проектування систем і конфіденційності тісно пов'язані з життєвим циклом розробки системи та впроваджуються протягом усього життєвого циклу розробки (див. SA-3). Організації можуть застосовувати принципи безпечного проектування та конфіденційності до нових систем, що розробляються, або до систем, які оновлюються. Для існуючих систем організації застосовують принципи безпечного проектування та конфіденційності для оновлення та модифікації системи, з урахуванням поточного стану апаратного, програмного забезпечення та мікропрограмних компонентів у цих системах.

Застосування принципів безпечного проектування і конфіденційності допомагає організаціям розробляти надійні, захищені та стійкі системи та зменшує сприйнятливість до збоїв, небезпеки, загроз та проблем конфіденційності для окремих осіб. Приклади принципів безпечного проектування системи включають: розробку багаторівневих засобів захисту; створення політики безпеки та конфіденційності, архітектури та елементів керування як основи для проектування та розробки; включення вимог безпеки та конфіденційності до життєвого циклу розробки системи; окреслення фізичних і логічних кордонів безпеки; забезпечення навчання розробників створенню безпечного програмного забезпечення; адаптація засобів контролю відповідно до потреб організації; і виконання моделювання загроз для визначення випадків використання, агентів загроз, векторів і шаблонів атак, шаблонів проектування та компенсаційного контролю, необхідного для зменшення ризику.

Організації, які застосовують інженерні принципи безпечного проектування та конфіденційності, можуть сприяти розробці надійних, безпечних систем, компонентів системи і послуг для системи; знизити ризик до прийнятного рівня; і приймати обґрунтовані рішення щодо управління ризиками. Принципи безпечного проектування системи також можна використовувати для захисту від певних ризиків ланцюга постачання та включати в конструкцію апаратного забезпечення, захищеного від несанкціонованого втручання.

Пов'язані заходи: PL-8, PM-7, RA-2, RA-3, RA-9, SA-3, SA-4, SA-15, SA-17, SA-20, SC-2, SC-3, SC-32, SC-39, SR-2, SR-3, SR-4, SR-5.

Посилення заходів:

(1) БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - ЧІТКА АБСТРАКЦІЯ

Реалізуйте принцип проектування безпеки чітких абстракцій.

Рекомендації з реалізації: Принцип чітких абстракцій — це принцип, за якого система має прості, чітко визначені інтерфейси та функції, які забезпечують узгоджене та інтуїтивно зрозуміле уявлення про дані та способи керування ними. Зрозумілість, простота, необхідність і достатність інтерфейсів системи у поєднанні з точним визначенням їхньої функціональної поведінки — сприяє легкому аналізу, перевірці та тестуванню, а також правильному та безпечному використанню системи. Чіткість абстракції суб'єктивна. Приклади, які відображають застосування цього принципу, включають уникнення надлишкових інтерфейсів, які не використовуються; приховування інформації; і уникнення семантичного перевантаження інтерфейсів або їх параметрів. Приховування інформації (тобто незалежне від представлення програмування) — це тип проектування, який використовується для забезпечення того, щоб внутрішнє представлення інформації в одному системному компоненті не було видимим для іншого системного компонента, який викликає перший компонент, таким чином, щоб опублікована абстракція не впливала на те, як даними можна керувати всередині.

Пов’язані заходи: Немає.

(2) БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - НАЙМЕНШ ПОШИРЕНИЙ МЕХАНІЗМ

Реалізація принципу проектування безпеки найменш поширеного механізму в [*Призначення: визначені організацією системи або компоненти системи*]

Рекомендації з реалізації: Принцип найменш поширеного механізму стверджує, що кількість механізмів, спільних для кількох користувачів і від яких залежать усі користувачі, зведена до мінімуму. Мінімізація механізму передбачає, що різні компоненти системи не використовують один ітой самий механізм для доступу до системного ресурсу. Кожен спільний механізм (особливо механізм, що включає спільні змінні) відображає потенційний інформаційний шлях між користувачами і має бути ретельно розроблений, щоб гарантувати, що він ненавмисно не порушить безпеку. Реалізація принципу найменш спільного механізму допомагає зменшити несприятливі наслідки спільного використання стану системи різними програмами. Одна програма, яка пошкоджує спільний стан (включаючи спільні змінні), потенційно може пошкодити інші програми, які залежать від цього стану. Принцип найменш загального механізму також підтримує принцип простоти конструкції та вирішує проблему прихованих каналів зберігання [LAMPSON73]

Пов’язані заходи: Немає.

(3) БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - МОДУЛЬНІСТЬ І БАГАТОРІВНЕВІСТЬ

Запровадити принципи проектування безпеки модульності та багаторівневості в [*Призначення: визначені організацією системи або системні компоненти*].

Рекомендації з реалізації: Принципи модульності та багаторівневості є основоположними для системної інженерії. Модульність і багаторівневість, отримані в результаті функціональної декомпозиції, ефективні в управлінні складною системою, оскільки дозволяють зрозуміти структуру системи. Модульна декомпозиція, або вдосконалення дизайну системи, є складним завданням і суперечить загальним принциповим положенням. Модульність служить для ізоляції функцій і пов'язаних структур даних у чітко визначені логічні одиниці. Розподіл системи на рівні дозволяє краще зрозуміти взаємозв'язки цих одиниць, щоб залежності були чіткими та можна було уникнути небажаної складності. Принцип модульності проектування безпеки розширює функціональну модульність, щоб включити міркування, засновані на довірі, надійності, привілеях і політиці безпеки. Модульна декомпозиція з урахуванням безпеки включає розподіл політик системам у мережі, поділ програм системи на процеси з окремими адресними просторами, розподіл політик системи на рівні та поділ процесів на суб'єкти з різними привілеями на основі доменних привілеїв, що підтримуються апаратним забезпеченням.

Пов'язані заходи: SC-2, SC-3.

(4) БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ – ЧАСТКОВО ВПОРЯДКОВАНІ ЗАЛЕЖНОСТІ

Запровадити принцип проектування безпеки частково впорядкованих залежностей у [*Призначення: визначені організацією системи або системні компоненти*].

Рекомендації з реалізації: Принцип частково впорядкованих залежностей стверджує, що синхронізація, виклики та інші залежності в системі є частково впорядкованими. Фундаментальною концепцією проектування системи є багаторівневість, за допомогою якої система організована в чітко визначені, функціонально пов'язані модулі або компоненти. Рівні лінійно впорядковані щодо міжрівневих залежностей, так що вищі рівні залежать від нижчих. Забезпечуючи функціональні можливості для вищих рівнів, деякі рівні можуть бути самодостатніми та не залежати від нижчих рівнів. Хоча часткове впорядкування всіх функцій у даній системі може бути неможливим, якщо циклічні залежності обмежені для виникнення в межах рівнів, властивими проблемами циклізму можна легше керувати. Частково впорядковані залежності та рівневість системи значно сприяють простоті та узгодженості дизайну системи та полегшують тестування і аналіз системи.

Пов'язані заходи: Немає.

(5) БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - ЕФЕКТИВНИЙ ОПОСЕРЕДКОВАНИЙ ДОСТУП

Реалізація принципу проектування безпеки ефективного опосередкованого доступу в [*Призначення: системи, визначені організацією, або системні компоненти*].

Рекомендації з реалізації: Принцип ефективного опосередкованого доступу стверджує, що механізми забезпечення виконання політики використовують найменш поширений доступний механізм, задовольняючи вимоги зацікавлених сторін у межах визначених обмежень. Проміжний доступ до ресурсів системи (тобто ЦП, пам'яті, пристроїв, комунікаційних портів, послуг, інфраструктури,

даних та інформації) часто є домінуючою функцією безпеки захищених систем. Це також дозволяє реалізувати захист можливостей, наданих системою зацікавленим сторонам. Проміжний доступ до ресурсів може призвести до обмеженої пропускної здатності в певних місцях системи, якщо вона спроектована неправильно. Наприклад, за допомогою апаратних механізмів можна досягти ефективного проміжного доступу. Після отримання доступу до низькорівневого ресурсу, такого як пам'ять, апаратні механізми захисту можуть гарантувати, що доступ поза межами не відбудеться.

Пов'язані заходи: AC-25.

(6) БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - МІНІМІЗОВАНИЙ ОБМІН

Запровадити принцип проектування безпеки з мінімальним спільним використанням у [*Призначення: визначені організацією системи або компоненти системи*].

Рекомендації з реалізації: Принцип мінільного спільного використання стверджує, що жоден комп'ютерний ресурс не використовується спільно між системними компонентами (наприклад, суб'єктами, процесами, функціями), якщо це не є абсолютно необхідною умовою. Мінімальний спільний доступ допомагає спростити проектування та впровадження системи. Щоб захистити ресурси домену користувача від довільних активних об'єктів, жоден ресурс не надається спільно, якщо цей спільний доступ не було явно запитано та надано. Необхідність спільного використання ресурсів може бути мотивована принципом розробки найменш загального механізму у випадку внутрішніх організацій або керована вимогами зацікавлених сторін. Однак внутрішній спільний доступ має бути ретельно розроблений для уникнення проблем із продуктивністю, прихованим зберіганням і синхронізацією. Спільний доступ за допомогою загального механізму може збільшити вразливість даних та інформації для неавторизованого доступу, розголошення, використання або модифікації та може негативно вплинути на внутрішні можливості системи. Щоб звести до мінімуму обмін, викликаний загальними механізмами, такі механізми можуть бути спроектовані з повторним входом або віртуалізацією для збереження розділення. Крім того, ретельно перевіряється використання глобальних даних для обміну інформацією. Відсутність інкапсуляції може заплутати зв'язки між об'єктами спільного використання.

Пов'язані заходи: SC-31.

(7) БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - ЗНИЖЕНА СКЛАДНІСТЬ

Запровадити принцип проектування безпеки зі зниженою складністю в [*Призначення: визначені організацією системи або компоненти системи*].

Рекомендації з реалізації: Принцип зниженої складності стверджує, що дизайн системи є максимально простим і малим. Невеликий і простий дизайн є зрозумілим, краще піддається аналізу та менш схильний до помилок. Принцип зменшеної складності застосовується до будь-якого аспекту системи, але він має особливе значення для безпеки через різноманітні аналізи, які виконуються для отримання доказів щодо нових властивостей безпеки системи. Застосування принципу зниженої складності сприяє здатності розробників системи розуміти

правильність і повноту функцій безпеки системи. Це також полегшує ідентифікацію потенційних вразливостей. Простота системи безпосередньо пов'язана з кількістю вразливостей, які вона міститиме; тобто простіші системи містять менше вразливостей. Перевага від зменшення складності полягає в тому, що легше зрозуміти, чи запланована політика безпеки була зафіксована в проекті системи, і що менше вразливостей, ймовірно, буде включено під час інженерного проектування системи. Додатковою перевагою є те, що будь-який такий висновок щодо правильності, повноти та наявності вразливостей можна зробити з вищим ступенем упевненості на відміну від висновків, зроблених у ситуаціях, коли дизайн системи складний. Перехід від старих до новіших технологій (наприклад, перехід від IPv4 до IPv6) може потребувати впровадження старішої та новішої технологій одночасно протягом перехідного періоду, що призводить до тимчасового збільшення складності системи під час такого переходу.

Пов'язані заходи: Немає.

(8) БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - ЕВОЛЮЦІЯ БЕЗПЕКИ В СИСТЕМІ

Реалізація принципу еволюції безпеки в [*Призначення: визначені організацією системи або компоненти системи*].

Рекомендації з реалізації: Принцип еволюції безпеки стверджує, що система розроблена для сприяння підтримці її властивостей безпеки, коли відбуваються зміни в структурі системи, інтерфейсах, взаємозв'язках (тобто архітектурі системи), функціональності або конфігурації (тобто застосуванні політики безпеки). Зміни включають нову, розширену або оновлену системну здатність; діяльність з технічного обслуговування та підтримки; і реконфігурацію. Хоча неможливо спланувати кожен аспект еволюції системи, оновлення та зміни системи можна передбачити шляхом аналізу місії чи стратегічного напрямку бізнесу, очікуваних змін у середовищі загроз та очікуваних потреб в обслуговуванні та підтримці. Нереалістично очікувати, що складні системи залишатимуться безпечними у ситуаціях, не передбачених під час розробки, незалежно від того, пов'язані такі ситуації з робочим середовищем чи використанням. Система може бути безпечною в деяких нових ситуаціях, але немає гарантії, що її поведінка завжди буде безпечною. Легше вбудувати надійність у систему з самого початку, і з цього випливає, що підтримка надійності системи вимагає планування змін, а не адаптації у випадковий або неметодичний спосіб. Переваги цього принципу включають зниження витрат постачальника протягом життєвого циклу, зниження права власності, покращення безпеки системи, більш ефективне управління ризиками безпеки та меншу невизначеність ризику.

Пов'язані заходи: CM-3.

(9) БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - ДОВІРЕНІ КОМПОНЕНТИ СИСТЕМИ

Запровадити принцип проектування довірених компонентів у [*Призначення: системи, визначені організацією, або системні компоненти*].

Рекомендації з реалізації: Принцип довірених компонентів стверджує, що компонент заслуговує довіри принаймні до рівня, співмірного із залежностями безпеки, які він підтримує (тобто, наскільки йому довіряють виконувати свої

функції безпеки іншими компонентами). Цей принцип дозволяє створити таку композицію компонентів, щоб надійність не була випадково знижена, і довіра, як наслідок, не була втрачена. Зрештою, цей принцип вимагає певної метрики, за допомогою якої можна виміряти довіру до компонента та надійність компонента в одній абстрактній шкалі. Принцип довірених компонентів особливо актуальний при розгляді систем і компонентів, у яких існують складні ланцюги довірчих залежностей. Довірчу залежність також називають довірчими відносинами, і можуть існувати ланцюги довірчих відносин.
Принцип довірених компонентів також застосовується до складного компонента, який складається з підкомпонентів (наприклад, підсистеми), які можуть мати різні рівні надійності. Припущення полягає в тому, що надійність складеного компонента є надійністю його найменш надійного субкомпонента. Можна припустити, що надійність конкретного складеного компонента є вищою, ніж ми припускаємо. Однак будь-яке таке обґрунтування відображає логічне міркування, засноване на чіткому формулюванні цілей надійності, а також на відповідних і достовірних доказах. Надійність складного компонента – це не те саме, що посилене застосування поглибленого захисту всередині компонента або реплікація компонентів. Методи глибокого захисту не підвищують достовірність цілого вище ніж найменш надійний компонент.

Пов’язані заходи: Немає.

(10) БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - ІЄРАРХІЧНА ДОВІРА

Запровадити принцип ієрархічної довіри в системі [*Призначення: визначені організацією системи або компоненти системи*].

Рекомендації з реалізації: Принцип ієрархічної довіри для компонентів базується на принципі довірених компонентів і стверджує, що залежності безпеки в системі створюватимуть частковий порядок, якщо вони зберігають принцип довірених компонентів. Часткове впорядкування забезпечує основу для обґрунтування надійності або гарантійного випадку (аргумент гарантії) при створенні безпечної системи з неоднорідно надійних компонентів. Для аналізу надійності системи, що складається з неоднорідно надійних компонентів, важливо усунути циклічні залежності щодо надійності. Якби більш надійний компонент, розташований на нижчому рівні системи, залежав би від менш надійного компонента на вищому рівні, це фактично помістило б компоненти в той самий «менш надійний» клас еквівалентності відповідно до принципу надійних компонентів. Довірчі відносини, або ланцюги довіри, можуть мати різні прояви. Наприклад, кореневий сертифікат ієрархії сертифікатів є найбільш надійним вузлом в ієрархії, тоді як листи в ієрархії можуть бути найменш надійними вузлами. Іншим прикладом є багаторівнева система високого рівня надійності, де ядро безпеки (включаючи апаратну базу), розташоване на найнижчому рівні системи, є найбільш надійним компонентом. Однак принцип ієрархічної довіри не забороняє використання надто надійних компонентів. У системі з низьким рівнем надійності можуть бути випадки, коли доцільно використовувати високонадійний компонент, а не менш надійний (наприклад, через доступність або інший фактор співвідношення витрат і вигод). У такому випадку будь-яка залежність високонадійного компонента від менш надійного компонента не погіршує надійність отриманої системи з низьким рівнем довіри.

Пов’язані заходи: Немає.

(11) БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - ЗВОРОТНІЙ ПОРІГ МОДИФІКАЦІЇ

Запровадити принцип проектування безпеки зворотного порогу модифікації в [*Призначення: визначені організацією системи або компоненти системи*].

Рекомендації з реалізації: Принцип зворотного порогу модифікації базується на принципі довірених компонентів та принципі ієрархічної довіри та стверджує, що ступінь захисту, наданий компоненту, співрозмірний з його надійністю. У міру того, як довіра до компонента зростає, захист від неавторизованої модифікації компонента також зростає до такого ж ступеня. Захист від несанкціонованої модифікації може бути у формі власного самозахисту компонента та вродженої надійності, або він може походити від захисту, наданого компоненту іншими елементами чи атрибутами архітектури безпеки (щоб включити захист у робочому середовищі).

Пов'язані заходи: Немає.

(12) БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - ІЄРАРХІЧНИЙ ЗАХИСТ

Запровадити принцип ієрархічного захисту в [*Призначення: визначені організацією системи або системні компоненти*].

Рекомендації з реалізації: Принцип ієрархічного захисту стверджує, що компонент не потрібно захищати від більш надійних компонентів. У гіршому випадку найбільш надійний компонент захищає себе від усіх інших компонентів. Наприклад, якщо ядро операційної системи вважається найбільш надійним компонентом у системі, то воно захищає себе від усіх ненадійних програм, які підтримує, але програми, навпаки, не потребують захисту від ядра. Надійність користувачів теж розглядається при застосування принципу ієрархічного захисту. Довіреній системі не потрібно захищати себе від настільки ж надійного користувача, що відображає використання ненадійних систем у середовищах «високого рівня системи», де користувачі заслуговують високої довіри та де застосовуються інші засоби захисту для обмеження та захисту середовища виконання «високого рівня системи».

Пов'язані заходи: Немає.

(13) БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - МІНІМІЗОВАНІ ЕЛЕМЕНТИ БЕЗПЕКИ

Запровадити принцип проектування безпеки з мінімізованими елементами безпеки в [*Призначення: визначені організацією системи або компоненти системи*].

Рекомендації з реалізації: Принцип мінімізації елементів безпеки передбачає відсутність у системі сторонніх довірених компонентів. Принцип мінімізації елементів безпеки має два аспекти: загальну вартість аналізу безпеки та складність аналізу безпеки. Довірені компоненти, як правило, дорожчі для створення та впровадження через підвищену жорсткість процесів розробки. Надійні компоненти вимагають детальнішого аналізу безпеки для підтвердження їх надійності. Таким чином, щоб знизити вартість і зменшити складність аналізу безпеки, система містить якомога менше надійних

компонентів. Аналіз взаємодії довірених компонентів з іншими компонентами системи є одним із найважливіших аспектів перевірки безпеки системи. Якщо взаємодія між компонентами є надмірно складною, безпеку системи також буде важче перевірити, ніж у системі, внутрішні довірчі відносини якої прості та зрозуміло побудовані. Загалом менша кількість довірених компонентів призводить до меншої кількості внутрішніх довірчих відносин і спрощення системи.

Пов'язані заходи: Немає.

(14) БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - НАЙМЕНШІ ПРИВІЛЕЇ

Запровадити принцип мінімальних привілеїв проектування безпеки в [*Призначення: системи, визначені організацією, або системні компоненти*].

Рекомендації з реалізації: Принцип найменших привілеїв стверджує, що кожному компоненту системи надається достатня кількість привілеїв для виконання визначених ним функцій, але не більше. Застосування принципу найменших привілеїв обмежує сферу дій компонента, що має два позитивні ефекти: вплив на безпеку збою, пошкодження або неправильного використання компонента матиме мінімальний вплив на безпеку, а аналіз безпеки компонента буде спрощений. Найменший привілей — це поширений принцип, який відображається в усіх аспектах проектування безпеки системи. Інтерфейси, які використовуються для виклику можливостей компонентів, доступні лише для певних підмножин користувачів, а конструкція компонентів підтримує досить дрібну деталізацію привілеїв. Наприклад, у випадку механізму аудиту може бути інтерфейс для менеджера аудиту, який налаштовує параметри аудиту; інтерфейс для оператора аудиту, який забезпечує безпечний збір і зберігання даних аудиту; і, нарешті, ще один інтерфейс для перевіряючого аудитора, якому потрібно лише переглядати зібрані дані аудиту, але не потрібно виконувати операції з цими даними.
На додаток до своїх проявів на системному інтерфейсі, найменші привілеї можуть використовуватися як керівний принцип внутрішньої структури самої системи. Одним із аспектів внутрішніх найменших привілеїв є конструювання модулів таким чином, щоб лише елементи, інкапсульовані модулем, безпосередньо керувалися функціями в модулі. Зовнішні по відношенню до модуля елементи, на які може вплинути робота модуля, мають опосередкований доступ через взаємодію (наприклад, через виклик функції) з модулем, який містить ці елементи. Інший аспект мінімальних внутрішніх привілеїв полягає в тому, що область даного модуля або компонента включає лише ті системні елементи, які необхідні для його функціональності, і що режими доступу до елементів (наприклад, читання, запис) є мінімальними.

Пов'язані заходи: AC-6, CM-7.

(15) БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - ПРЕДИКАТНИЙ ДОЗВІЛ

Реалізація принципу безпеки предикатного дозволу в [*Призначення: визначені організацією системи або системні компоненти*].

Рекомендації з реалізації: Предикатний дозвіл розділенням привілеїв – це дозвіл від кількох уповноважених суб'єктів про надання згоди перед тим, як буде

дозволено продовжити надзвичайно важливу операцію або отримання доступу до конфіденційних даних, інформації чи ресурсів. Це також еквівалентно розподілу обов'язків. Розподіл привілеїв між декількома сторонами зменшує ймовірність зловживань і гарантує, що жоден нещасний випадок, обман чи зловживання довірою не є достатніми для здійснення невиправної дії, яка може призвести до значних збитків. Параметри конструкції для такого механізму можуть вимагати одночасних дій (наприклад, вистріл з ядерної зброї вимагає, щоб дві різні уповноважені особи віддали правильну команду протягом невеликого часового вікна) або послідовності операцій, де кожна послідовна дія забезпечується деякими попередніми, але жодна особа не може виконати більше однієї дії.

Пов'язані заходи: AC-5.

(16) БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - САМОСТІЙНА НАДІЙНІСТЬ

Впровадити принцип надійності в системі безпеки [*Призначення: визначені організацією системи або компоненти системи*].

Рекомендації з реалізації: Принцип самостійної надійності стверджує, що системи мінімізують свою залежність від інших систем щодо їх власної стійкості до корозії. Система за замовчуванням є надійною, і будь-яке з'єднання із зовнішнім об'єктом використовується для доповнення її функцій. Якщо системі необхідно підтримувати зв'язок із іншим зовнішнім об'єктом, щоб підтримувати свою надійність, тоді ця система буде вразливою до зловмисних і незловмисних загроз, які можуть призвести до втрати або погіршення цього з'єднання. Перевага принципу самостійної надійності полягає в тому, що ізоляція системи зробить її менш вразливою для атак. Наслідком цього принципу є здатність системи (або системного компонента) працювати ізольовано, а потім повторно синхронізуватися з іншими компонентами, коли знову потрібне з'єднання з ними.

Пов'язані заходи: Немає.

(17) БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - БЕЗПЕЧНО РОЗПОДІЛЕНА КОМПОЗИЦІЯ

Запровадити принцип безпечно розподіленої композиції в [*Призначення: визначені організацією системи або системні компоненти*].

Рекомендації з реалізації: Принцип безпечно розподіленої композиції стверджує, що композиція розподілених компонентів, які застосовують однакову політику безпеки системи, призводить до системи, яка забезпечує виконання цієї політики принаймні так само добре, як і окремі компоненти. Багато принципів проектування безпеки систем стосуються того, як компоненти можуть або повинні взаємодіяти. Необхідність створити або включити можливість із складу розподілених компонентів може збільшити релевантність цих принципів. Зокрема, переміщення політики безпеки з автономної на розподілену систему або систему системної інженерії може мати несподівані або миттєві результати. Комунікаційні протоколи та механізми узгодженості розподілених даних допомагають забезпечити узгоджене застосування політики в розподіленій системі. Щоб забезпечити загальносистемний рівень гарантії правильного застосування політики, архітектура безпеки розподіленої складеної системи ретельно аналізується.

Пов’язані заходи: Немає.

(18) БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - ДОВІРЕНІ КАНАЛИ КОМУНІКАЦІЇ

Проектування довірених каналів зв’язку в [*Призначення: визначені організацією системи або компоненти системи*].

Рекомендації з реалізації: Довірені канали зв’язку проектуються там, де існує потенційна загроза для зв’язку між компонентами (тобто взаємозв’язків між компонентами), кожен канал зв’язку є надійним до рівня, який відповідає залежностям безпеки, які він підтримує (тобто як інші компоненти довіряють йому виконувати свої функції безпеки). Довірені канали зв’язку досягаються шляхом поєднання обмеження доступу до каналу зв’язку (щоб забезпечити прийнятну відповідність надійності кінцевих точок, залучених у зв’язок) і застосування наскрізного захисту для даних, що передаються через канал зв’язку (для захисту від перехоплення та модифікації та ще більше підвищити гарантію належного наскрізного зв’язку).

Пов’язані заходи: SC-8, SC-12, SC-13.

(19) БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - ПОСТІЙНИЙ ЗАХИСТ

Запровадити принцип безперервного захисту в [*Призначення: визначені організацією системи або компоненти системи*].

Рекомендації з реалізації: Принцип постійного захисту стверджує, що компоненти та дані, які використовуються для забезпечення виконання політики безпеки, мають безперервний захист, який узгоджується з політикою безпеки та архітектурою безпеки. Жодних гарантій того, що система може забезпечити захист конфіденційності, цілісності, доступності та конфіденційності для своїх проектних можливостей, неможливо зробити, якщо є прогалини в захисті. Такі гарантії щодо здатності забезпечити надані можливості вимагають постійного захисту даних та інформації. Тобто не може бути періодів, протягом яких дані та інформація залишаються незахищеними під час керування системою (тобто під час створення, зберігання, обробки чи передачі даних та інформації, а також під час ініціалізації, виконання, збою системи, переривання та вимкнення). Безперервний захист вимагає дотримання принципів концепції еталонного монітора (тобто кожен запит перевіряється еталонним монітором; еталонний монітор здатний захистити себе від несанкціонованого втручання; і достатню впевненість у правильності та повноті механізму можна отримати за допомогою аналізу та тестування) та принципу безпечного збою та відновлення (тобто збереження безпечного стану під час помилки, несправності, відмови та успішної атаки; збереження безпечного стану під час відновлення до нормального, погіршеного або альтернативного режиму роботи).

Безперервний захист також поширюється на системи, призначені для роботи в різних конфігураціях, включаючи ті, які забезпечують повну робочу здатність, і конфігурації в погіршеному режимі, які забезпечують часткову робочу здатність. Принцип безперервного захисту вимагає, щоб зміни в політиках безпеки системи можна було простежити до операційної потреби, яка керує конфігурацією, і щоб їх можна було перевірити (тобто можна перевірити, що запропоновані зміни не переведуть систему в небезпечний стан). Недостатня відстежуваність і перевірка можуть призвести до непослідовних станів або

розривів захисту через складні проблеми, які не можна виправити. Використання попередньо перевірених визначень конфігурації, які відображають нову політику безпеки, дає змогу аналізу визначити, що перехід від старої політики до нової є по суті атомарним і що будь-які залишкові ефекти від старої політики гарантовано не суперечать новій політиці. Здатність демонструвати постійний захист ґрунтується на чіткому формулюванні потреб у захисті життєвого циклу як вимог безпеки зацікавлених сторін.

Пов’язані заходи: AC-25.

(20) БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - БЕЗПЕЧНЕ КЕРУВАННЯ МЕТАДАНИМИ

Запровадити принцип безпечного керування метаданими в [*Призначення: визначені організацією системи або компоненти системи*].

Рекомендації з реалізації: Принцип безпечного керування метаданими стверджує, що метадані є об’єктами «першого класу» для політики безпеки, коли політика вимагає повного захисту інформації або самозахисту підсистеми безпеки. Принцип безпечного керування метаданими ґрунтується на визнанні того, що система, підсистема чи компонент не можуть досягти самозахисту, якщо вони не захищають дані, на які вони покладаються для правильного виконання. Дані зазвичай не інтерпретуються системою, яка їх зберігає. Вони можуть мати семантичне значення (тобто містити інформацію) для користувачів і програм, які обробляють дані. І навпаки, метадані — це інформація про дані, наприклад ім’я файлу або дата створення файлу. Метадані прив’язані до цільових даних, які вони описують у спосіб, який система може інтерпретувати, але їх не потрібно зберігати всередині цільових даних або близько до них. Можуть існувати метадані, метою яких є самі метадані (наприклад, рівень класифікації або рівень впливу назви файлу), включаючи метадані з самопосиланням.
Очевидна вторинність метаданих може призвести до нехтування їх законною потребою в захисті, що призведе до порушення політики безпеки, включаючи викрадання інформації. Особливе важливо звернути увагу на захист метаданих, пов’язаних з системами багаторівневої безпеки (MLS). Системи MLS забезпечують доступ суб'єкта до об'єкта на основі відносних рівнів чутливості. Звідси випливає, що всі суб’єкти та об’єкти, що знаходяться в зоні контролю системи MLS, або прямо позначені, або опосередковано приписуються рівнями чутливості. Наслідком мічених метаданих для систем MLS є те, що об’єкти, що містять метадані, маркуються. Як і під час оцінювання потреб захисту даних, увага приділяється тому, щоб захист конфіденційності та цілісності оцінювався окремо, уточнювався та розподілявся для метаданих, як це було б зроблено для даних місії, бізнесу та системи.

Пов’язані заходи: Немає.

(21) БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - САМОАНАЛІЗ

Запровадити принцип самоаналізу безпеки в [*Завдання: визначені організацією системи або компоненти системи*].

Рекомендації з реалізації: Принцип самоаналізу стверджує, що компонент системи здатний оцінювати свій внутрішній стан і функціональність в обмеженій мірі на різних етапах виконання, і що ця здатність до самоаналізу є

пропорційною рівню надійності, закладеному в систему. На системному рівні самоаналіз може бути досягнутий за допомогою ієрархічних оцінок надійності, створених за принципом «знизу вгору». У цьому підході компоненти нижчого рівня перевіряють цілісність даних і правильну функціональність (в обмеженій мірі) компонентів вищого рівня. Наприклад, довірені послідовності завантаження включають довірений компонент нижчого рівня, який засвідчує надійність наступних компонентів вищого рівня, щоб можна було встановити перехідний ланцюг довіри. У корені компонент засвідчує сам себе, що зазвичай передбачає аксіоматичне або нав'язане середовищем припущення щодо його цілісності. Результати самоаналізу можна використовувати для захисту від зовнішніх помилок, внутрішньої несправності або тимчасових помилок. Дотримуючись цього принципу, деякі прості несправності або помилки можна виявити, не дозволяючи наслідкам помилки або несправності поширюватися за межі компонента. Крім того, самопаналіз можна використовувати для підтвердження конфігурації компонента, виявлення будь-яких потенційних конфліктів у цій конфігурації.

Пов'язані заходи: CA-7.

(22) БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - ЗВІТНІСТЬ І ВІДСТЕЖУВАНІСТЬ

Запровадження принципу звітності та відстеження безпеки в [*Призначення: визначені організацією системи або компоненти системи*].

Рекомендації з реалізації: Принцип звітності та відстежуваності стверджує, що можна відстежити дії, пов'язані з безпекою (тобто, суб'єктно-об'єктні взаємодії) до суб'єкта, від імені якого виконуються дії. Принцип звітності та відстеження вимагає надійної інфраструктури, яка може записувати деталі про дії, що впливають на безпеку системи (наприклад, підсистема аудиту). Щоб записати деталі про дії, система здатна однозначно ідентифікувати суб'єкт, від імені якого виконується дія, а також записати відповідну послідовність дій, які виконуються. Політика звітності також вимагає, щоб сам контрольний журнал був захищений від несанкціонованого доступу та модифікації. Принцип найменших привілеїв допомагає відстежувати дії до конкретних суб'єктів, оскільки він збільшує деталізацію звітності. Пов'язування певних дій із системними об'єктами та, зрештою, користувачами, а також захист контрольного журналу від несанкціонованого доступу та модифікацій забезпечує неспростовність, оскільки після запису дії неможливо змінити контрольний слід. Інша важлива функція, яку виконує звітність і відстеження, полягає в рутинному та криміналістичному аналізі подій, пов'язаних із порушенням політики безпеки. Аналіз журналів аудиту може надати додаткову інформацію, корисну для визначення шляху або компонента, який дозволив порушити політику безпеки, і дії осіб, пов'язані з порушенням політики безпеки.

Пов'язані заходи: AC-6, AU-2, AU-3, AU-6, AU-9, AU-10, AU-12, IA-2, IR-4.

(23) БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - БЕЗПЕЧНІ ПАРАМЕТРИ ЗА ЗАМОВЧУВАННЯМ

Реалізація принципу безпеки за замовчуванням у [*Призначення: визначені організацією системи або компоненти системи*].

Рекомендації з реалізації: Принцип безпечних параметрів за замовчуванням

стверджує, що стандартна конфігурація системи (включаючи її складові підсистеми, компоненти та механізми) відображає обмежувальне та консервативне застосування політики безпеки. Принцип безпечних параметрів за замовчуванням застосовується до початкової (тобто типової) конфігурації системи, а також до проектування безпеки та контролю доступу та інших функцій безпеки, які дотримуються стратегії «заборонити, якщо не авторизовано явно». Аспект початкової конфігурації цього принципу вимагає, щоб будь-яка конфігурація системи, підсистеми або системного компонента «як постачалася» не сприяла порушенню політики безпеки та не могла перешкоджати роботі системи в конфігурації за замовчуванням у тих випадках, коли сама політика безпеки вимагає налаштування користувача.

Обмежувальні параметри за замовчуванням означають, що система працюватиме «як при постачанні» з відповідним самозахистом і матиме змогу запобігти порушенням безпеки до встановлення запланованої політики безпеки та конфігурації системи. У випадках, коли захист, який забезпечується продуктом «як доставлено», є неадекватним, зацікавлені сторони оцінюють ризик його використання до встановлення безпечного початкового стану. Дотримання принципу безпеки за замовчуванням гарантує, що система буде встановлена в безпечному стані після успішного завершення ініціалізації. У ситуаціях, коли системі не вдається завершити ініціалізацію, вона або виконає необхідну операцію, використовуючи безпечні параметри за замовчуванням, або не виконає операцію. Зверніться до принципів безперервного захисту, безпечної відмови та відновлення, які паралельні цьому принципу, щоб забезпечити можливість виявлення та відновлення після відмови.

Інженерний підхід до безпеки цього принципу стверджує, що механізми безпеки відхиляють запити, якщо запит не визнано правильно сформованим і сумісним з політикою безпеки. Небезпечна альтернатива — дозволити запит, якщо не буде показано, що він не відповідає політиці. У великій системі умови, які задовольняються для надання запиту, який відхилено за замовчуванням, часто набагато компактніші та повніші, ніж ті, які потрібно було б перевірити, щоб відхилити запит, який надається за замовчуванням.

Пов’язані заходи: CM-2, CM-6, SA-4.

(24) БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - ЗБОЇ БЕЗПЕКИ І ВІДНОВЛЕННЯ

Реалізуйте принцип проектування безпечного збою та відновлення в [*Призначення: визначені організацією системи або компоненти системи*].

Рекомендації з реалізації: Принцип безпечного збою та відновлення полягає у тому, що збій системної функції чи механізму, чи будь-яка дія відновлення у відповідь на збій не призведе до порушення політики безпеки. Принцип безпечного збою та відновлення паралельний принципу безперервного захисту для гарантування, що система здатна виявляти (в певних межах) фактичну та загрозливу несправність на будь-якому етапі її роботи (тобто ініціалізація, нормальна робота, завершення роботи та технічне обслуговування) та вживати відповідних заходів, для гарантування збереження політики безпеки. Крім того, якщо система спроектована так, що здатна відновлюватися після загроз або збоїв для відновлення звичайних, знижених або альтернативних безпечних операцій та забезпечує підтримання безпечного стану без порушень політики безпеки.

Збій – це стан, за якого поведінка компонента відхиляється від заданої або очікуваної поведінки для явно задокументованого вхідного сигналу. Після виявлення збою функції безпеки, система може змінити налаштування так, щоб

обійти несправний компонент, зберігаючи безпеку та забезпечуючи всі або частину функціональних можливостей вихідної системи чи повністю вимкнутися для запобігання порушенням політики безпеки. Для цього, функції реконфігурації системи розробляються для забезпечення безперервного виконання політики безпеки на різних етапах функціонування.

Інший метод, який можна використати для відновлення після збоїв, полягає у виконанні відкату до безпечного стану (який може бути початковим станом), а потім або завершення роботи, або заміни служби чи компонента, які вийшли з ладу, для відновлення безпечних операцій. Відмова компонента може бути виявлена або не виявлена компонентами, які його використовують. Принцип безпечного збою вказує на те, що компоненти виходять з ладу в стані, який забороняє, а не надає доступ. Наприклад, номінально «атомарна» операція, перервана до завершення, не порушує політику безпеки та призначена для обробки подій переривання за допомогою використання атомарності вищого рівня та механізмів відкату (наприклад, транзакцій). Якщо послуга використовується, її властивості атомарності добре задокументовані та охарактеризовані, щоб компонент, який користується цією послугою, міг належним чином виявляти та обробляти події переривання. Наприклад, система розроблена так, щоб реагувати на відключення та підтримувати повторну синхронізацію та узгодженість даних після відключення.

Стратегії захисту від збоїв, які використовують реплікацію механізмів застосування політики (глибокий захист), можуть дозволити системі продовжувати працювати в безпечному стані, навіть якщо один механізм не зміг захистити систему. Проте, якщо механізми подібні, додатковий захист може бути ілюзорним, оскільки супротивник може просто атакувати серією. Таким чином у мережевій системі порушення безпеки в одній системі чи службі може дозволити зловмиснику зробити те ж саме в інших подібних реплікованих системах і службах. Застосовуючи кілька механізмів захисту, характеристики яких значно відрізняються, можна зменшити ймовірність копіювання чи повторення атак. Проводять аналіз для розуміння витрат та переваг таких методів резервування напротивагу збільшення використання ресурсів і негативного впливу на загальну продуктивність системи. Додатковий аналіз проводять, коли складність цих механізмів зростає, як у випадку динамічної поведінки. Підвищена складність зазвичай знижує надійність. Якщо ресурс неможливо постійно захищати, дуже важливо виявити та усунути будь-які порушення безпеки, перш ніж ресурс знову буде використаний у безпечному контексті.

Пов’язані заходи: CP-10, CP-12, SC-7, SC-8, SC-24, SI-13.

(25) БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - ЕКОНОМІЧНА БЕЗПЕКА

Впровадити принцип проектування економічної безпеки в [*Завдання: визначені організацією системи або компоненти системи*].

Рекомендації з реалізації: Принцип економічної безпеки стверджує, що механізми безпеки не коштують дорожче, ніж потенційна шкода, яка може виникнути внаслідок порушення безпеки. Це важлива для безпеки форма аналізу витрат і вигод, яка використовується в управлінні ризиками. Припущення щодо вартості аналізу витрат і вигод заважають розробнику системи включати механізми безпеки більшої міцності, ніж необхідно, де міцність механізму пропорційна вартості. Принцип економічної безпеки також вимагає аналізу переваг гарантій відносно вартості такої гарантії з точки зору зусиль, витрачених на отримання

відповідних і достовірних доказів, а також необхідного аналізу для оцінки та отримання висновків щодо надійності та ризику на основі доказів.

Пов'язані заходи: RA-3.

(26) БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - БЕЗПЕКА ПРОДУКТИВНОСТІ

Запровадити принцип безпеки продуктивності в [*Призначення: визначені організацією системи або компоненти системи*].

Рекомендації з реалізації: Принцип безпеки продуктивності стверджує, що механізми безпеки побудовані таким чином, щоб вони не погіршували продуктивність системи без потреби. Вимоги зацікавлених сторін і проектування продуктивності та безпеки в системі точно сформульовані та визначені пріоритетними. Щоб реалізація системи відповідала вимогам проектування та була визнана прийнятною для зацікавлених сторін (тобто перевірка на відповідність вимогам зацікавлених сторін), розробники дотримуються визначених обмежень, у тому, що можливості продуктивності потребують певних можливостей захисту. Загальний вплив служб безпеки, що потребують інтенсивних обчислень (наприклад, криптографії), оцінено та продемонстровано, що вони не мають значного впливу на питання продуктивності з вищим пріоритетом або вважаються такими, що забезпечують прийнятний компроміс продуктивності для надійного захисту. Компенсаційні механізми включають служби безпеки, які вимагають менше обчислювальних потужностей, якщо вони недоступні або недостатні. Недостатність служби безпеки визначається функціональними можливостями та міцністю механізму. Міцність механізму вибирається з огляду на вимоги безпеки та критичні для продуктивності накладні витрати (наприклад, керування криптографічним ключем) і оцінку можливостей загрози.

Принцип безпеки продуктивності веде до включення функцій, які допомагають у застосуванні політики безпеки, але спричиняють мінімальні накладні витрати, наприклад апаратні механізми низького рівня, на основі яких можна створювати служби вищого рівня. Такі низькорівневі механізми зазвичай дуже специфічні, мають дуже обмежену функціональність і оптимізовані для продуктивності. Наприклад, коли права доступу до частини пам'яті надано, багато систем використовують апаратні механізми, щоб гарантувати, що подальший доступ включатиме правильну адресу пам'яті та буде здійснений у правильний спосіб. Застосування цього принципу підсилює необхідність проектування в системі безпеки з нуля та включення простих механізмів на нижніх рівнях, які можна використовувати як будівельні блоки для механізмів вищого рівня.

Пов'язані заходи: SC-12, SC-13, SI-2, SI-7.

(27) БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - ЛЮДСЬКИЙ ФАКТОР БЕЗПЕКИ

Запровадити принцип безпеки людського фактору в [*Завдання: визначені організацією системи або компоненти системи*].

Рекомендації з реалізації: Принцип безпеки, заснованої на людському факторі, передбачає, що інтерфейс користувача для функцій безпеки та допоміжних служб є інтуїтивно зрозумілим, зручним і забезпечує зворотній зв'язок щодо дій

користувача, які впливають на таку політику та її застосування. Механізми, які забезпечують дотримання політики безпеки, не є нав'язливими для користувача та розроблені таким чином, щоб не знижувати його ефективність. Механізми застосування політики безпеки також надають користувачеві значущий, чіткий і відповідний відгук і попередження, коли приймаються небезпечні рішення. Особлива увага приділяється інтерфейсам, за допомогою яких персонал, відповідальний за адміністрування та роботу системи, налаштовує конфігурацію та політики безпеки. В ідеалі такий персонал здатний зрозуміти вплив свого вибору. Персонал із системними адміністративними та експлуатаційними обов'язками може налаштовувати системи перед запуском і адмініструвати їх під час роботи з упевненістю, що їхні наміри правильно зіставлені з механізмами системи. Служби безпеки, функції та механізми не перешкоджають і не ускладнюють використання системи за призначенням. Існує компроміс між зручністю використання системи та суворістю, необхідною для виконання політики безпеки. Якщо механізми безпеки незручні або складні у використанні, користувачі можуть вимикати їх, уникати їх використання, або використовувати способами, несумісними з вимогами безпеки та потребами захисту, для задоволення яких їх було розроблено.

Пов'язані заходи: Немає.

(28) БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - ПРИЙНЯТНА БЕЗПЕКА

Реалізуйте принцип проектування прийнятної безпеки в [*Призначення: визначені організацією системи або компоненти системи*].

Рекомендації з реалізації: Принцип прийнятної безпеки вимагає, щоб рівень конфіденційності та продуктивності, які забезпечує система, відповідали очікуванням користувачів. Сприйняття особистої конфіденційності може вплинути на поведінку, мораль і ефективність користувачів. Виходячи з організаційної політики конфіденційності та дизайну системи, користувачі повинні мати можливість обмежити свої дії, щоб захистити свою конфіденційність. Якщо система не забезпечує інтуїтивно зрозумілий інтерфейс або не відповідає очікуванням щодо конфіденційності та продуктивності, користувачі можуть повністю уникати систему, або використовувати її у спосіб, який може бути неефективним або навіть небезпечним.

Пов'язані заходи: Немає.

(29) БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - ПОВТОРЮВАНІ І ДОКУМЕНТОВАНІ ПРОЦЕДУРИ

Запровадити принцип повторюваних і документованих процедур у [*Призначення: визначені організацією системи або системні компоненти*].

Рекомендації з реалізації: Принцип повторюваних і документованих процедур стверджує, що техніки і методи, які використовуються для створення компонента системи, дозволяють пізніше повністю і правильно реконструювати той самий компонент. Повторювані та документовані процедури підтримують розробку компонента, ідентичного компоненту, створеному раніше, який широко використовується. У випадку інших артефактів системи (наприклад, документації та результатів тестування) повторюваність підтримує послідовність і можливість перевірки артефактів. Повторювані та документовані процедури можуть бути

запроваджені на різних етапах життєвого циклу розробки системи та сприяють здатності оцінювати вимоги гарантії для системи. Приклади включають систематичні процедури для розробки та перегляду коду, процедури для управління конфігурацією засобів розробки та артефактів системи, а також процедури для доставки системи.

Пов'язані заходи: CM-1, SA-1, SA-10, SA-11, SA-15, SA-17, SC-1, SI-1.

(30) БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - ПРОЦЕСУАЛЬНА СТРОГІСТЬ

Запровадити принцип процедурної строгості в [*Призначення: визначені організацією системи або системні компоненти*].

Рекомендації з реалізації: Принцип процедурної строгості стверджує, що строгість процесу життєвого циклу системи співмірна з його передбачуваною надійністю. Строгість процедур визначає обсяг, глибину та деталізацію процедур життєвого циклу системи. Суворі процедури життєвого циклу системи дають впевненість в тому, що система працює коректно та не містить функцій, що можуть працювати декількома способами. По-перше, процедури накладають стримування та противаги на процес життєвого циклу, щоб запобігти впровадженню невизначеної функціональності, по-друге – суворі процедури, що застосовуються під час розробки системи безпеки та подальших специфікацій і проектних документів, дають розуміння реальної побудови системи, замість того, щоб вірити, що реалізований компонент є авторитетним (що потенційно оманливо).

Нарешті, модифікувати існуючий компонент системи легше, якщо є детальні специфікації, які описують його поточний дизайн, замість того, щоб вивчати вихідний код або схеми, щоб спробувати зрозуміти, як він працює. Суворість процедур допомагає гарантувати, що функціональні вимоги безпеки та гарантії були задоволені, і це сприяє створенню більш обґрунтованої основи для визначення надійності та ризику. Суворість процедури повинна відповідати бажаному ступеню впевненості для системи. Якщо необхідна надійність системи низька, високий рівень процедурної жорсткості може додати непотрібних витрат, тоді як висока надійність є критичною і вартість високої процедурної строгості в такому випадку є обгрунтованою.

Пов'язані заходи: Немає.

(31) БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - БЕЗПЕЧНА МОДИФІКАЦІЯ СИСТЕМИ

Реалізація принципу безпечної модифікації системи в [*Призначення: визначені організацією системи або компоненти системи*].

Рекомендації з реалізації: Принцип безпечної модифікації системи стверджує, що модифікація системи підтримує безпеку системи з огляду на вимоги безпеки та толерантність до ризику зацікавлених сторін. Оновлення або модифікації системи можуть перетворити безпечну систему на незахищену. Процедури модифікації системи гарантують, що якщо система має підтримувати свою надійність, до будь-яких змін в системі застосовується така ж суворість, як під час її початкової розробки. Оскільки модифікації можуть вплинути на здатність системи підтримувати свій безпечний стан, необхідний ретельний аналіз безпеки модифікації перед її впровадженням і розгортанням. Цей принцип є

паралельним принципу безпечної еволюції.

Пов'язані заходи: CM-3, CM-4.

(32) БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - ДОСТАТНЄ ДОКУМЕНТУВАННЯ

Запровадити принцип достатнього документування в [*Призначення: визначені організацією системи або компоненти системи*].

Рекомендації з реалізації: Принцип достатнього документування стверджує, що персонал організації, відповідальний за взаємодію з системою, забезпечений відповідною документацією та іншою інформацією для підтримки правильного функціонування безпеки системи. Незважаючи на спроби дотримуватися таких принципів, як безпека з урахуванням людського фактору та прийнятна безпека, системи за своєю суттю є складними, а задум використання механізмів безпеки та наслідки неправильного використання або неправильної конфігурації механізмів безпеки не завжди інтуїтивно очевидні. Необізнані та недостатньо навчені користувачі можуть створити вразливі місця через помилки недогляду та вчинення неумисних дій. Наявність документації та навчання допомагає забезпечити обізнаність персоналу, який відіграє вирішальну роль у досягненні таких принципів, як постійний захист. Документація має бути написана чітко та підтримуватися навчанням, яке забезпечує обізнаність із безпекою та розуміння пов'язаних із безпекою обов'язків.

Пов'язані заходи: AT-2, AT-3, SA-5.

(33) БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - МІНІМІЗАЦІЯ

Запровадити принцип мінімізації конфіденційності за допомогою [*Призначення: процеси, визначені організацією*].

Рекомендації з реалізації: Принцип мінімізації стверджує, що організації повинні обробляти лише таку персональну інформацію, яка має безпосереднє відношення та необхідна для досягнення авторизованої мети, і зберігати її лише до тих пір, доки це необхідно для досягнення мети. В організаціях мають діяти процеси, що відповідають чинному законодавству та політикам, для впровадження принципу мінімізації.

Пов'язані заходи: PE-8, PM-25, SC-42, SI-12.

Посилання: [PRIVACT], [OMB A-130], [FIPS 199], [FIPS 200], [SP 800-37], [SP 800-53A], [SP 800-60-1], [SP 800-60-2], [SP 800-160-1], [IR 8062].

## SA-9 ЗОВНІШНІ ПОСЛУГИ ДЛЯ СИСТЕМИ

Заходи захисту:

a. Вимагати, щоб постачальники зовнішніх послуг для системи відповідали вимогам безпеки та приватності в організації та застосовували такі заходи захисту [*Призначення: встановлені організацією заходи безпеки та приватності*].

b. Визначити та задокументувати нагляд організаціїповноваження та обов'язки користувачів щодо зовнішніх послуг для системи.

c. Використовувати наступні процеси, методи та техніки для постійного моніторингу дотримання контролю зовнішніми постачальниками послуг: [*Призначення: визначені організацією процеси, методи та техніки*].

Рекомендації з реалізації: Зовнішні сервіси — це ті сервіси, які реалізуються поза межами системи і надаються зовнішнім постачальником, де організація не має прямого контролю за впровадженням необхідних заходів захисту або оцінкою ефективності впроваджених заходів. Організації можуть встановлювати відносини із зовнішніми постачальниками послуг різними способами (ділове партнерство, контракти, міжвідомчі угоди, ліцензійні угоди, спільні підприємства та обміни ланцюгами постачання). Відповідальність за управління ризиками щодо використання зовнішніх послуг для системи залишається на уповноважених посадових особах. Для зовнішніх по відношенню до організацій послуг ланцюжок довіри вимагає, щоб організації встановили та зберігали певний рівень впевненості в тому, що кожен постачальник у відносинах «споживач-постачальник» забезпечує адекватний захист послуг, що надаються. Ступінь і характер цього ланцюга довіри змінюються залежно від відносин між організаціями та зовнішніми постачальниками. Організації документують основу для довірчих відносин для їх контролю. Документація зовнішніх послуг для системи включає державні органи, постачальників послуг, ролі та обов'язки безпеки кінцевих користувачів, а також угоди про рівень обслуговування. Угоди про рівень обслуговування визначають очікувані показники ефективності запроваджених заходів захисту, описують вимірні результати та визначають засоби правового захисту та вимоги до реагування на виявлені випадки невідповідності

Пов'язані заходи: AC-20, CA-3, CP-2, IR-4, IR-7, PL-10, PL-11, PS-7, SA-2, SA-4, SR-3, SR-5.

Посилення заходів:

(1) ЗОВНІШНІ ПОСЛУГИ ДЛЯ СИСТЕМИ- ОЦІНЮВАННЯ РИЗИКІВ ТА ОРГАНІЗАЦІЙНІ ПОГОДЖЕННЯ

(a) Проводити організаційне оцінювання ризиків перед придбанням або переданням послуг інформаційної безпеки служб інформаційної безпеки.

(b) Переконатися, що придбання або передача спеціалізованих служб інформаційної безпеки погоджені [*Призначення: визначеним організацією персоналом або посадовими особами*].

Рекомендації з реалізації: Послуги інформаційної безпеки включають роботу пристроїв безпеки, таких як брандмауери або служби керування ключами, а також моніторинг інцидентів, аналіз і реагування. Ризики, які оцінюються, можуть включати ризики системи, місії чи бізнесу, безпеки, конфіденційності чи ланцюга постачання.

Пов'язані заходи: CA-6, RA-3, RA-8.

(2) ЗОВНІШНІ ПОСЛУГИ ДЛЯ СИСТЕМИ- ВИЗНАЧЕННЯ ФУНКЦІЙ, ПОРТІВ, ПРОТОКОЛІВ ТА СЛУЖБ

Вимагати від постачальників наведених нижче зовнішніх послуг для системи [*Призначення: визначених організацією зовнішніх* послуг для системи] визначити функції, порти, протоколи та інші служби, необхідні для використання таких служб.

Рекомендації з реалізації: Інформація від зовнішніх постачальників послуг щодо конкретних функцій, портів, протоколів та служб, що використовуються при наданні таких послуг, може бути корисною, коли виникає потреба зрозуміти компроміси, пов'язані з обмеженням певних функцій та послуг або блокуванням певних портів та протоколів.

Пов'язані заходи: CM-6, CM-7.

(3) ЗОВНІШНІ ПОСЛУГИ ДЛЯ СИСТЕМИ - СТВОРЕННЯ ТА ПІДТРИМКА ДОВІРЧИХ ВІДНОСИН З ПОСТАЧАЛЬНИКАМИ

Створити, задокументувати та підтримувати довірчі відносини із зовнішніми постачальниками послуг на основі таких вимог, властивостей, факторів або умов: [*Призначення: визначених організацією вимог, властивостей, факторів або умов щодо безпеки та приватності, що визначають прийнятні довірчі відносини*].

Рекомендації з реалізації: Довірчі відносини між організаціями та зовнішніми постачальниками послуг відображають ступінь впевненості в тому, що ризик від використання зовнішніх послуг знаходиться на прийнятному рівні. Довірчі стосунки можуть допомогти організаціям отримати підвищений рівень впевненості в тому, що постачальники послуг забезпечують адекватний захист послуг, що надаються, а також можуть бути корисними під час реагування на інциденти або під час планування оновлень. Довірчі відносини можуть бути складними через потенційно велику кількість суб'єктів, які беруть участь у взаємодії між споживачем і постачальником, підпорядковані відносини та рівні довіри, а також типи взаємодії між сторонами. У деяких випадках ступінь довіри ґрунтується на рівні контролю, який організації можуть здійснювати над зовнішніми постачальниками послуг щодо заходів захисту, необхідних для захисту послуги, інформації чи приватності особи. Рівень контролю встановлюється умовами контрактів або угод про рівень обслуговування

Пов'язані заходи: SR-2.

(4) ЗОВНІШНІ ПОСЛУГИ ДЛЯ СИСТЕМИ- УЗГОДЖЕННЯ ІНТЕРЕСІВ СПОЖИВАЧІВ І ПОСТАЧАЛЬНИКІВ

Виконайте такі дії, щоб переконатися, що інтереси [*Призначення: визначених організацією зовнішніх постачальників послуг*] узгоджуються з інтересами організації та відображають їх: [*Призначення: дії, визначені організацією*].

Рекомендації з реалізації: Якщо інтереси постачальників послуг відрізняються від інтересів організації, то наявність необхідних технічних, управлінських або операційних заходів захисту може бути недостатнім, якщо такі постачальники, які впроваджують і керують цими заходами захисту, не працюють у спосіб, що відповідає інтересам організацій-споживачів. Заходи, які вживають організації для вирішення таких проблем, включають вимоги перевірки даних для обраного персоналу постачальника послуг; перевірки прав власності; використання лише надійних постачальників послуг, таких як постачальники, з якими організації мали успішні довірчі відносини; а також проведення регулярних, періодичних, позапланових відвідувань об'єктів постачальника послуг.

Пов'язані заходи: Немає.

(5) ЗОВНІШНІ ПОСЛУГИ ДЛЯ СИСТЕМИ- МІСЦЕ ОБРОБКИ, ЗБЕРІГАННЯ ТА ОБСЛУГОВУВАННЯ

Обмежити розташування [*Вибір (один або більше): обробка інформації; інформація або дані; системні служби*] до [*Призначення: визначені організацією місця*] на основі [*Призначення: визначених організацією вимог або умов*].

Рекомендації з реалізації: Місце обробки інформації, зберігання інформації та даних або послуг для системи може мати прямий вплив на здатність організацій успішно виконувати свою місію та бізнес-функції. Вплив виникає, коли зовнішні постачальники контролюють розташування обробки, зберігання чи послуг. Критерії, які використовують зовнішні постачальники для вибору місць обробки, зберігання чи обслуговування, можуть відрізнятися від критеріїв, які використовують організації. Наприклад, організації можуть забажати, щоб місця зберігання даних або інформації були обмежені певними місцями, щоб допомогти полегшити заходи реагування на інциденти у випадку інцидентів або порушень інформаційної безпеки. Діяльність реагування на інциденти, включаючи судово-медичний аналіз і постфактумне розслідування, може бути піддано негативному впливу регулюючих законів, політик або протоколів у місцях обробки та зберігання та/або місцях, з яких надходять системні служби.

Пов'язані заходи: SA-5, SR-4.

(6) ЗОВНІШНІ ПОСЛУГИ ДЛЯ СИСТЕМИ- КРИПТОГРАФІЧНІ КЛЮЧІ, КЕРОВАНІ ОРГАНІЗАЦІЄЮ

Зберігати контроль над криптографічними ключами для зашифрованої інформації, яка зберігається або передається через зовнішню систему.

Рекомендації з реалізації: Збереження контролю над криптографічними ключами у зовнішній системі запобігає дешифруванню даних організації персоналом зовнішньої системи. Контроль організації криптографічних ключів може бути реалізований шляхом шифрування та дешифрування даних всередині організації, коли дані надсилаються до зовнішньої системи та отримуються від неї, або шляхом використання компонента, який дозволяє функціям шифрування та дешифрування бути локальними для зовнішньої системи, але дозволяє ексклюзивний доступ до ключів шифрування організації.

Пов'язані заходи: SC-12, SC-13, SI-4.

(7) ЗОВНІШНІ ПОСЛУГИ ДЛЯ СИСТЕМИ- ПЕРЕВІРКА ЦІЛІСНОСТІ, ЩО КОНТРОЛЮЄТЬСЯ ОРГАНІЗАЦІЄЮ

Забезпечити можливість перевірки цілісності інформації в організації під час її перебування в зовнішній системі.

Рекомендації з реалізації: Зберігання інформації організації у зовнішній системі може обмежити видимість стану безпеки її даних. Здатність організації перевіряти та підтверджувати цілісність збережених даних без передачі їх із зовнішньої системи забезпечує таку видимість.

Пов'язані заходи: SI-7.

(8) ЗОВНІШНІ ПОСЛУГИ ДЛЯ СИСТЕМИ- МІСЦЕ ОБРОБКИ ТА ЗБЕРІГАННЯ – ЮРИСДИКЦІЯ УКРАЇНИ

Обмежити географічне розміщення обробки та зберігання даних об’єктами, розташованими в межах юридичної юрисдикції України.

Рекомендації з реалізації: Географічне розташування обробки та зберігання даних може мати прямий вплив на здатність організацій успішно виконувати свою місію та бізнес-функції. Компрометація або порушення інформації та систем, які мають великий вплив, може мати серйозні або катастрофічно несприятливі наслідки для активів та операцій організації, окремих осіб, інших організацій і країни. Обмеження обробки та зберігання важливої інформації об’єктами в межах юридичної юрисдикції України забезпечує більший контроль над такою обробкою та зберіганням.

Пов’язані заходи: SA-5, SR-4.

Посилання: [OMB A-130], [SP 800-35], [SP 800-160-1], [SP 800-161], [SP 800-171].

## SA-10 УПРАВЛІННЯ КОНФІГУРАЦІЄЮ РОЗРОБНИКА

Заходи захисту:

Вимагати від розробника системи, системного компонента або системної служби:

a. виконання управління конфігурацією під час [*Вибір (один або кілька): проєктування; розробки; реалізації; експлуатації; видалення*] системи, компонента або служби;

b. документувати, керувати та контролювати цілісність змін у [*Призначення: визначених організацією елементах конфігурації при управлінні конфігурацією*];

c. впроваджувати тільки схвалені організацією зміни в системі, компоненті або службі;

d. документувати зміни в системі, компоненті або службі та можливі наслідки таких змін для безпеки та приватності;

e. відстежувати недоліки безпеки та усунення дефектів у системі, компоненті або службі та повідомляти про результати [*Призначення: визначений організацією персонал*].

Рекомендації з реалізації: Організації розглядають якість і повноту керування конфігурацією, яку здійснюють розробники, як пряме свідчення застосування ефективних заходів захисту. Заходи захисту включають захист головних копій матеріалу, який використовується для створення важливих для безпеки частин системного обладнання, програмного забезпечення та вбудованого програмного забезпечення від несанкціонованої модифікації або знищення. Підтримка цілісності змін у системі, системному компоненті чи системній службі вимагає суворого контролю конфігурації протягом усього життєвого циклу розробки системи для відстеження авторизованих змін і запобігання несанкціонованим змінам. Елементи конфігурації, які розміщуються під керуванням конфігурації, включають формальну модель; функціональні, високорівневі та низькорівневі специфікації проектування; інші проектні дані; документація щодо реалізації; вихідний код і схеми обладнання; поточна запущена версія об'єктного коду; інструменти для порівняння нових версій

описів обладнання та вихідного коду, що стосуються безпеки, з попередніми версіями; а також тестове обладнання та документація. Залежно від місії та бізнес-потреб організацій і характеру діючих договірних відносин розробники можуть надавати підтримку керування конфігурацією на стадії експлуатації та обслуговування життєвого циклу розробки системи.

Пов'язані заходи: CM-2, CM-3, CM-4, CM-7, CM-9, SA-4, SA-5, SA-8, SA-15, SI-2, SR-3, SR-4, CP-5, CP -6.

Посилення заходів:

(1) УПРАВЛІННЯ КОНФІГУРАЦІЄЮ РОЗРОБНИКА - ПЕРЕВІРКА ЦІЛІСНОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА МІКРОПРОГРАМ

Вимагати від розробника системи, системного компонента або системної служби забезпечити перевірку цілісності програмного забезпечення та компонентів програмного забезпечення.

Рекомендації з реалізації: Перевірка цілісності програмного забезпечення та мікропрограми дозволяє організаціям виявляти несанкціоновані зміни компонентів програмного забезпечення та мікропрограм за допомогою наданих розробниками інструментів, методів і механізмів. Механізми перевірки цілісності також можуть усунути підробку програмного забезпечення та компонентів мікропрограм. Організації перевіряють цілісність програмного забезпечення та мікропрограмних компонентів, наприклад, за допомогою безпечних односторонніх гешів, наданих розробниками. Поставки програмного забезпечення та компонентів мікропрограм також включають оновлення для таких компонентів.

Пов'язані заходи: SI-7, SR-11.

(2) УПРАВЛІННЯ КОНФІГУРАЦІЄЮ РОЗРОБНИКА - АЛЬТЕРНАТИВНІ ПРОЦЕСИ КЕРУВАННЯ КОНФІГУРАЦІЄЮ

Забезпечити альтернативний процес керування конфігурацією за допомогою організаційного персоналу за відсутності спеціалізованої команди керування конфігурацією розробників.

Рекомендації з реалізації: Альтернативні процеси керування конфігурацією можуть знадобитися, коли організації використовують комерційні готові продукти інформаційних технологій. Альтернативні процеси керування конфігурацією включають персонал організації, який переглядає та затверджує запропоновані зміни до систем, компонентів системи і послуг для системи, а також проводить аналіз впливу на безпеку та приватність перед впровадженням змін у системи, компонент чи службу.

Пов'язані заходи: Немає.

(3) УПРАВЛІННЯ КОНФІГУРАЦІЄЮ РОЗРОБНИКА - ПЕРЕВІРКА ЦІЛІСНОСТІ АПАРАТНИХ ЗАСОБІВ

Вимагати від розробника системи, компонента системи або системної служби забезпечувати перевірку цілісності апаратних компонентів.

Рекомендації з реалізації: Перевірка цілісності апаратного забезпечення

дозволяє організаціям виявляти несанкціоновані зміни компонентів апаратного забезпечення за допомогою наданих розробником інструментів, методів, і механізмів. Організації можуть перевіряти цілісність апаратних компонентів за допомогою етикеток, які важко копіювати, серійних номерів, які можна перевірити, наданих розробниками, а також вимагаючи використання технологій захисту від несанкціонованого доступу. Поставлені апаратні компоненти також включають оновлення апаратного забезпечення та мікропрограм для таких компонентів.

Пов'язані заходи: SI-7.

(4) УПРАВЛІННЯ КОНФІГУРАЦІЄЮ РОЗРОБНИКА - ДОВІРЧЕ ГЕНЕРУВАННЯ

Вимагати від розробника системи, системного компонента або системної служби використовувати інструменти для порівняння новозгенерованих версій апаратних описів, вихідного коду та об'єктного коду, що стосуються безпеки, з попередніми версіями.

Рекомендації з реалізації: Надійна генерація описів, вихідного коду та об'єктного коду стосується авторизованих змін апаратного забезпечення, програмного забезпечення та компонентів мікропрограм між версіями під час розробки. Основна увага зосереджена на ефективності процесу керування конфігурацією розробником, щоб гарантувати, що нові згенеровані версії описів обладнання, що стосуються безпеки, вихідного коду та об'єктного коду, продовжують застосовувати політику безпеки для системи, системного компонента або системної служби . Навпаки, SA-10(1) і SA-10(3) дозволяють організаціям виявляти неавторизовані зміни в апаратних, програмних і мікропрограмних компонентах за допомогою інструментів, методів або механізмів, наданих розробниками.

Пов'язані заходи: Немає.

(5) УПРАВЛІННЯ КОНФІГУРАЦІЄЮ РОЗРОБНИКА - ВІДОБРАЖЕННЯ ЦІЛІСНОСТІ ДЛЯ КЕРУВАННЯ ВЕРСІЯМИ

Вимагати від розробника системи, системного компонента або системної служби підтримувати цілісність відображення між основними даними збірки, що описують поточну версію апаратного, програмного забезпечення та мікропрограм, що стосуються безпеки, і локальною головною копією даних для поточних версій.

Рекомендації з реалізації: Відображення цілісності для контролю версій стосується змін апаратного, програмного забезпечення та компонентів мікропрограм під час початкової розробки та оновлень життєвого циклу розробки системи. Підтримка цілісності між основними копіями апаратного, програмного та вбудованого програмного забезпечення (включно з проектами, кресленнями апаратного забезпечення, вихідним кодом) і еквівалентними даними в основних копіях в операційних середовищах має важливе значення для забезпечення доступності систем організації, які підтримують критичні місії і бізнес-функції.

Пов'язані заходи: Немає.

(6) УПРАВЛІННЯ КОНФІГУРАЦІЄЮ РОЗРОБНИКА - ДОВІРЕНЕ ПОСТАЧАННЯ

Вимагати від розробника системи, системного компонента або системної служби виконувати процедури для забезпечення того, щоб апаратні засоби, програмне забезпечення й оновлення прошивки, що стосуються безпеки й оновлюються в організації, точно відповідали оригінальним копіям.

Рекомендації з реалізації: Довірене постачання оновлень апаратного, програмного та мікропрограмного забезпечення, пов'язаного із безпекою, допомагає переконатися, що ці оновлення є правильним представленням оригінальних копій, які зберігаються розробником, і не змінюються під час розповсюдження.

Пов'язані заходи: Немає.

(7) УПРАВЛІННЯ КОНФІГУРАЦІЄЮ РОЗРОБНИКА - ПРЕДСТАВНИКИ БЕЗПЕКИ ТА ПРИВАТНОСТІ

Вимагати, щоб [*Призначення: визначені організацією представники безпеки та приватності*] були включені в [*Призначення: визначене організацією керування змінами конфігурації та процес контролю*].

Рекомендації з реалізації: Представники безпеки та приватності можуть включати офіцерів системної безпеки, старших офіцерів інформаційної безпеки агентства, старших посадових осіб агентства з приватності та офіцерів конфіденційності системи. Персонал, який має досвід інформаційної безпеки та приватності є важливим, оскільки зміни конфігурацій системи можуть мати непередбачені побічні ефекти, та можуть мати відношення до безпеки чи приватності. Виявлення таких змін на ранній стадії процесу може допомогти уникнути ненавмисних негативних наслідків, які зрештою можуть вплинути на стан безпеки та приватності систем. Процес управління змінами конфігурації та вдосконалення контролю стосується процесу керування змінами та контролю, визначеного організаціями в SA-10b.

Пов'язані заходи: Немає.

Посилання: [FIPS 140-3], [FIPS 180-4], [FIPS 202], [SP 800-128], [SP 800-160-1].

## SA-11 ТЕСТУВАННЯ ТА ОЦІНЮВАННЯ РОЗРОБНИКА

Заходи захисту:
Вимагати від розробника системи, системного компонента або системної служби на всіх етапах проєктування та життєвого циклу розробки системи:

a. створити та впровадити план з оцінювання безпеки та приватності;

b. виконати [*Вибір (один або кілька): одиниця; інтеграція; система; регресія*] тестування/оцінювання *[Призначення: з визначеною організацією частотою*] з [*Призначення: визначена організацією глибиною та охопленням*];

c. надати докази (свідчення) виконання плану оцінювання та результати тестування й оцінювань;

d. впровадити перевірку процесу виправлення недоліків;

e. виправити дефекти, виявлені під час тестування та оцінювання.

Рекомендації з реалізації: Тестування та оціннювання розробки підтверджує, що необхідні заходи захисту реалізовано правильно і вони працюють за призначенням, забезпечують виконання бажаної політики безпеки та приватності та відповідають установленим вимогам безпеки та приватності. Властивості безпеки систем і конфіденційність окремих осіб можуть залежати від взаємозв'язку компонентів системи або змін у цих компонентах. Взаємозв'язки або зміни, включаючи оновлення або заміну програм, операційних систем і мікропрограм, можуть негативно вплинути на раніше реалізовані заходи захисту. Постійне оцінювання під час розробки дозволяє проводити додаткові типи тестування та оцінювання, які розробники можуть проводити для зменшення або усунення потенційних недоліків. Тестування спеціальних програмних компонентів може вимагати таких підходів, як ручний перегляд коду, огляд архітектури безпеки та тестування на проникнення, а також статичний аналіз, динамічний аналіз, двійковий аналіз або гібридний аналіз.
Розробники можуть використовувати підходи до аналізу разом із різноманітними інструментами безпеки та фаззингом при огляді вихідного коду. Плани оцінки безпеки та приватності включають конкретні дії, які планують виконати розробники, зокрема типи аналізів, тестування, оцінки та оглядів компонентів програмного забезпечення та мікропрограми; ступінь суворості, який буде застосований; частота поточного тестування та оцінювання; і типи артефактів, створених під час цих процесів. Глибина тестування та оцінювання стосується суворості та рівня деталізації, пов'язаних із процесом оцінювання. Охоплення тестування та оцінювання відноситься до обсягу (тобто кількості та типу) артефактів, включених до процесу оцінювання. Контракти визначають критерії прийнятності для планів оцінки безпеки та приватності, процесів усунення недоліків і підтвердження того, що плани та процеси були ретельно застосовані. Методи перевірки та захисту планів оцінювання, доказів і документації відповідають категорії безпеки або рівню класифікації системи. Контракти можуть визначати вимоги щодо захисту документації.

Пов'язані заходи: CA-2, CA-7, CM-4, SA-3, SA-4, SA-5, SA-8, SA-15, SA-17, SI-2, SR-5, SR-6, SR-7.

Посилення заходів:

(1) ТЕСТУВАННЯ ТА ОЦІНЮВАННЯ РОЗРОБНИКА - АНАЛІЗ СТАТИЧНОГО КОДУ

Вимагати від розробника системи, системного компонента або системної служби використовувати інструменти аналізу статичних кодів для виявлення поширених недоліків і документувати результати аналізу.

Рекомендації з реалізації: Статичний аналіз коду надає технологію та методологію перевірки безпеки та включає перевірку на наявність слабких місць у коді, а також на включення бібліотек чи іншого включеного коду з відомими вразливими місцями або застарілого чи того, що більше не підтримується розробником. Статичний аналіз коду можна використовувати для виявлення вразливостей і застосування безпечних методів кодування. Він найбільш ефективний, коли використовується на ранніх стадіях процесу розробки, коли кожна зміна коду може автоматично сканувати на потенційні недоліки. Статичний аналіз коду може надати чіткі вказівки щодо виправлення та виявити дефекти, які необхідно виправити. Докази правильного впровадження статичного аналізу можуть включати сукупну щільність дефектів для критичних типів дефектів, докази того, що дефекти були перевірені розробниками або

фахівцями з безпеки, і докази того, що дефекти були виправлені. Висока щільність ігнорованих результатів, які зазвичай називають хибними спрацьовуваннями, вказує на потенційну проблему з процесом аналізу або інструментом аналізу. У таких випадках організації зважують достовірність доказів із доказами з інших джерел.

Пов'язані заходи: Немає.

(2) ТЕСТУВАННЯ ТА ОЦІНЮВАННЯ РОЗРОБНИКА - МОДЕЛЮВАННЯ ЗАГРОЗ ТА АНАЛІЗ ВРАЗЛИВОСТЕЙ

Вимагати від розробника системи, системного компонента або системної служби виконувати моделювання загроз та аналіз вразливостей під час розробки та під час подальшого тестування й оцінювання системи, компонента або служби, що:

(a) використовує [*Призначення: визначену організацією інформацію щодо критичності, середовища функціювання, відомих або передбачуваних загроз і прийнятних рівнів ризику*];

(b) використовує такі інструменти та методи: [*Завдання: інструменти та методи, визначені організацією*]; впровадив [*Призначення: визначені організацією інструменти та методи*];

(c) проводить моделювання та аналізи на такому рівні ретельності: [*Завдання: визначена організацією широта та глибина моделювання та аналізу*];

(d) надає докази (свідчення), які відповідають таким критеріям прийнятності [*Призначення: визначеним організацією критеріям прийняття*].

Рекомендації з реалізації: Системи, системні компоненти та системні служби можуть суттєво відрізнятися від функціональних і проектних специфікацій, створених під час вимог і етапів проектування життєвого циклу розробки системи. Таким чином, оновлення моделювання загроз і аналізу вразливостей цих систем, компонентів системи і послуг для системи під час розробки та перед поставкою мають вирішальне значення для їх ефективної роботи. Моделювання загроз і аналіз вразливостей на цій стадії життєвого циклу розробки системи гарантують, що зміни в проектуванні та реалізації були враховані, а вразливості, створені внаслідок цих змін, були переглянуті та пом'якшені.

Пов'язані заходи: PM-15, RA-3, RA-5.

(3) ТЕСТУВАННЯ ТА ОЦІНЮВАННЯ РОЗРОБНИКА - НЕЗАЛЕЖНА ПЕРЕВІРКА ПЛАНІВ ОЦІНЮВАННЯ ТА ДОКАЗІВ

(a) Вимагати від незалежного агента, що задовольняє [*Призначення: визначені організацією критерії незалежності*] перевірити правильність виконання планів оцінювання безпеки та приватності розробника й доказів (свідчень), отриманих під час тестування та оцінювання.

(b) Переконатися, що незалежному агентові надано достатньо інформації для завершення процесу верифікації або надані повноваження для отримання такої інформації.

Рекомендації з реалізації: Незалежні агенти повинні мати відповідну кваліфікацію, включаючи досвід, навички, навчання та сертифікати для

перевірки правильності реалізації планів оцінки безпеки та приватності розробників.

Пов'язані заходи: AT-3, RA-5.

(4) ТЕСТУВАННЯ ТА ОЦІНЮВАННЯ РОЗРОБНИКА - РУЧНИЙ АНАЛІЗ КОДІВ

Вимагати від розробника системи, системного компонента або системної служби виконувати ручний аналіз коду [*Призначення: визначений організацією певний код*], використовуючи [*Призначення: визначені організацією процеси, процедури та/або методики*].

Рекомендації з реалізації: Ручний аналіз коду зазвичай зарезервований для критичного програмного забезпечення та мікропрограмних компонентів системи. Такий аналіз ефективний для виявлення слабких місць, які вимагають знання вимог програми або контексту, який у більшості випадків недоступний для автоматизованих аналітичних інструментів і методів, таких як статичний і динамічний аналіз. Переваги ручного аналізу включають можливість перевірки заходів захисту матриці керування доступом, заходів захисту відповідності додатків та перегляд детальних аспектів криптографічних реалізацій.

Пов'язані заходи: Немає.

(5) ТЕСТУВАННЯ ТА ОЦІНЮВАННЯ РОЗРОБНИКА - ТЕСТУВАННЯ НА ПРОНИКНЕННЯ

Вимагати від розробника системи, системного компонента або системної служби виконувати тестування на проникнення:

a) з таким рівнем детальності [*Призначення: визначена організацією широта і глибина*];

b) за таких обмежень [*Призначення: визначені організацією обмеження*].

Рекомендації з реалізації: Тестування на проникнення – це метод оцінки, у якій оцінювачі, використовуючи всю доступну документацію на продукт або систему і працюючи в умовах певних обмежень, намагаються обійти реалізовані функції безпеки та приватності. Корисна інформація для оцінювачів, які проводять тестування на проникнення, включає технічні характеристики продукту та системи, вихідний код, а також посібники для адміністратора та оператора. Тестування на проникнення може включати тестування білої скриньки, сірої скриньки або чорної скриньки з аналізом, що виконується кваліфікованими фахівцями, які імітують дії противника. Метою тестування на проникнення є виявлення вразливостей у системах, компонентах системи і службах, які є результатом помилок впровадження, помилок конфігурації або інших операційних слабких місць чи недоліків. Тести на проникнення можна виконувати в поєднанні з автоматизованими та ручними перевірками коду, щоб забезпечити вищий рівень аналізу, ніж зазвичай. Коли інформація про сеанс користувача та інша персональна інформація фіксується або записується під час тестування на проникнення, така інформація обробляється належним чином для захисту приватності.

Пов'язані заходи: CA-8, PM-14 , PM-25, PT-2, SA-3, SI-2, SI-6.

(6) ТЕСТУВАННЯ ТА ОЦІНЮВАННЯ РОЗРОБНИКА - АНАЛІЗ ПОВЕРХНІ АТАКИ

Вимагати від розробника системи, компонента системи або системної служби виконувати аналіз поверхніх атак (вразливостей).

Рекомендації з реалізації: Поверхня атаки — це загальна кількість можливих уразливостей інформаційної системи. Поверхні атаки включають будь-які доступні області, де слабкі місця або недоліки в апаратному, програмному та мікропрограмному забезпеченні надають зловмисникам можливість використовувати вразливості. Огляди поверхонь атак гарантують, що розробники аналізують зміни в проектуванні та реалізації систем і пом'якшують вектори атак, створені в результаті змін. Виправлення виявлених недоліків включає скасування небезпечних функцій.

Пов'язані заходи: SA-15.

(7) ТЕСТУВАННЯ ТА ОЦІНЮВАННЯ РОЗРОБНИКА - ПЕРЕВІРКА ОБСЯГУ ТЕСТУВАННЯ ТА ОЦІНЮВАННЯ

Вимагати від розробника системи, системного компонента або системної служби перевіряти, що обсяг тестування й оцінювання забезпечує повне охоплення необхідних засобів захисту та приватності на [*Призначення: визначену організацією глибину тестування та оцінювання*].

Рекомендації з реалізації: Перевірка того, що тестування та оцінювання забезпечують повне охоплення необхідних заходів захисту, які можна здійснити за допомогою різноманітних аналітичних методів, починаючи від неофіційних до формальних. Кожен з цих методів забезпечує зростаючий рівень впевненості, який відповідає ступеню формальності аналізу. Суворе охоплення заходів захисту на найвищих рівнях надійності може бути досягнуто за допомогою формальних методів моделювання та аналізу, включаючи кореляцію між впровадженими заходами захисту та відповідними тестовими випадками.

Пов'язані заходи: SA-15.

(8) ТЕСТУВАННЯ ТА ОЦІНЮВАННЯ РОЗРОБНИКА - ДИНАМІЧНИЙ АНАЛІЗ КОДУ

Вимагати від розробника системи, системного компонента або системної служби використовувати динамічні інструменти аналізу коду для виявлення загальних недоліків та документування результатів аналізу.

Рекомендації з реалізації: Динамічний аналіз коду забезпечує перевірку програмного забезпечення під час виконання за допомогою інструментів, здатних контролювати програми на предмет пошкодження пам'яті, проблем із привілеями користувачів та інших потенційних проблем безпеки. Динамічний аналіз коду використовує інструменти виконання, щоб гарантувати, що функціональні можливості безпеки працюють так, як вони були розроблені. Тип динамічного аналізу, відомий як фаз-тестування, викликає збої програм шляхом навмисного введення неправильних або випадкових даних у програми. Стратегії фаз-тестування виводяться з передбачуваного використання програм, а також

функціональних і проектних специфікацій для програм. Щоб зрозуміти обсяг динамічного аналізу коду та надану гарантію, організації також можуть розглянути можливість проведення аналізу охоплення коду (тобто перевірки ступеня коду за допомогою таких показників, як відсоток перевірених підпрограм або відсоток операторів програми, викликаних під час виконання набору тестів) та/або аналіз узгодженості (тобто перевірка слів, які не є доречними в коді програмного забезпечення, наприклад слів неанглійською мовою або образливих термінів).

Пов'язані заходи: Немає.

(9) ТЕСТУВАННЯ ТА ОЦІНЮВАННЯ РОЗРОБНИКА - ІНТЕРАКТИВНЕ ТЕСТУВАННЯ БЕЗПЕКИ ДОДАТКІВ

Вимагати від розробника системи, системного компонента або системної служби використання інтерактивних інструментів тестування безпеки програми для виявлення недоліків і документування результатів.

Рекомендації з реалізації: Інтерактивне тестування безпеки додатків (також відоме як інструментальне) — це метод виявлення вразливостей шляхом спостереження за додатками під час тестування на предмет їх виконання. Використання інструментарію базується на прямих вимірюваннях фактично запущених додатків і використовує доступ до коду, взаємодії з користувачем, бібліотек, фреймворків, підключень і конфігурацій для безпосереднього вимірювання ефективності керування. У поєднанні з методами аналізу інтерактивне тестування безпеки програми може виявити широкий спектр потенційних вразливостей і підтвердити ефективність контролю. Тестування на основі інструментів працює в режимі реального часу та може використовуватися безперервно протягом життєвого циклу розробки системи.

Пов'язані заходи: Немає.

Посилання: [ISO 15408-3], [SP 800-30], [SP 800-53A], [SP 800-154], [SP 800-160-1].

## SA-12 КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ

[Вилучено: включено до класу SR]

Посилення заходів:

(1) КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - СТРАТЕГІЇ, ІНСТРУМЕНТИ ТА МЕТОДИ ЗАКУПІВЕЛЬ

[Вилучено: включено до класу SR-5].

(2) КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - АНАЛІЗ ПОСТАЧАЛЬНИКІВ

[Вилучено: включено до класу SR-6].

(3) КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - НАДІЙНЕ ПЕРЕВЕЗЕННЯ ТА ЗБЕРІГАННЯ

[Вилучено: включено до SR-3].

(4) КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - ДИВЕРСИФІКАЦІЯ ПОСТАЧАЛЬНИКІВ

[Вилучено: включено до SR-3 (1)].

(5) КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - ОБМЕЖЕННЯ ШКОДИ

[Вилучено: включено до SR-3 (2)].

(6) КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - МІНІМІЗАЦІЯ ЧАСУ ЗАКУПІВЕЛЬ

[Вилучено: включено до SR-5 (1)].

(7) КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - ОЦІНЮВАННЯ ПЕРЕД ВИБОРОМ, ПРИЙНЯТТЯМ ТА ОНОВЛЕННЯМ

[Вилучено: включено до SR-5 (2)].

(8) КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - ВИКОРИСТАННЯ ВСЕБІЧНОЇ РОЗВІДУВАЛЬНОЇ ІНФОРМАЦІЇ

[Вилучено: включено до RA-3 (2)].

(9) КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - ОПЕРАЦІЙНА БЕЗПЕКА

[Вилучено: включено до SR-7].

(10) КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - ПЕРЕВІРКА НА СПРАВЖНІСТЬ І НЕЗМІНЕНІСТЬ

[Вилучено: включено до SR-4 (3)].

(11) КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - ТЕСТУВАННЯ ТА АНАЛІЗ НА ПРОНИКНЕННЯ

[Вилучено: включено до SR-6 (1)].

(12) КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - УГОДИ ПРО ПОВІДОМЛЕННЯ

[Вилучено: включено до SR-8].

(13) КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - КОМПОНЕНТИ КРИТИЧНИХ СИСТЕМ

[Вилучено: включено до MA-6 та RA-9].

(14) КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - ІДЕНТИЧНІСТЬ ТА ПРОСТЕЖУВАНІСТЬ

[Вилучено: включено до SR-4 (1) та SR-4 (2)].

(15) КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - ПРОЦЕСИ ДЛЯ УСУНЕННЯ НЕДОЛІКІВ АБО ДЕФЕКТІВ

[Вилучено: включено до SR-3].

## SA-13 ДОВІРЧІСТЬ

[Вилучено: Включено до SA-8].

## SA-14 АНАЛІЗ КРИТИЧНОСТІ

[Вилучено: Включено до RA-9].

Посилення заходів:

(1) КРИТИЧНІ КОМПОНЕНТИ БЕЗ ЖИТТЄЗДАТНИХ АЛЬТЕРНАТИВНИХ ДЖЕРЕЛ

[Вилучено: Включено до SA-20].

## SA-15 ПРОЦЕСИ, СТАНДАРТИ ТА ІНСТРУМЕНТИ РОЗРОБКИ

Заходи захисту:

a. Вимагати від розробника системи, системного компонента або системної служби слідувати документованому процесу розробки, який:

1. явно відповідає вимогам безпеки та приватності;

2. визначає стандарти й інструменти, які використовуються в процесі розробки;

3. документує конкретні параметри та конфігурації інструментарію, що використовуються в процесі розробки;

4. документує, управляє та забезпечує цілісність змін у процесі та/або інструментах, які використовуються в процесі розробки.

b. Ознайомитися з процесом розробки, стандартами, інструментами, параметрами інструментарію і конфігураціями інструментів [*Призначення: визначена організацією частота*], щоб визначити, чи можуть вибрані й використовувані процеси, стандарти, інструменти, параметри та конфігурації інструментів задовольнити [*Призначення: визначені організацією вимоги до безпеки та приватності*].

Рекомендації з реалізації: Засоби розробки включають мови програмування та системи автоматизованого проектування. Огляди процесів розробки включають використання моделей зрілості для визначення потенційної ефективності таких процесів. Підтримка цілісності змін в інструментах і процесах сприяє ефективній оцінці ризиків ланцюга постачання і зменшенню їх наслідків. Така цілісність вимагає контролю конфігурації протягом життєвого циклу розробки системи для відстеження авторизованих змін і запобігання несанкціонованим змінам.

Пов’язані заходи: MA-6, SA-3, SA-4, SA-8, SA-10, SA-11, SR-3, SR-4, SR-5, SR-6,

SR-9.

Посилення заходів:

(1) ПРОЦЕС, СТАНДАРТИ ТА ІНСТРУМЕНТИ РОЗРОБКИ - ПОКАЗНИКИ ЯКОСТІ

Вимагати від розробника системи, компонента системи або системної служби:

(a) визначити показники якості на початку процесу розробки;

(b) надати докази відповідності показникам якості [*Вибір (один або більше):* [*Призначення: визначена організацією частота*]; [*Призначення: визначені організацією етапи розгляду програми*]; *після постачання*].

Рекомендації з реалізації: Організації використовують показники якості для встановлення прийнятних рівнів якості системи. Метрики можуть включати показники якості, які є наборами критеріїв завершення або стандартів достатності, які представляють задовільне виконання конкретних етапів проекту розробки системи. Наприклад, перевірка якості може вимагати усунення всіх попереджень компілятора або визначення того, що такі попередження не впливають на ефективність необхідних можливостей безпеки чи приватності. На етапах виконання проектування контроль якості забезпечує чіткі, недвозначні показники прогресу. Інші показники застосовуються до всього проекту вцілому. Метрики можуть включати визначення порогових значень серйозності вразливостей відповідно до стійкості організації щодо ризику, наприклад вимоги відсутності відомих вразливостей у поставленій системі із середньою або високою серйозністю загальної системи оцінки вразливостей (CVSS).

Пов’язані заходи: Немає.

(2) ПРОЦЕС, СТАНДАРТИ ТА ІНСТРУМЕНТИ РОЗРОБКИ - ЗАСОБИ ВІДСТЕЖЕННЯ БЕЗПЕКИ ТА ПРИВАТНОСТІ

Вимагати від розробника системи, системного компонента або системної служби вибирати та використовувати засоби відстеження безпеки та приватності під час процесу розробки.

Рекомендації з реалізації: Група розробників системи обирає і розгортає засоби відстеження безпеки та приватності, включаючи системи відстеження вразливостей або робочих елементів, які полегшують призначення, сортування, фільтрацію та відстеження виконаних робочих елементів або завдань, пов’язаних із процесами розробки.

Пов’язані заходи: SA-11.

(3) ПРОЦЕС, СТАНДАРТИ ТА ІНСТРУМЕНТИ РОЗРОБКИ - АНАЛІЗ КРИТИЧНОСТІ

Вимагати від розробника системи, системного компонента або системної служби виконати аналіз критичності:

a) у наступних точках ухвалення рішень у життєвому циклі розробки системи: [*Призначення: визначені організацією точки ухвалення рішень у життєвому циклі розробки системи*];

b) на наступному рівні суворості [*Призначення: визначена організацією ширина/глибина аналізу критичності*].

Рекомендації з реалізації: Аналіз критичності, який виконує розробник, надає вхідні дані для аналізу критичності, який виконує організація. Внесок розробників є важливим для аналізу критичності організацією, оскільки вона може не мати доступу до детальної проектної документації для компонентів системи, які розроблені як комерційні готові продукти. Така проектна документація включає функціональні специфікації, проекти високого рівня, проекти низького рівня, вихідний код і схеми обладнання. Аналіз критичності важливий для систем організації, які позначаються як активи високої вартості. Активи високої вартості можуть бути системами з помірним або високим впливом через підвищений конкурентний інтерес або потенційний негативний вплив на державну установу. Внесок розробників особливо важливий, коли організації проводять аналіз критичності ланцюга постачання.

Пов'язані заходи: RA-9.

(4) ПРОЦЕС, СТАНДАРТИ ТА ІНСТРУМЕНТИ РОЗРОБКИ - МОДЕЛЮВАННЯ ЗАГРОЗ ТА АНАЛІЗ ВРАЗЛИВОСТЕЙ

[Вилучено: Включено до SA-11 (2)].

(5) ПРОЦЕС, СТАНДАРТИ ТА ІНСТРУМЕНТИ РОЗРОБКИ - ЗМЕНШЕННЯ ПОВЕРХНІ АТАКИ

Вимагати від розробника системи, системного компонента або системної служби зменшити поверхню атаки до [*Призначення: визначені організацією межі*].

Рекомендації з реалізації: Зменшення площі атаки тісно пов'язане з аналізом загроз і вразливостей, а також архітектурою системи. Зменшення поверхні атаки — це засіб зменшення ризику для організацій, даючи зловмисникам менше можливостей використовувати слабкі місця або недоліки (тобто потенційні вразливості) у системах, компонентах системи і послуг для системи. Зменшення поверхні атаки включає в себе реалізацію концепції багаторівневого захисту, застосування принципів найменших привілеїв і найменших функціональних можливостей, застосування безпечних практик розробки програмного забезпечення, припинення використання небезпечних функцій, зменшення точок входу, доступних для неавторизованих користувачів, зменшення кількості коду, який виконується, і видалення програми інтерфейсів програмування (API), уразливих до атак.

Пов'язані заходи: AC-6, CM-7, RA-3.

(6) ПРОЦЕС, СТАНДАРТИ ТА ІНСТРУМЕНТИ РОЗРОБКИ - ПОСТІЙНЕ ВДОСКОНАЛЕННЯ

Вимагає від розробника системи, системного компонента або системної служби реалізувати явний процес для постійного вдосконалення процесу розробки.

Рекомендації з реалізації: Розробники систем, компонентів системи і послуг для системи розглядають ефективність і результативність своїх процесів розробки для досягнення цілей якості та вирішення можливостей безпеки та приватності

в поточних загрозливих середовищах.

Пов’язані заходи: Немає.

(7) ПРОЦЕС, СТАНДАРТИ ТА ІНСТРУМЕНТИ РОЗРОБКИ - АВТОМАТИЗОВАНИЙ АНАЛІЗ ВРАЗЛИВОСТЕЙ

Вимагати від розробника системи, компонента системи або системної служби [*Призначення: частота, визначена організацією*]:

(a) виконувати автоматизований аналіз вразливостей за допомогою [*Призначення: визначені організацією інструменти*];

(b) визначити потенційні можливості використання виявлених вразливостей;

(c) визначити потенційні можливості зменшення ризику для вразливих місць;

(d) надавати результати аналізу [*Призначення: визначено організацією персоналу або посадовим особам*].

Рекомендації з реалізації: Автоматизовані інструменти можуть бути ефективними в аналізі слабких місць або недоліків у великих і складних системах, які можна використовувати, розставляючи пріоритети вразливостей за ступенем серйозності та надаючи рекомендації щодо зменшення ризиків

Пов’язані заходи: RA-5, SA-11.

(8) ПРОЦЕС, СТАНДАРТИ ТА ІНСТРУМЕНТИ РОЗРОБКИ - ПОВТОРНЕ ВИКОРИСТАННЯ ІНФОРМАЦІЇ ПРО ЗАГРОЗИ ТА ВРАЗЛИВОСТІ

Вимагати від розробника системи, компонента системи або системної служби використовувати моделювання загроз та аналіз вразливостей з аналогічних систем, компонентів або служб для інформування про поточний процес розробки.

Рекомендації з реалізації: Аналіз вразливостей, виявлених у подібних програмних продуктах, може свідчити про потенційні проблеми з проектуванням і впровадженням систем, що розробляються. Подібні системи або системні компоненти можуть існувати в організаціях-розробниках. Інформація про вразливості доступна з різних державних і приватних джерел, включаючи національну базу даних про вразливості NIST.

Пов’язані заходи: Немає.

(9) ПРОЦЕС, СТАНДАРТИ ТА ІНСТРУМЕНТИ РОЗРОБКИ - ВИКОРИСТАННЯ РЕАЛЬНИХ ДАНИХ

[Вилучено: Включено до SA-3 (2)].

(10) ПРОЦЕС, СТАНДАРТИ ТА ІНСТРУМЕНТИ РОЗРОБКИ - ПЛАН РЕАГУВАННЯ НА ІНЦИДЕНТИ

Вимагати від розробника системи, компонента системи або системної служби надавати, реалізовувати та перевіряти план реагування на інциденти.

Рекомендації з реалізації: План реагування на інциденти, наданий

розробниками, може надавати інформацію, недоступну для організацій, і бути включений до плану реагування на інциденти в організації. Інформація для розробників також може бути надзвичайно корисною, наприклад, коли організації реагують на вразливості в комерційних готових продуктах.

Пов'язані заходи: IR-8.

(11) ПРОЦЕС, СТАНДАРТИ ТА ІНСТРУМЕНТИ РОЗРОБКИ - РЕЗЕРВУВАННЯ СИСТЕМИ АБО КОМПОНЕНТА

Вимагати від розробника системи або системного компонента резервування системи або компонента, який буде випущено або доставлено разом з відповідними доказами, що підтверджують остаточну перевірку безпеки та приватності.

Рекомендації з реалізації: Архівування системи або компонентів системи вимагає від розробника збереження ключових артефактів розробки, включаючи специфікації апаратного забезпечення, вихідний код, об'єктний код і відповідну документацію з процесу розробки, яка може забезпечити готову базову конфігурацію для оновлень або модифікацій системи та компонентів.

Пов'язані заходи: CM-2.

(12) ПРОЦЕС, СТАНДАРТИ ТА ІНСТРУМЕНТИ РОЗРОБКИ - МІНІМІЗАЦІЯ ПЕРСОНАЛЬНОЇ ІНФОРМАЦІЇ

Вимагати від розробника системи чи системного компонента мінімізувати використання персональної інформації в середовищах розробки та тестування.

Рекомендації з реалізації: Організації можуть мінімізувати ризик конфіденційності особи, використовуючи такі методи, як деідентифікація або синтетичні дані. Обмеження використання ідентифікаційної інформації в середовищах розробки та тестування допомагає знизити рівень ризику конфіденційності, який створює система.

Пов'язані заходи: PM-25, SA-3, SA-8.

Посилання: [SP 800-160-1], [IR 8179].

## SA-16 НАВЧАННЯ, ЩО НАДАЄТЬСЯ РОЗРОБНИКАМИ

Заходи захисту:
Вимагати від розробника системи, системного компонента або системної служби забезпечити наступне навчання щодо правильного використання та функціонування реалізованих функцій, заходів і механізмів безпеки та приватності [*Призначення: визначене організацією навчання*].

Рекомендації з реалізації: Навчання персоналу має важливе значення для забезпечення ефективності заходів захисту, впроваджених в системах організації. Типи навчання включають веб- та комп'ютерне навчання, навчання в аудиторії та практичне навчання (включаючи мікронавчання). Організації також можуть запросити навчальні матеріали від розробників для проведення внутрішнього навчання або запропонувати самонавчання персоналу організації. Організації визначають тип необхідного навчання та можуть вимагати різних типів навчання для різних функцій безпеки та приватності, заходів захисту та механізмів.

Пов’язані заходи: AT-2, AT-3, PE-3, SA-4, SA-5.

Посилення заходів: Немає.

Посилання: Немає.

## SA-17 ПРОЄКТ ТА АРХІТЕКТУРА БЕЗПЕКИ ТА ПРИВАТНОСТІ ДЛЯ РОЗРОБНИКА

Заходи захисту:
Вимагати від розробника системи, системного компонента або системної служби створення специфікації проєкту та архітектури безпеки та приватності, яка:

a. узгоджується з архітектурою безпеки та приватності організації яка є невід’ємною частиною корпоративної архітектури організації;

b. точно та повністю описує необхідні функції безпеки та приватності, а також розподіл заходів захисту між фізичними та логічними компонентами;

c. пояснює, як разом працюють окремі функції, механізми та служби безпеки для забезпечення необхідних можливостей безпеки та єдиного підходу до захисту.

Рекомендації з реалізації: Архітектура безпеки та приватності розробників спрямована на зовнішніх розробників, хоча їх також можна застосовувати і для внутрішньої (власної) розробки. Навпаки, PL-8 спрямований на внутрішніх розробників, які гарантують, що організації розроблять архітектуру безпеки та приватності, інтегровану з архітектурою організації. Різниця між SA-17 і PL-8 особливо важлива, коли організації передають розробку систем, компонентів системи або послуг для системи аутсорсингу та коли існує вимога продемонструвати узгодженість з корпоративною архітектурою та архітектурою безпеки та приватності організації. [ISO 15408-2], [ISO 15408-3] і [SP 800-160-1] надають інформацію про архітектуру та безпеки, включаючи офіційні моделі політики, компоненти, що стосуються безпеки, формальну та неофіційну переписку, концептуально просте проектування, і структурування для найменших привілеїв і тестування.

Пов’язані заходи: PL-2, PL-8, PM-7, SA-3, SA-4, SA-8, SC-7.

Посилення заходів:

(1) ПРОЄКТ ТА АРХІТЕКТУРА БЕЗПЕКИ ТА ПРИВАТНОСТІ РОЗРОБНИКА - ФОРМАЛЬНА МОДЕЛЬ ПОЛІТИКИ

Вимагати від розробника системи, компонента системи або системної служби:

(a) створювати, як невіддільну частину процесу розробки, формальну модель політики, що описує [*Призначення: визначені організацією елементи організаційної політики безпеки*], які підлягають виконанню;

(b) довести, що формальна модель політики є внутрішньо послідовною і достатньою для виконання визначених елементів політики безпеки організації, коли вона реалізована.

Рекомендації з реалізації: Формальні моделі описують певну поведінку або політику безпеки та приватності за допомогою формальних мов, таким чином дозволяючи формально підтвердити правильність цієї поведінки та політики. Не всі компоненти системи можна моделювати. Як правило, формальні специфікації охоплюють поведінку або політики, такі як недискреційні політики контролю доступу. Організації обирають формальну мову моделювання та підхід на основі характеру поведінки та політики, які необхідно описати, та наявних інструментів.

Пов'язані заходи: AC-3, AC-4, AC -25.

(2) ПРОЄКТ ТА АРХІТЕКТУРА БЕЗПЕКИ ТА ПРИВАТНОСТІ РОЗРОБНИКА - КОМПОНЕНТИ, ЩО НЕОБХІДНІ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ

Вимагати від розробника системи, компонента системи або системної служби:

(a) визначити апаратне, програмне та мікропрограмне забезпечення, що необхідне для забезпечення безпеки;

(b) надати обґрунтування того, що визначення апаратного, програмного та мікропрограмного забезпечення, яке необхідне для забезпечення безпеки, є повним.

Рекомендації з реалізації: Релевантне для безпеки апаратне, програмне та вбудоване програмне забезпечення представляють частину системи, компонента або служби, яка, як довіряється, працюватиме правильно для підтримки необхідних властивостей безпеки.

Пов'язані заходи: AC -25, SA-5.

(3) ПРОЄКТ ТА АРХІТЕКТУРА БЕЗПЕКИ ТА ПРИВАТНОСТІ РОЗРОБНИКА - ФОРМАЛЬНА ВІДПОВІДНІСТЬ

Вимагати від розробника системи, компонента системи або системної служби:

(a) створювати, як невіддільну частину процесу розробки, офіційну специфікацію верхнього рівня, яка визначає інтерфейси апаратного, програмного та мікропрограмного забезпечення, що необхідне для забезпечення безпеки, з погляду виключень, повідомлень про помилки та ефектів;

(b) надавати докази, якщо це можливо, з додатковою неофіційною демонстрацією, що формальна специфікація верхнього рівня відповідає формальній моделі політики;

(c) показувати через неофіційну демонстрацію, що формальна специфікація верхнього рівня повністю охоплює інтерфейси апаратного, програмного та мікропрограмного забезпечення, яке необхідне для забезпечення безпеки;

(d) демонструвати, що формальна специфікація верхнього рівня є точним описом реалізованого апаратного, програмного та мікропрограмного забезпечення, яке необхідне для забезпечення безпеки;

(e) описувати апаратне, програмне та мікропрограмне забезпечення, що необхідне для забезпечення безпеки, яке не розглядається в офіційній специфікації верхнього рівня, але є строго внутрішнім для апаратного, програмного та мікропрограмного забезпечення, що необхідне для забезпечення безпеки.

Рекомендації з реалізації: Формальні методи можуть бути використані, щоб показати, що властивості безпеки високого рівня задовольняють формальному опису системи, і що формальний опис системи правильно реалізований описом деякого нижчого рівня, включаючи опис апаратного забезпечення. Узгодженість між офіційною специфікацією верхнього рівня та формальними моделями політики, як правило, не піддається повному доказу. Тому для демонстрації такої послідовності може знадобитися поєднання формальних і неформальних методів. Узгодженість між офіційною специфікацією верхнього рівня та фактичною реалізацією може вимагати використання неофіційної демонстрації через обмеження застосовності формальних методів, щоб довести, що специфікація точно відображає реалізацію. Апаратні, програмні та мікропрограмні механізми, внутрішні для компонентів, що мають відношення до безпеки, включають регістри відображення та прямий вхід і вихід з пам'яті.

Пов'язані заходи: AC-3, AC-4, AC -25, SA-4, SA-5.

(4) ПРОЄКТ ТА АРХІТЕКТУРА БЕЗПЕКИ ТА ПРИВАТНОСТІ РОЗРОБНИКА - НЕФОРМАЛЬНА ВІДПОВІДНІСТЬ

Вимагати від розробника системи, компонента системи або системної служби:

(a) створювати, як невіддільну частину процесу розробки, неформальну описову специфікацію верхнього рівня, яка визначає інтерфейси апаратного, програмного та мікропрограмного забезпечення, що необхідне для забезпечення безпеки, з погляду виключень, повідомлень про помилки та ефекти;

(b) демонструвати через [*Вибір: неофіційна демонстрація, переконливий аргумент з формальними методами і т. д.*], що описова специфікація верхнього рівня узгоджується з формальною моделлю політики;

(c) показати за допомогою неофіційної демонстрації, що описова специфікація верхнього рівня повністю охоплює інтерфейси апаратного, програмного та мікропрограмного забезпечення, пов'язаного з безпекою;

(d) показати, що описова специфікація верхнього рівня є точним описом інтерфейсів апаратного, програмного та мікропрограмного забезпечення, пов'язаного з безпекою;

(e) описати важливе для безпеки апаратне, програмне забезпечення та механізми вбудованого програмного забезпечення, які не розглядаються в описовій специфікації верхнього рівня, але важливі для безпеки апаратного забезпечення та мікропрограмного забезпечення.

Рекомендації з реалізації: Узгодженість між описовою специфікацією верхнього рівня (тобто проектом високого/низького рівня) та моделлю формальної політики, як правило, не піддається повному доведенню. Тому для демонстрації такої послідовності може знадобитися поєднання формальних і неформальних методів. Механізми апаратного, програмного та мікропрограмного забезпечення, суворо внутрішні для апаратного, програмного та мікропрограмного забезпечення, що мають відношення до безпеки, включають регістри відображення та прямий вхід і вихід пам'яті.

Пов'язані заходи: SA-5.

(5) ПРОЄКТ ТА АРХІТЕКТУРА БЕЗПЕКИ ТА ПРИВАТНОСТІ РОЗРОБНИКА - КОНЦЕПТУАЛЬНИЙ ПРОЄКТ

Вимагати від розробника системи, компонента системи або системної служби:

(a) розробити та структурувати апаратне, програмне й мікропрограмне забезпечення, що необхідне для забезпечення безпеки та використовує повний, концептуально простий механізм захисту з точно визначеною семантикою;

(b) внутрішньо структурувати апаратне, програмне та мікропрограмне забезпечення, що має відношення до безпеки, зі специфікаціями цього механізму.

Рекомендації з реалізації: Принцип зменшеної складності стверджує, що проект системи є максимально простим і малим (див. SA-8(7)). Невеликий і простий проект легше зрозуміти й проаналізувати і має, як правило, менше помилок (див. AC-25, SA-8(13)). Принцип зменшеної складності застосовується до будь-якого аспекту системи, але він має особливе значення для безпеки через різноманітні аналізи, які виконуються для отримання доказів щодо нових властивостей безпеки системи. Застосування принципу зниженої складності сприяє здатності розробників системи розуміти правильність і повноту функцій безпеки системи та полегшує ідентифікацію потенційних вразливостей. Наслідок зменшення складності стверджує, що простота системи безпосередньо пов'язана з кількістю вразливостей, які вона міститиме. Тобто простіші системи містять менше вразливостей. Важливою перевагою зниження складності є те, що легше зрозуміти, чи була політика безпеки зафіксована в системі, і що менше вразливостей, ймовірно, буде введено під час інженерних робіт. Додатковою перевагою є те, що будь-який такий висновок щодо правильності, повноти та наявності вразливостей можна зробити з вищим ступенем упевненості на відміну від висновків, зроблених у ситуаціях, коли проект системи є складним.

Пов'язані заходи: AC -25, SA-8, SC-3.

(6) ПРОЄКТ ТА АРХІТЕКТУРА БЕЗПЕКИ ТА ПРИВАТНОСТІ РОЗРОБНИКА - СТРУКТУРА ДЛЯ ТЕСТУВАННЯ

Вимагати від розробника системи, системного компонента або системної служби структурувати відповідне апаратне, програмне та мікропрограмне забезпечення для тестування.

Рекомендації з реалізації: Застосування принципів проектування безпеки в [SP 800-160-1] сприяє повному, узгодженому та комплексному тестуванню й оцінці

систем, компонентів системи і послуг. Ретельність такого тестування сприяє створенню доказів для створення ефективного випадку гарантії або аргументу щодо надійності системи, системного компонента або послуги.

Пов'язані заходи: SA-5, SA-11.

(7) ПРОЄКТ ТА АРХІТЕКТУРА БЕЗПЕКИ ТА ПРИВАТНОСТІ РОЗРОБНИКА - СТРУКТУРА ДЛЯ НАЙМЕНШОГО ПРИВІЛЕЮ

Вимагати від розробника системи, системного компонента або системної служби структурувати апаратне, програмне та мікропрограмне забезпечення, необхідне для забезпечення безпеки таким чином, щоб полегшити контроль доступу з найменшими привілеями.

Рекомендації з реалізації: Принцип найменших привілеїв стверджує, що кожному компоненту надається достатня кількість привілеїв для виконання визначених ним функцій, але не більше (див. SA-8(14)). Застосування принципу найменших привілеїв обмежує сферу дій компонента, що має два бажаних ефекту. По-перше, вплив на безпеку збою, пошкодження або неправильного використання компонента системи призводить до мінімізації впливу на безпеку. По-друге, спрощується аналіз безпеки компонента. Найменший привілей — це поширений принцип, який відображається в усіх аспектах проектування безпечної системи. Інтерфейси, які використовуються для виклику можливостей компонентів, доступні лише для певних підмножин користувачів, а конструкція компонентів підтримує досить дрібну деталізацію привілеїв. Наприклад, у випадку механізму аудиту може бути інтерфейс для менеджера аудиту, який налаштовує параметри аудиту; інтерфейс для оператора аудиту, який забезпечує безпечний збір і зберігання даних аудиту; і, нарешті, ще один інтерфейс для перевіряючого аудитора, якому потрібно лише переглядати зібрані дані аудиту, але не потрібно виконувати операції з цими даними. На додаток до своїх проявів на інтерфейсі системи, найменші привілеї можуть використовуватися як керівний принцип для внутрішньої структури самої системи. Одним із аспектів внутрішніх найменших привілеїв є конструювання модулів таким чином, щоб лише елементи, інкапсульовані модулем, безпосередньо керувалися функціями в модулі. Зовнішні по відношенню до модуля елементи, на які може вплинути робота модуля, одержують непрямий доступ через взаємодію (наприклад, через виклик функції) з модулем, який містить ці елементи. Іншим аспектом внутрішніх найменших привілеїв є те, що область даного модуля або компонента включає лише ті елементи системи, які необхідні для його функціональності, а режими доступу до елементів (наприклад, читання, запис) мінімальні.

Пов'язані заходи: AC-5, AC-6, SA-8.

(8) ПРОЄКТ ТА АРХІТЕКТУРА БЕЗПЕКИ ТА ПРИВАТНОСТІ РОЗРОБНИКА - ОРКЕСТРОВКА

Проектування [*Призначення: визначені організацією критичні системи або системні компоненти*] зі скоординованою поведінкою для реалізації таких можливостей: [*Призначення: визначені організацією можливості, за системою чи компонентом*].

Рекомендації з реалізації: Ресурси безпеки, які розподілені, розташовані на різних рівнях або в різних елементах системи чи реалізовані для підтримки різних аспектів надійності, можуть взаємодіяти непередбаченими або

неправильними способами. Негативні наслідки можуть включати каскадні збої, перешкоди або розриви в охопленні. Координація поведінки ресурсів безпеки (наприклад, шляхом забезпечення встановлення одного патча на всіх ресурсах перед внесенням змін у конфігурацію, які припускають, що патч поширюється) може запобігти таким негативним взаємодіям.

Пов'язані заходи: Немає.

(9) ПРОЄКТ ТА АРХІТЕКТУРА БЕЗПЕКИ ТА ПРИВАТНОСТІ РОЗРОБНИКА - РІЗНОМАНІТНІСТЬ ПРОЕКТУВАННЯ

Використовуйте різне проектування для [*Призначення: визначені організацією критично важливі системи або компоненти системи*], щоб задовольнити загальний набір вимог або забезпечити еквівалентну функціональність.

Рекомендації з реалізації: Різноманітність проектування досягається шляхом надання однакової специфікації вимог багатьом розробникам, кожен з яких відповідає за розробку варіанту системи або системного компонента, який має відповідати заданим вимогам. Варіативність може бути в проектуванні програмного забезпечення чи апаратного забезпечення або в обох випадках одразу. Відмінності в конструкціях варіантів можуть бути результатом досвіду розробника (наприклад, попереднього використання шаблону проектування), стилю проектування (наприклад, під час розкладання необхідної функції на менші, визначення того, що є окремою функцією і як розбити функції на підфункції), вибір бібліотек і середовище розробки (наприклад, різні інструменти проектування полегшують візуалізацію деяких шаблонів проектування). Різноманітність проектування апаратного забезпечення включає прийняття різних рішень щодо того, яку інформацію зберігати в аналоговій формі, а яку інформацію перетворювати в цифрову форму, передачу тієї самої інформації в різний час і введення затримок у вибірці (часова рознесеність). Різноманітність проектування зазвичай використовується для підтримки відмовостійкості.

Пов'язані заходи: Немає.

Посилання: [ISO 15408-2], [ISO 15408-3], [SP 800-160-1].

## SA-18 ЗАХИСТ ТА ВИЯВЛЕННЯ ПІДРОБКИ

[Вилучено: Включено до SR-9].

Посилення заходів:

(1) ЗАХИСТ ТА ВИЯВЛЕННЯ ПІДРОБКИ - ЕТАПИ ЖИТТЄВОГО ЦИКЛУ РОЗРОБКИ СИСТЕМИ

[Вилучено: Включено до SR-9 (1)].

(2) ЗАХИСТ ТА ВИЯВЛЕННЯ ПІДРОБКИ - ПЕРЕВІРКА СИСТЕМ АБО КОМПОНЕНТІВ

[Вилучено: Включено до SR-10]

## SA-19 СПРАВЖНІСТЬ КОМПОНЕНТА

[Вилучено: Включено до SR-11]

Посилення заходів:

(1) СПРАВЖНІСТЬ КОМПОНЕНТА - НАВЧАННЯ БОРОТЬБІ З ПІДРОБЛЕННЯМ

[Вилучено: Включено до SR-11 (1)]

(2) СПРАВЖНІСТЬ КОМПОНЕНТА - УПРАВЛІННЯ КОНФІГУРАЦІЄЮ ДЛЯ ОБСЛУГОВУВАННЯ ТА РЕМОНТУ КОМПОНЕНТІВ

[Вилучено: Включено до SR-11 (2)]

(3) СПРАВЖНІСТЬ КОМПОНЕНТА - УТИЛІЗАЦІЯ КОМПОНЕНТІВ

[Вилучено: Включено до SR-12]

(4) СПРАВЖНІСТЬ КОМПОНЕНТА - СКАНУВАННЯ НА ПІДРОБКУ

[Вилучено: Включено до SR-11 (3)]

## SA-20 ІНДИВІДУАЛЬНА РОЗРОБКА КРИТИЧНИХ КОМПОНЕНТІВ

Заходи захисту:

Повторно реалізувати або налаштувати [*Призначення: визначені організацією критичні компоненти системи*].

Рекомендації з реалізації: Організації визначають, що певним компонентам системи, ймовірно, не можна довіряти через загрози та вразливі місця в них, та для яких неможливо впровадити життєздатних заходи захисту для належного зменшення ризику. Повторна реалізація або спеціальна розробка таких компонентів може задовольнити вимоги щодо вищої впевненості та здійснюється шляхом ініціювання змін компонентів системи (включаючи апаратне, програмне та мікропрограмне забезпечення) для зменшення вірогідності стандартних атак зловмисників. У ситуаціях, коли альтернативне джерело не доступне, а організації вирішують не перевпроваджувати чи не розробляти на замовлення критичні компоненти системи, можна застосувати додаткові заходи захисту. Контроль включає розширений аудит, обмеження доступу до вихідного коду та утиліт системи, а також захист від видалення файлів системи та програм.

Пов’язані заходи: CP-2, RA-9, SA-8.

Посилення заходів: Немає.

Посилання: [SP 800-160-1].

## SA-21 ПЕРЕВІРКА РОЗРОБНИКА

Заходи захисту:

Вимагати, щоб розробник [*Призначення: визначених організацією системи, компонент системи або послуги*]:

a. мав відповідні дозволи доступу, як визначено призначеним [*Призначення: визначеним організацією уповноваженим органом*];

b. відповідає таким додатковим критеріям перевірки персоналу: [*Призначення: визначені організацією додаткові критерії перевірки персоналу*].

Рекомендації з реалізації: Перевірка здійснюється щодо зовнішніх розробників. Внутрішня перевірка розробників регулюється PS-3. Оскільки система, компонент системи або системна служба можуть використовуватися в критично важливих діях, важливих для інтересів національної або економічної безпеки України , організації зацікавлені в тому, щоб розробники заслуговували на довіру. Ступінь довіри, який вимагається від розробників, може відповідати рівню довіри осіб, які отримують доступ до систем, компонентів системи або послуг для системи після розгортання. Критерії авторизації та перевірки персоналу включають допуски, перевірку репутації, громадянство та національність. Надійність розробника також може включати перевірку та аналіз власності компанії та відносин, які компанія має з організаціями, які потенційно можуть вплинути на якість і надійність систем, компонентів або послуг, що розробляються. Виконання необхідних критеріїв авторизації доступу та перевірки персоналу включає надання списку всіх осіб, які мають право виконувати дії з розробки у вибраній системі, системному компоненті чи службі, щоб організації могли підтвердити, що розробник задовольнив вимоги авторизації та перевірки.

Пов'язані заходи: PS-2, PS-3, PS-6, PS-7, SA-4, SR-6.

Посилення заходів:

(1) СКРИНІНГ РОЗРОБНИКА - ПЕРЕВІРКА СКРИНІНГУ

[Вилучено: включено до SA-21]

Посилання: Немає.

## SA-22 КОМПОНЕНТИ СИСТЕМИ, ЩО НЕ ПІДТРИМУЮТЬСЯ

Заходи захисту:

a. Замінювати компоненти системи, якщо підтримка компонентів більше не доступна розробнику, постачальнику або виробнику.

b. Надавати такі варіанти альтернативних джерел для подальшої підтримки непідтримуваних компонентів [*Вибір (один або більше): внутрішня підтримка; [Призначення: підтримка, визначена організацією від зовнішніх постачальників*]].

Рекомендації з реалізації: Підтримка компонентів системи включає виправлення програмного забезпечення, оновлення мікропрограм, запасні частини та контракти на технічне обслуговування. Прикладом непідтримуваних компонентів є випадки, коли постачальники більше не надають критичних програмних виправлень або оновлень продуктів, що може призвести до можливості для зловмисників використовувати слабкі місця в установлених компонентах. Винятки із заміни непідтримуваних компонентів системи включають системи, які забезпечують критично важливу місію або бізнес-можливості, де нові технології недоступні або де системи настільки ізольовані, що встановлення замінних компонентів

неможливе. Альтернативні джерела підтримки вирішують необхідність забезпечення постійної підтримки компонентів системи, які більше не підтримуються оригінальними виробниками, розробниками або постачальниками, коли такі компоненти залишаються важливими для місії організації та бізнес-функцій. Якщо необхідно, організації можуть створити внутрішню підтримку, розробивши налаштовані виправлення для критичних компонентів програмного забезпечення, або альтернативно отримати послуги зовнішніх постачальників, які надають постійну підтримку для визначених непідтримуваних компонентів через договірні відносини. Такі договірні відносини можуть включати постачальників програмного забезпечення з доданою вартістю і відкритим кодом. Підвищений ризик використання непідтримуваних компонентів системи можна зменшити, наприклад, заборонивши підключення таких компонентів до загальнодоступних чи неконтрольованих мереж або запровадивши інші форми ізоляції.

Пов'язані заходи: PL-2, SA-3.

Посилення заходів:

(1) КОМПОНЕНТИ СИСТЕМИ, ЩО НЕ ПІДТРИМУЮТЬСЯ - АЛЬТЕРНАТИВНІ ДЖЕРЕЛА ДЛЯ ПОСТІЙНОЇ ПІДТРИМКИ

[Вилучено: включено до SA-22].

Посилання: Немає.

## SA-23 СПЕЦІАЛІЗАЦІЯ

Заходи захисту: Покращення [*Вибір (один або кілька): проектування; модифікація; збільшення; реконфігурація*] на [*Призначення: системи або системні компоненти, визначені організацією*], які підтримують важливі служби або функції для підвищення надійності цих систем або компонентів.

Рекомендації з реалізації: Часто необхідно покращити систему або компонент системи, який підтримує важливі послуги або функції, щоб максимізувати надійність ресурсу. Іноді це вдосконалення виконується на рівні проектування. В інших випадках це робиться після проектування, або шляхом модифікації розглянутої системи, або шляхом доповнення системи додатковими компонентами. Наприклад, додаткові функції автентифікації або неспростування можуть бути додані до системи, щоб покращити ідентичність критичних ресурсів іншим ресурсам, які залежать від ресурсів, визначених організацією.

Пов'язані заходи: RA-9, SA-8.

Посилення заходів: Немає.

Посилання: [SP 800-160-1], [SP 800-160-2].

## 10.18 Клас заходів захисту SC — ЗАХИСТ ІНФОРМАЦІЙНОЇ СИСТЕМИ ТА КОМУНІКАЦІЙ

### SC-1 ПОЛІТИКА ТА ПРОЦЕДУРИ ЗАХИСТУ СИСТЕМИ ТА КОМУНІКАЦІЙ

Заходи захисту:

a. Розробити, задокументувати та поширити серед [*Призначення: визначеного організацією персоналу або посадових осіб*]:

   1. Політику захисту системи та комунікацій, яка:

      (a) містить мету, сферу застосування, ролі, обов'язки, відповідальність керівництва, координацію між організаційними підрозділами та систему контролю відповідності (complaince);

      (b) відповідає чинному законодавству, виконавчим наказам, директивам, нормам, політикам, стандартам та керівним принципам.

   2. Процедури для сприяння впровадженню політики в області захисту систем і комунікацій, а також пов'язаних з ними систем і засобів захисту зв'язку.

b. Призначити [*Призначення: визначена організацією посадову особу*] для управління політикою та процедурами захисту системи та комунікацій.

c. Переглядати та оновлювати:

   1. поточну політику захисту системи та комунікацій [*Призначення: визначена організацією частота*];

   2. поточні процедури захисту системи та комунікацій [*Призначення: визначена організацією частота*].

Рекомендації з реалізації: Цей захід захисту стосується встановлення політики та процедур для ефективного здійснення заходів та їх посилень у класі SC. Стратегія управління ризиками є важливим фактором у встановленні політики та процедур. Комплексна політика та процедури допомагають забезпечити безпеку та приватність. За наявності політики, а також планів захисту інформації та персональних даних на рівні організації, конкретні системні політики та процедури можуть бути не потрібні. Політика може бути внесена до складу загальної політики безпеки та приватності або може бути представлена кількома політиками (у випадках складної архітектури). Процедури описують, як має реалізуватися політика чи заходи захисту та як вони можуть бути спрямовані на персонал або роль, що є об'єктом процедури. Процедури можуть бути задокументовані в планах захисту інформації та персональних даних (як один або декілька документів).

Пов'язані заходи: PM-9, PS-8, SA-8, SI-12.

Посилення заходів: Немає.

Посилання: [OMB A-130], [SP 800-12], [SP 800-100].

### SC-2 РОЗДІЛЕННЯ ФУНКЦІЙ

Заходи захисту:
Розділяти функціональність користувача, включно зі службами, що призначені для користувача інтерфейсу, від функціональності системного управління.

Рекомендації з реалізації: До функціонала системного управління належать, наприклад, функції адміністрування баз даних, мережевих компонентів, робочих станцій або серверів. Для цих функцій зазвичай потрібен привілейований доступ користувача. Розділення функцій користувача від функцій управління системою має бути фізичним або логічним. Організації реалізують розділення функцій управління системою від функцій користувача, за допомогою: різних комп'ютерів, екземплярів операційних систем, центральних процесорних блоків або мережевих адрес; застосування методів віртуалізації; поєднання тих чи інших методів. Цей тип розподілу охоплює, наприклад, вебадміністративні інтерфейси, які використовують окремі методи автентифікації для користувачів будь-яких інших ресурсів системи. Розмежування функцій системи і користувача може містити ізоляцію адміністративних інтерфейсів у різних доменах з додатковими заходами захисту.

Пов'язані заходи: AC-6, SA-4, SA-8, SC-3, SC-7, SC-22, SC-32, SC-39.

Посилення заходів:

(1) РОЗДІЛЕННЯ ФУНКЦІЙ - ІНТЕРФЕЙСИ ДЛЯ НЕПРИВІЛЕЙОВАНИХ КОРИСТУВАЧІВ

Запобігати наданню функціональності системного управління в інтерфейсі для непривілейованих користувачів.

Рекомендації з реалізації: Запобігання представлення функціональності управління системою на інтерфейсах для непривілейованих користувачів гарантує, що можливості адміністрування системи, включно з привілеями адміністратора, не будуть доступними широкому загалу користувачів. Обмеження доступу користувачів також забороняє використання опції "сірого екрану", яка зазвичай використовується для усунення доступу до такої інформації. Одним із можливих рішень є приховування опцій системного адміністрування доти, доки користувачі не встановлять сеанси з правами адміністратора.

Пов'язані заходи: AC-3.

(2) РОЗДІЛЕННЯ ФУНКЦІЙ - ВІДОКРЕМЛЕННЯ

Зберігайте інформацію з додатків і програмного забезпечення окремо.

Рекомендації з реалізації: Якщо систему скомпрометовано, збереження додатків і програмного забезпечення окремо від інформації про взаємодію користувачів із додатком може краще захистити індивідуальну конфіденційність.

Пов'язані заходи: Немає.

Посилання: Немає.

## SC-3 ІЗОЛЯЦІЯ ФУНКЦІЙ БЕЗПЕКИ

Заходи захисту: Ізолювати функції безпеки від інших функцій.

Рекомендації з реалізації: Функції безпеки ізольовані від функцій, що не пов'язані з безпекою, за допомогою розділів і доменів в системі. Межа ізоляції контролює доступ і захищає цілісність апаратного та програмного забезпечення, яке виконує функції безпеки системи, а також захищає їх від несанкціонованого доступу. В ідеалі весь код в межах визначеної межі ізоляції функцій безпеки повинен містити лише код, що стосується безпеки, іноді як виняток необхідно включати функції, що не стосуються безпеки. Ізоляція функцій безпеки від функцій, що не стосуються безпеки, може бути досягнута шляхом застосування принципів проектування системної безпеки, викладених у SA-8, зокрема SA-8(1), SA-8(3), SA-8(4), SA-8(10), SA-8(12), SA-8(13), SA-8(14) та SA-8(18).

Пов’язані заходи: AC-3, AC-6, AC-25, CM-2, CM-4, SA-4, SA-5, SA-8, SA-15, SA-17, SC-2, SC-7, SC-32, SC-39, SI-16.

Посилення заходів:

(1) ІЗОЛЯЦІЯ ФУНКЦІЙ БЕЗПЕКИ - РОЗДІЛЕННЯ АПАРАТНОГО ЗАБЕЗПЕЧЕННЯ

Використовувати механізми розділення апаратних засобів для реалізації ізоляції функцій безпеки.

Рекомендації з реалізації: До механізмів розділення обладнання належать, наприклад, апаратні кільцеві архітектури, які зазвичай реалізуються в межах мікропроцесорів, і апаратно-застосовану сегментацію адрес, що використовується для підтримки логічно відмінних об’єктів зберігання з окремими атрибутами.

Пов’язані заходи: Немає.

(2) ІЗОЛЯЦІЯ ФУНКЦІЙ БЕЗПЕКИ - ФУНКЦІЇ УПРАВЛІННЯ ДОСТУПОМ ТА ПОТОКОМ

Ізолювати функції безпеки, що забезпечують управління доступом та інформаційним потоком від функцій, не пов’язаних з безпекою та інших функцій безпеки.

Рекомендації з реалізації: До функцій захисту, які мають бути ізольовані від функцій забезпечення контролю доступу та потоку, належать, наприклад, функції аудиту, виявлення вторгнень та антивірусні функції.

Пов’язані заходи: Немає.

(3) ІЗОЛЯЦІЯ ФУНКЦІЙ БЕЗПЕКИ - МІНІМІЗАЦІЯ ФУНКЦІОНАЛЬНОСТІ

Мінімізувати кількість функцій, не пов’язаних з безпекою, що входять до сфери ізоляції, яка містить функції безпеки.

Рекомендації з реалізації: Мінімізувати кількість функцій, не пов’язаних з безпекою, що входять до сфери ізоляції, яка містить функції безпеки. Фундаментальна мета проектування полягає в тому, щоб конкретні частини систем, які забезпечують інформаційну безпеку, були мінімального розміру та складності. Мінімізація кількості функцій, не пов'язаних з безпекою, у

компонентах системи, що мають відношення до безпеки компонентів системи дозволяє проектувальникам та реалізаторам зосередитись лише на тих функціях які необхідні для забезпечення бажаного рівня безпеки (як правило, це управління доступом).

(4) ІЗОЛЯЦІЯ ФУНКЦІЙ БЕЗПЕКИ - ЗВ'ЯЗОК МОДУЛІВ ТА З'ЄДНАННЯ

Впроваджувати функції безпеки здебільшого як незалежні модулі, що максимізують внутрішню зв'язність у модулях і мінімізують зв'язок між модулями.

Рекомендації з реалізації: Зменшення взаємодії між модулями допомагає обмежити функції безпеки та керувати складністю. Концепції зв'язування та з'єднання є важливими щодо модульності в розробці програмного забезпечення. Зв'язування стосується залежностей, які один модуль має від інших модулів. З'єднання стосується зв'язку між функціями в модулі. Найкращі практики в розробці програмного забезпечення та інженерії захисту систем покладаються на багатошаровість, мінімізацію та модульну декомпозицію для зменшення та управління складністю. Це виробляє модулі програмного забезпечення, які є з'єднаними та слабко пов'язаними.

Пов'язані заходи: Немає.

(5) ІЗОЛЯЦІЯ ФУНКЦІЙ БЕЗПЕКИ - БАГАТОРІВНЕВА СТРУКТУРА

Реалізувати функції безпеки як багаторівневу структуру, що мінімізує взаємодію між рівнями конструкції та уникає будь-якої залежності нижчих рівнів від функціональності або правильності вищих рівнів.

Рекомендації з реалізації: Реалізація багаторівневих структур із мінімізованою взаємодією між функціями безпеки та нециклічними рівнями (тобто функції нижчого рівня не залежать від функцій вищого рівня) дозволяє ізолювати функції безпеки та керувати складністю.

Пов'язані заходи: Немає.

Посилання: Немає.

## SC-4 ІНФОРМАЦІЯ В ЗАГАЛЬНИХ РЕСУРСАХ СИСТЕМИ

Заходи захисту:
Запобігати несанкціонованій та ненавмисній передачі інформації через спільні системні ресурси.

Рекомендації з реалізації: Цей захід захисту запобігає доступу до інформації для поточних користувачів або ролей (або поточних процесів, що діють від імені поточних користувачів або ролей), яка генерується діями попередніх користувачів або ролей (або діями процесів, що діють від імені попередніх користувачів або ролей). Цей захід безпеки також застосовується до зашифрованої інформації. Управління інформацією в загальних ресурсах системи називається повторним використанням об'єктів. Цей захід безпеки не стосується залишкової інформації.

Пов'язані заходи: AC-3, AC-4, SA-8.

Посилення заходів:

(1) ІНФОРМАЦІЯ В ЗАГАЛЬНИХ РЕСУРСАХ СИСТЕМИ - РІВНІ БЕЗПЕКИ

[Вилучено: включено до SC-4].

(2) ІНФОРМАЦІЯ В ЗАГАЛЬНИХ РЕСУРСАХ СИСТЕМИ - БАГАТОРІВНЕВА АБО ПЕРІОДИЧНА ОБРОБКА

Запобігати несанкціонованій передачі інформації через спільні ресурси відповідно до [*Призначення: визначених організацією процедур*], коли системна обробка явно перемикається між різними категоріями таємності інформації або категоріями безпеки.

Рекомендації з реалізації: Це посилення застосовується, коли є явні зміни в рівнях обробки інформації під час функціонування системи. Така ситуація може виникнути, наприклад, під час багаторівневої або періодичної обробки інформації з різними рівнями класифікації або категоріями безпеки. Визначені організацією процедури можуть охоплювати, наприклад, затверджені процеси «забілення».

Пов'язані заходи: Немає.

Посилання: Немає.

## SC-5 ЗАХИСТ ВІД АТАК «ВІДМОВА В ОБСЛУГОВУВАННІ»

Заходи захисту:

a. [*Призначення: захистити від; Обмежити*] наслідки наступних типів подій відмови в обслуговуванні (DoS): [*Призначення: визначені організацією типи подій відмови в обслуговуванні*];

b. Застосувати наступні заходи захисту для досягнення мети відмови обслуговування [*Призначення: заходи захисту визначені організацією, за типом події відмови в обслуговуванні*].

Рекомендації з реалізації: «Відмова в обслуговувані» може статися через атаку порушника або відсутність внутрішнього планування для підтримки потреб організації щодо потужності та пропускної здатності. Є безліч технологій для обмеження або усунення наслідків подій «відмови в обслуговуванні». Наприклад, пристрої захисту можуть фільтрувати певні типи пакетів для забезпечення захисту компонентів системи у внутрішніх мережах від прямого впливу «відмови в обслуговуванні». Використання збільшеної пропускної спроможності мережі та пропускної спроможності в поєднанні з надмірністю послуг також зменшує сприйнятливість до «відмови в обслуговуванні».

Пов'язані заходи: CP-2, IR-4, SC-6, SC-7, SC-40.

Посилення заходів:

(1) ЗАХИСТ ВІД АТАК «ВІДМОВА В ОБСЛУГОВУВАННІ» - ОБМЕЖЕННЯ ВНУТРІШНІХ КОРИСТУВАЧІВ

Обмежити здатність осіб запускати [*Призначення: визначені організацією атаки на відмову в обслуговуванні*] проти інших систем.

Рекомендації з реалізації: Обмеження можливостей окремих осіб здійснювати атаки на відмову в обслуговуванні вимагає щоб механізми, які зазвичай використовуються для таких атак, були недоступні. До таких осіб належать вороже налаштовані інсайдери або зовнішні супротивники, які зламали або скомпрометували систему і використовують її для здійснення атаки на відмову в обслуговуванні. Організації можуть обмежити можливість окремих осіб підключатися та передавати довільну інформацію через транспортний носій (наприклад, дротові мережі, бездротові мережі, підроблені пакети інтернет-протоколу). Організації також можуть обмежити можливість окремих осіб використовувати надмірні системні ресурси. Захист від окремих осіб, які можуть здійснювати атаки на відмову в обслуговуванні, може бути реалізований на конкретних системах або граничних пристроях, які забороняють вихід до потенційних систем-цілей.

Пов’язані заходи: Немає.

(2) ЗАХИСТ ВІД АТАК «ВІДМОВА В ОБСЛУГОВУВАННІ» - ПРОДУКТИВНІСТЬ, ПРОПУСКНА ЗДАТНІСТЬ ТА НАДМІРНІСТЬ

Управляти продуктивністю, пропускною здатністю або іншою надмірністю для обмеження наслідків атак «відмова в обслуговуванні».

Рекомендації з реалізації: Керування потужністю гарантує наявність достатньої потужності для протидії атакам затоплення. Керування потужністю включає встановлення вибраних пріоритетів використання, квот, розподіл або балансування навантаження.

Пов’язані заходи: Немає.

(3) ЗАХИСТ ВІД АТАК «ВІДМОВА В ОБСЛУГОВУВАННІ» - ВИЯВЛЕННЯ ТА МОНІТОРИНГ

(a) Використовувати [*Призначення: визначені організацією засоби моніторингу*] для виявлення показників атаки «відмова в обслуговуванні» системи.

(b) Проводити моніторинг [*Призначення: визначених організацією ресурсів системи*], щоб визначити, чи наявні ресурси є достатніми для запобігання ефективним атакам «відмова в обслуговуванні».

Рекомендації з реалізації: Організації враховують використання та потужність ресурсів системи під час управління ризиками, пов'язаними з відмовою в обслуговуванні через зловмисні атаки. Відмова в обслуговуванні можуть походити із зовнішніх або внутрішніх джерел. Системні ресурси, які є чутливими до відмови в обслуговуванні включають фізичне сховище на диску, пам'ять і цикли процесора. Методи, що використовуються для запобігання атакам на використання та ємність сховища, пов'язаних з відмовою в обслуговуванні, включають встановлення дискових квот, налаштування систем на автоматичне сповіщення адміністраторів, коли досягнення певних порогових значень ємності сховища, використання технологій стиснення файлів для максимізації доступного місця в сховищі, а також створення окремих розділів для даних системи і користувача.

Пов’язані заходи: CA-7, SI-4.

Посилання: [SP 800-189].

## SC-6 ДОСТУПНІСТЬ РЕСУРСІВ

Заходи захисту:

Забезпечити захист доступності ресурсів, виділивши [*Призначення: визначені організацією ресурси*], по [*Вибір (один або кілька); пріоритет; квоти; [Призначення: визначені організацією заходи з безпеки*]].

Рекомендації з реалізації: Захист пріоритетів запобігає затримці процесів з низьким пріоритетом або втручанню їх у систему, що обслуговує процеси більш високого пріоритету. Квоти заважають користувачам або процесам отримувати більше заздалегідь визначених обсягів ресурсів. Цей захід безпеки не застосовується до компонентів системи, для яких є лише окремі користувачі або ролі.

Пов’язані заходи: SC-5.

Посилення заходів: Немає.

Посилання: [OMB M-08-05], [DHS TIC].

## SC-7 ЗАХИСТ ПЕРИМЕТРА

Заходи захисту:

a. Контролювати та управляти зв’язком на зовнішньому периметрі системи та на ключових внутрішніх периметрах всередині системи.

b. Реалізувати підмережі для загальнодоступних компонентів системи, які є [*Вибір: фізично; логічно*] відділені від внутрішніх мереж організації.

c. Підключатися до зовнішніх мереж або систем тільки через керовані інтерфейси, що складаються з пристроїв захисту периметру, і розташованих відповідно до архітектури безпеки та приватності організації.

Рекомендації з реалізації: До керованих інтерфейсів належать, наприклад, шлюзи, маршрутизатори, міжмережеві екрани, захисні пристрої, процедури аналізу шкідливого коду, зашифровані тунелі, що реалізовані в архітектурі безпеки. Підмережі, які фізично або логічно відокремлені від внутрішніх мереж, називаються демілітаризованими зонами. Обмеження або заборона інтерфейсів в системах організації містить, наприклад, обмеження зовнішнього вебтрафіку на призначених вебсерверах у межах керованих інтерфейсів. Комерційні послуги зв’язку зазвичай надаються мережевими компонентами та консолідованими системами управління. Такі послуги можуть становити джерела підвищеного ризику. [SP 800-189] надає додаткову інформацію про методи перевірки адреси джерела для запобігання вхідному та вихідному трафіку з підробленими адресами. Захист периметру може бути реалізований як загальний захід захисту для всієї мережі організації або її частини, щоб периметр, який потрібно захистити, був більшим, ніж межа певної системи (тобто межа авторизації).

Пов’язані заходи: AC-4, AC-17, AC-18, AC-19, AC-20, AU-13, CA-3, CM-2, CM-4, CM-7, CM-10, CP-8, CP-10, IR-4, MA-4, PE-3, PL-8, SA-8, SA-17, PM-12, SC-5, SC-32,

SC-35, SC-43.

Посилення заходів:

(1) ЗАХИСТ ПЕРИМЕТРА - ФІЗИЧНО ВІДДІЛЕНІ ПІДМЕРЕЖІ

[Вилучено: Включено до SC-7].

(2) ЗАХИСТ ПЕРИМЕТРА - ПУБЛІЧНИЙ ДОСТУП

[Вилучено: Включено до SC-7].

(3) ЗАХИСТ ПЕРИМЕТРА - ТОЧКИ ДОСТУПУ

Обмежити кількість зовнішніх мережевих підключень до системи.

Рекомендації з реалізації: Обмеження кількості зовнішніх мережевих підключень полегшує моніторинг вхідного та вихідного комунікаційного трафіку. Довірені інтернет з'єднання (Trusted Internet Connection)[DHS TIC] є прикладом директиви, яка вимагає обмеження кількості зовнішніх мережевих з'єднань. Обмеження кількості зовнішніх мережевих підключень до системи важливо під час перехідних періодів від старих до нових технологій (наприклад, під час переходу від мережевих протоколів IPv4 до IPv6). Такі переходи можуть вимагати одночасного впровадження старої і новіших технологій одночасно протягом перехідного періоду і, таким чином, збільшити кількість точок доступу до системи.

Пов'язані заходи: Немає.

(4) ЗАХИСТ ПЕРИМЕТРА - ЗОВНІШНІ КОМУНІКАЦІЙНІ СЛУЖБИ

(a) Запровадити керований інтерфейс для кожної зовнішньої комунікаційної служби.

(b) Створити політику управління трафіком для кожного керованого інтерфейсу.

(c) Забезпечити конфіденційність та цілісність інформації, що передається через кожний інтерфейс.

(d) Документувати кожне виключення з політики управління трафіком за допомогою підтримки завдань / потреби та тривалості цієї потреби.

(e) Переглянути виключення з політики управління трафіком [*Призначення: визначення організацією частота*] та видалити виключання, які більше не явно підтримуються цілями.

(f) Запобігти несанкціонованому обміну трафіком управління із зовнішніми мережами;

(g) Публікувати інформацію, щоб дозволити віддаленим мережам виявляти несанкціонований трафік керування з внутрішніх мереж;

(h) Фільтрувати несанкціонований трафік керування із зовнішніх мереж.

Рекомендації з реалізації: Зовнішні комунікаційні служби можуть надавати послуги передачі даних та/або голосові послуги зв'язку. Дивіться [SP 800-189] для отримання додаткової інформації про використання інфраструктури відкритих ключів (RPKI) для захисту маршрутів BGP та виявлення несанкціонованих оголошень BGP.

Пов’язані заходи: AC-3, SC-8, SC-20, SC-21, SC-22.

(5) ЗАХИСТ ПЕРИМЕТРА - ВІДМОВА ЗА ЗАМОВЧУВАННЯМ — ДОЗВІЛ ЗА ВИНЯТКОМ

Заборонити за умовчанням трафік мережевого зв’язку та дозволити трафік мережевого зв’язку за винятком [*Вибір (один або кілька): керованих інтерфейсів; для [Призначення: системи, визначені організацією*]].

Рекомендації з реалізації: Відмова за замовчуванням і дозвіл за винятком застосовуються до вхідного та вихідного мережевого трафіку. Політика мережевого трафіку зв’язку «заборона всього» гарантує, що дозволено лише ті підключення до системи, які є важливими та схваленими. За замовчуванням заборонити та дозволити за винятком також застосовується до системи, підключеної до зовнішньої система.

Пов’язані заходи: Немає.

(6) ЗАХИСТ ПЕРИМЕТРА - ВІДПОВІДЬ НА РОЗПІЗНАНІ ПОМИЛКИ

[Вилучено: Включено до SC-7(18)].

(7) ЗАХИСТ ПЕРИМЕТРА - ЗАПОБІГАННЯ ПОДІЛУ ТУНЕЛЮВАННЯ ДЛЯ ВІДДАЛЕНИХ ПРИСТРОЇВ

Запобігати розділеному тунелюванню для віддалених пристроїв, які підключаються до систем організації, якщо розділений тунель не убезпечений за допомогою [*Призначення: визначені організацією заходи безпеки*].

Рекомендації з реалізації: Розділене тунелювання — це процес, який дозволяє віддаленому користувачеві або пристрою встановлювати з’єднання із системою та одночасно спілкуватися через якесь інше з’єднання з ресурсом у зовнішній мережі. Цей спосіб доступу до мережі дозволяє користувачеві отримувати доступ до віддалених пристроїв і одночасно до неконтрольованих мереж. Розділене тунелювання може бути зручним віддаленим користувачам для зв’язку з локальними системними ресурсами, такими як принтери або файлові сервери. Однак воно може сприяти неавторизованим зовнішнім підключенням, роблячи систему вразливою до атак і викрадання інформації. Розділеному тунелюванню можна запобігти, вимкнувши параметри конфігурації, які дозволяють таку можливість у віддалених пристроях, і запобігши можливостям налаштування цих параметрів конфігурації користувачами. Запобігання також можна досягти шляхом виявлення розділеного тунелювання (або параметрів конфігурації, які дозволяють розділене тунелювання) у віддаленому пристрої та шляхом заборони підключення, якщо віддалений пристрій використовує розділене тунелювання. Також, можна використовувати віртуальну приватну мережу (VPN) для безпечного надання розділеного тунелю. Безпечно налаштована VPN включає блокування з’єднання з ексклюзивними, керованими та названими середовищами або з певним набором попередньо затверджених

адрес без контролю користувача.

Пов’язані заходи: Немає.

(8) ЗАХИСТ ПЕРИМЕТРА - МАРШРУТИЗАЦІЯ ТРАФІКУ З АВТЕНТИФІКОВАНИХ ПРОКСІ-СЕРВЕРІВ

Здійснювати маршрутизацію [*Призначення: визначений організацією внутрішній трафік комунікацій*] до [*Призначення: визначені організацією зовнішні мережі*] через автентифіковані проксі-сервери на керованих інтерфейсах.

Рекомендації з реалізації: Зовнішні мережі — це мережі поза контролем організації. Проксі-сервер — це сервер (тобто система або додаток), який діє як посередник для клієнтів, які запитують системні ресурси від серверів в організації або зовнішніх серверів. Системні ресурси, які можуть запитуватися, включають файли, підключення, вебсторінки або служби. Запити клієнта, створені через підключення до проксі-сервера, оцінюються для управління складністю та забезпечення додаткового захисту шляхом обмеження прямого підключення. Пристрої фільтрації вебвмісту є одними з найпоширеніших проксі-серверів, які надають доступ до Інтернету. Проксі-сервери можуть підтримувати реєстрацію сеансів протоколу керування передачею та блокування певних уніфікованих локаторів ресурсів, адрес Інтернет-протоколу та доменних імен. Веб-проксі можна налаштувати за допомогою визначених організацією списків авторизованих і неавторизованих вебсайтів. Зауважте, що проксі-сервери можуть перешкоджати використанню віртуальних приватних мереж (VPN) і створювати потенціал для атак «людина посередині» (залежно від реалізації).

Пов’язані заходи: AC-3.

(9) ЗАХИСТ ПЕРИМЕТРА - ОБМЕЖЕННЯ ТРАФІКУ ВИХІДНИХ ПОВІДОМЛЕНЬ

(a) Виявляти та забороняти вихідний трафік зв’язку, що створює загрозу для зовнішніх систем.

(b) Проводити аудит ідентичності внутрішніх користувачів, пов’язаних з відмовою у зв’язку.

Рекомендації з реалізації: Виявлення вихідного комунікаційного трафіку через внутрішні дії, які можуть становити загрозу зовнішнім системам, називається виявленням екструзії. Виявлення екструзії здійснюється в системі на керованих інтерфейсах. Виявлення екструзії включає аналіз вхідного та вихідного трафіку зв’язку під час пошуку ознак внутрішніх загроз безпеці зовнішніх систем. Внутрішні загрози для зовнішніх систем включають трафік, що вказує на атаки на відмову в обслуговуванні, трафік із підробленими адресами джерела та трафік, який містить шкідливий код. Організації мають критерії для визначення, оновлення та керування виявленими загрозами, пов’язаними з виявленням екструзії.

Пов’язані заходи: AU-2, AU-6, SC-5, SC-38, SC-44, SI-3, SI-4.

(10) ЗАХИСТ ПЕРИМЕТРА - ЗАПОБІГАННЯ ЕКСФІЛЬТРАЦІЇ

(a) Запобігати ексфільтрації інформації.

(b) Проводити тести на ексфільтрацію [*Призначення: визначена організацією частота*].

Рекомендації з реалізації: Запобігання витоку інформації стосується як навмисного, так і ненавмисного витоку інформації. Методи, що використовуються для запобігання витоку інформації з систем можуть бути реалізовані на внутрішніх та зовнішніх кінцевих пристораях і через керовані інтерфейси. Вони включають дотримання форматів протоколів, моніторинг маячків активності систем, відключення зовнішніх мережевих інтерфейсів, за винятком випадків, коли це явно необхідно, використання аналізу профілю трафіку для виявлення відхилень від очікуваного обсягу та типів аналіз профілю трафіку для виявлення відхилень від очікуваного обсягу та типів трафіку, зворотні дзвінки в командно-контрольні центри, проведення тестування на проникнення, моніторинг на предмет стеганографії, розбирання та збирання заголовків пакетів, використання засоби запобігання втраті та витоку даних. Пристрої, які забезпечують суворе дотримання форматів протоколів, включають брандмауери з глибокою перевіркою пакетів і шлюзи розширюваної мови розмітки (XML) шлюзи. Пристрої перевіряють дотримання форматів і специфікацій протоколів на рівні додатків і виявляють вразливості, які не можуть бути виявлені пристроями, що працюють на мережевому або транспортному рівнях. Запобігання витоку схоже на запобігання втраті даних або запобігання витоку даних і тісно пов'язане з міждоменними рішеннями та системними засобами.

Пов’язані заходи: SI-3, AC-2, CA-8.

(11) ЗАХИСТ ПЕРИМЕТРА - ОБМЕЖЕННЯ ТРАФІКУ ВХІДНИХ ПОВІДОМЛЕНЬ

Дозволяти вхідні повідомлення лише від [*Призначення: визначені організацією авторизовані джерела*] та направляти їх до [*Призначення: визначені організацією визначені місця призначення*].

Рекомендації з реалізації: Загальні методи перевірки адреси джерела застосовуються для обмеження використання незаконних і нерозподілених адрес, а також адрес, які слід використовувати лише в системі. Обмеження вхідного трафіку зв’язку забезпечує визначення того, що пари адрес джерела та призначення представляють авторизовані або дозволені зв’язки. Визначення можуть ґрунтуватися на кількох факторах, включаючи наявність таких пар адрес у списках авторизованих або дозволених комунікацій, відсутність таких пар адрес у списках неавторизованих або заборонених пар або дотримання більш загальних правил щодо авторизованого чи дозволеного джерела та призначення пари. Надійна автентифікація мережевих адрес неможлива без використання явних протоколів безпеки, тому адреси часто можуть бути підробленими. Крім того, можна використовувати методи обмеження вхідного трафіку на основі ідентичності, включаючи списки контролю доступу маршрутизатора та правила брандмауера.

Пов’язані заходи: AC-3.

(12) ЗАХИСТ ПЕРИМЕТРА - ЗАХИСТ НА ОСНОВІ ХОСТУ

Реалізувати [*Призначення: визначені організацією механізми захисту периметру на основі хосту*] в [*Призначення: визначені організацією компоненти системи*].

Рекомендації з реалізації: Механізми захисту периметра на основі хосту включають брандмауери на основі хоста. Компоненти системи, які використовують механізми захисту меж хоста, включають сервери, робочі станції, ноутбуки та мобільні пристрої.

Пов'язані заходи: Немає.

(13) ЗАХИСТ ПЕРИМЕТРА - ІЗОЛЯЦІЯ ЗАСОБІВ БЕЗПЕКИ, МЕХАНІЗМІВ І КОМПОНЕНТІВ ПІДТРИМКИ

Ізолювати [*Призначення: визначені організацією засоби, механізми та компоненти підтримки, пов'язані з інформаційною безпекою*] від інших внутрішніх компонентів системи шляхом реалізації фізично окремих підмереж з керованими інтерфейсами з іншими компонентами системи.

Рекомендації з реалізації: Фізично відокремлені підмережі з керованими інтерфейсами корисні для ізоляції засобів захисту комп'ютерної мережі від критично важливих операційних мереж обробки, щоб запобігти виявленню зловмисниками методів аналізу та криміналістики, які застосовуються організаціями.

Пов'язані заходи: SC-2, SC-3.

(14) ЗАХИСТ ПЕРИМЕТРА - ЗАХИСТ ВІД НЕСАНКЦІОНОВАНИХ ФІЗИЧНИХ З'ЄДНАНЬ

Забезпечити захист від несанкціонованих фізичних з'єднань через [*Призначення: визначені організацією керовані інтерфейси*].

Рекомендації з реалізації: Системи, які працюють з різними категоріями безпеки або рівнями класифікації, можуть використовувати загальні фізичні та організаційні заходи захисту, оскільки системи можуть спільно використовувати простір в межах одних і тих самих об'єктів. На практиці можливо, що ці окремі системи можуть мати спільні кімнати для обладнання, шафи для електропроводки та шляхи розподілу кабелів. Захист від несанкціонованих фізичних підключень можна досягти за допомогою чітко визначених і фізично розділених кабельних лотків, з'єднувальних рамок і коммутаційних панелей для кожної сторони керованих інтерфейсів із засобами контролю фізичного доступу, які забезпечують обмежений авторизований доступ до цих елементів.

Пов'язані заходи: PE-4, PE-19.

(15) ЗАХИСТ ПЕРИМЕТРА - МАРШРУТИЗАЦІЯ ДОСТУПУ ДО ПРИВІЛЕЙОВАНОЇ МЕРЕЖІ

Здійснювати маршрутизацію всього мережевого привілейованого доступу через спеціальний керований інтерфейс у цілях управління доступом та аудиту.

Рекомендації з реалізації: Привілейований доступ забезпечує кращий доступ до функцій системи, включаючи функції безпеки. Зловмисники намагаються отримати привілейований доступ до систем за допомогою віддаленого доступу, щоб спричинити несприятливий вплив на місію чи бізнес, наприклад, шляхом викрадання інформації або виведення з ладу критично важливої можливості

системи. Маршрутизація мережевих запитів привілейованого доступу через виділений керований інтерфейс ще більше обмежує привілейований доступ для покращення контролю та аудиту доступу.

Пов'язані заходи: AC-2, AC-3, AU-2, SI-4.

(16) ЗАХИСТ ПЕРИМЕТРА - ЗАПОБІГАННЯ ВИЯВЛЕННЮ КОМПОНЕНТІВ І ПРИСТРОЇВ

Запобігати виявленню конкретних компонентів системи, які представляють керований інтерфейс.

Рекомендації з реалізації: Запобігання виявленню компонентів системи, що представляють керований інтерфейс, допомагає захистити мережеві адреси цих компонентів від виявлення за допомогою звичайних інструментів і методів, які використовуються для ідентифікації пристроїв у мережах. Мережні адреси недоступні для виявлення, тому для доступу до них потрібні попередні знання. Запобігти виявленню компонентів і пристроїв можна, не публікуючи мережеві адреси, використовуючи трансляцію мережевих адрес або не вводячи адреси в системи доменних імен. Ще один спосіб запобігання — періодична зміна мережевих адрес.

Пов'язані заходи: Немає.

(17) ЗАХИСТ ПЕРИМЕТРА - АВТОМАТИЧНЕ ПРИМУСОВЕ ВИКОНАННЯ ФОРМАТІВ ПРОТОКОЛІВ

Дотримуватися форматів протоколів.

Рекомендації з реалізації: Компоненти системи, які забезпечують дотримання форматів протоколів, включають брандмауери для глибокої перевірки пакетів і шлюзи XML. Компоненти перевіряють дотримання форматів протоколів і специфікацій на прикладному рівні та виявляють уразливості, які не можуть бути виявлені пристроями, що працюють на мережевому або транспортному рівнях.

Пов'язані заходи: SC-4.

(18) ЗАХИСТ ПЕРИМЕТРА - ЗБІЙ У БЕЗПЕЦІ

Запобігати входу систем у незахищені стани в разі аварійного завершення роботи пристрою захисту периметра.

Рекомендації з реалізації: Захищеність від збоїв — це умова, яка досягається за допомогою механізмів, які гарантують, що у випадку операційних збоїв пристроїв захисту периметра на керованих інтерфейсах системи не переходять у незахищений стан, де призначені властивості безпеки більше не зберігаються. Керовані інтерфейси включають маршрутизатори, брандмауери та шлюзи програм, які знаходяться в захищених підмережах (зазвичай їх називають демілітаризованими зонами). Збої пристроїв захисту периметра не можуть призвести до або спричинити надходження зовнішньої по відношенню до пристроїв інформації до пристроїв, а також збої не можуть дозволити несанкціонований розповсюдження інформації.

Пов'язані заходи: CP-2, CP-12, SC-24.

(19) ЗАХИСТ ПЕРИМЕТРА - БЛОКУВАННЯ КОМУНІКАЦІЇ ВІД ХОСТІВ, ЩО НАЛАШТОВАНІ ПОЗА ОРГАНІЗАЦІЄЮ

Блокувати трафік вхідних та вихідних повідомлень між [*Призначення: визначені організацією клієнти комунікацій*], які незалежно налаштовуються кінцевими користувачами та зовнішніми постачальниками послуг.

Рекомендації з реалізації: Комунікаційні клієнти, незалежно налаштовані кінцевими користувачами та зовнішніми постачальниками послуг, включають клієнти обміну миттєвими повідомленнями, програмне забезпечення та програми для відеоконференцій. Блокування трафіку не поширюється на комунікаційні клієнти, налаштовані організаціями для виконання авторизованих функцій.

Пов'язані заходи: Немає.

(20) ЗАХИСТ ПЕРИМЕТРА - ДИНАМІЧНА ІЗОЛЯЦІЯ ТА ВІДОКРЕМЛЕННЯ

Надавати можливість динамічно ізолювати або відокремлювати [*Призначення: визначені організацією системні компоненти*] від інших компонентів системи.

Рекомендації з реалізації: Можливість динамічної ізоляції певних внутрішніх компонентів системи корисна, коли необхідно розділити або відокремити системні компоненти сумнівного походження від компонентів, які мають більшу надійність. Ізоляція компонентів зменшує поверхню атаки систем організації. Ізоляція вибраних компонентів системи також може обмежити шкоду від успішних атак, коли такі атаки відбуваються.

Пов'язані заходи: Немає.

(21) ЗАХИСТ ПЕРИМЕТРА - ІЗОЛЯЦІЯ КОМПОНЕНТІВ СИСТЕМИ

Впровадити механізми захисту периметра, щоб відокремити [*Призначення: визначений організацією компонент системи*], що підтримує [*Призначення: визначені організацією цілі та/або функції*].

Рекомендації з реалізації: Організації можуть ізолювати компоненти системи, які виконують різні місії або бізнес-функції. Така ізоляція обмежує несанкціоновані потоки інформації між системними компонентами та дає можливість забезпечувати вищий рівень захисту для вибраних компонентів системи. Ізоляція компонентів системи за допомогою механізмів захисту периметра забезпечує можливість посилення захисту окремих компонентів системи та ефективнішого контролю потоків інформації між цими компонентами. Ізоляція компонентів системи забезпечує посилений захист, який обмежує потенційну шкоду від ворожих кібератак і помилок. Ступінь ізоляції змінюється залежно від обраних механізмів. Механізми захисту кордонів включають маршрутизатори, шлюзи та брандмауери, які розділяють компоненти системи на фізично окремі мережі або підмережі; міждоменні пристрої, що розділяють підмережі; методи віртуалізації; і шифрування потоків інформації між компонентами системи за допомогою різних ключів шифрування

Пов'язані заходи: CA-9.

(22) ЗАХИСТ ПЕРИМЕТРА - ОКРЕМІ ПІДМЕРЕЖІ ДЛЯ ПІДКЛЮЧЕННЯ ДО РІЗНИХ ДОМЕНІВ БЕЗПЕКИ

Реалізувати окремі мережні адреси для підключення до систем у різних доменах безпеки.

Рекомендації з реалізації: Розмежування систем на окремі підмережі допомагає забезпечити відповідний рівень захисту мережевих з'єднань із різними доменами безпеки, які містять інформацію з різними категоріями безпеки або рівнями класифікації.

Пов'язані заходи: Немає.

(23) ЗАХИСТ ПЕРИМЕТРА - ВІДКЛЮЧЕННЯ ФУНКЦІЇ ЗВОРОТНОГО ЗВ'ЯЗКУ ВІДПРАВНИКА ПРО ПОМИЛКУ ПЕРЕВІРКИ ПРОТОКОЛУ

Відключити зворотній зв'язок з відправниками при збої перевірки формату протоколу.

Рекомендації з реалізації: Вимкнення зворотного зв'язку з відправниками у разі помилки у форматі перевірки протоколу запобігає зловмисникам отримання інформації, яка інакше була б недоступна.

Пов'язані заходи: Немає.

(24) ЗАХИСТ ПЕРИМЕТРА - ПЕРСОНАЛЬНІ ДАНІ

Для систем, які обробляють, зберігають або передають персональні дані:

(a) Застосовувати [*Призначення: визначені організацією правила обробки*] до елементів персональних даних.

(b) Проводити контроль за дозволеною обробкою даних на зовнішньому периметрі системи та на ключових внутрішніх периметрах у системі.

(c) Документувати кожне виключення при обробці.

(d) Переглядати та видаляти винятки, які більше не підтримуються.

Рекомендації з реалізації: Управління обробкою персональних даних є важливим аспектом захисту приватності особи. Застосування, моніторинг та документування винятки з правил обробки гарантують, що особиста інформація обробляється тільки відповідно до встановлених вимог конфіденційності.

Пов'язані заходи: SI-15, PT-2.

(25) ЗАХИСТ ПЕРИМЕТРА - З'ЄДНАННЯ З НЕСЕКРЕТНИМИ НАЦІОНАЛЬНИМИ СИСТЕМАМИ БЕЗПЕКИ

Заборонити пряме підключення [*Призначення: визначена організацією несекретна система національної безпеки*] до зовнішньої мережі без використання [*Призначення: визначений організацією пристрій захисту кордонів*].

Рекомендації з реалізації: Пряме з'єднання – це виділене фізичне або віртуальне з'єднання між двома чи більше системами. Організації зазвичай не мають

повного контролю над зовнішніми мережами, включно з Інтернетом. Пристрої захисту кордонів (наприклад, брандмауери, шлюзи та маршрутизатори) забезпечують комунікації та потоки інформації між некласифікованими системами національної безпеки та зовнішніми мережами.

Пов'язані заходи: Немає.

(26) ЗАХИСТ ПЕРИМЕТРА - ЗЄДНАННЯ З СЕКРЕТНИМИ НАЦІОНАЛЬНИМИ СИСТЕМАМИ БЕЗПЕКИ

Заборонити пряме підключення секретної системи національної безпеки до зовнішньої мережі без використання [*Призначення: пристрій захисту кордонів, визначений організацією*].

Рекомендації з реалізації: Пряме з'єднання – це виділене фізичне або віртуальне з'єднання між двома чи більше системами. Зазвичай організації не мають повного контролю над зовнішніми мережами, включаючи Інтернет. Пристрої захисту кордонів (наприклад, брандмауери, шлюзи та маршрутизатори) забезпечують передачу даних та потоки інформації між секретними системами національної безпеки та зовнішніми мережами. Крім того, перевірені пристрої захисту кордонів (зазвичай керований інтерфейс або міждоменні системи) забезпечують примусовий контроль потоку інформації від систем до зовнішніх мереж.

Пов'язані заходи: Немає.

(27) ЗАХИСТ ПЕРИМЕТРА - ЗЄДНАННЯ З СЕКРЕТНИМИ НЕ НАЦІОНАЛЬНИМИ СИСТЕМАМИ БЕЗПЕКИ

Заборонити пряме підключення [*Призначення: визначена організацією несекретна не національна система безпеки*] до зовнішньої мережі без використання [*Призначення: визначений організацією пристрій захисту кордонів*].

Рекомендації з реалізації: Пряме з'єднання – це виділене фізичне або віртуальне з'єднання між двома чи більше системами. Організації зазвичай не мають повного контролю над зовнішніми мережами, включно з Інтернетом. Пристрої захисту кордонів (наприклад, брандмауери, шлюзи та маршрутизатори) забезпечують передачу даних та потоки інформації між некласифікованими не національними системами безпеки та зовнішніми мережами.

Пов'язані заходи: Немає.

(28) ЗАХИСТ ПЕРИМЕТРА - ЗЄДНАННЯ З ЗАГАЛЬНОДОСТУПНИМИ МЕРЕЖАМИ

Заборонити пряме підключення [*Призначення: система, визначена організацією*] до загальнодоступної мережі.

Рекомендації з реалізації: Пряме з'єднання – це виділене фізичне або віртуальне з'єднання між двома чи більше системами. Загальнодоступна мережа — це загальнодоступна мережа, включаючи Інтернет та організаційні корпоративні мережі з публічним доступом.

Пов'язані заходи: Немає.

(29) ЗАХИСТ ПЕРИМЕТРА - ОКРЕМІ ПІДМЕРЕЖІ ДЛЯ ІЗОЛЯЦІЇ ФУНКЦІЙ

Реалізувати [*Вибір: фізично; логічно*] розділені підмережі для ізоляції наступних критичних компонентів системи і функцій: [*Призначення: визначені організацією критичні системні компоненти та функції*].

Рекомендації з реалізації: Відокремлення критичних компонентів системи і функцій від інших некритичних компонентів системи і функцій через окремі підмережі може бути необхідне для зменшення катастрофічних порушень чи компрометації, що призводять до збоїв системи. Наприклад, фізичне відокремлення командно-контрольної функції від розважальної під час польоту через окремі підмережі забезпечує підвищений рівень надійності критичних функцій системи.

Пов'язані заходи: Немає.

Посилання: [OMB A-130], [FIPS 199], [SP 800-37], [SP 800-41], [SP 800-77], [SP 800-189].

## SC-8 КОНФІДЕНЦІЙНІСТЬ ТА ЦІЛІСНІСТЬ ПЕРЕДАЧІ

Заходи захисту:

Забезпечити [*Вибір (один або кілька): конфіденційність; цілісність*] інформації, що передається.

Рекомендації з реалізації: Цей захід захисту застосовується до внутрішніх і зовнішніх мереж та будь-яких компонентів системи, які можуть передавати інформацію, включно з, наприклад, серверами, ноутбуками, персональними комп'ютерами, мобільними пристроями, принтерами, копіювальними пристроями, сканерами. Інформація, яка передається по незахищених каналах зв'язку може бути перехоплена або модифікована. Захист конфіденційності та цілісності інформації може здійснюватися фізичними або логічними засобами. Фізичний захист може бути досягнуто за допомогою захищених систем розподілу. Логічний захист може бути досягнуто за допомогою методів шифрування. Організаціям, що покладаються на комерційних постачальників послуг, що пропонують послуги передачі як товарні послуги, а не як повністю спеціалізовані послуги, може бути важко отримати необхідні гарантії щодо здійснення необхідних заходів безпеки для забезпечення конфіденційності та цілісності передачі. У таких ситуаціях організації визначають, які види послуг конфіденційності, цілісності та доступності в стандартних комерційних пакетах послуг комунікацій необхідно забезпечувати. Якщо неможливо або недоцільно отримати необхідний захід безпеки та гарантії ефективності за допомогою відповідних транспортних засобів, організації можуть впроваджувати відповідні компенсаційні заходи безпеки або явно прийняти додатковий ризик.

Пов'язані заходи: AC-17, AC-18, AU-10, IA-3, IA-8, IA-9, MA-4, PE-4, SA-4, SA-8, SC-7, SC-16, SC-20, SC-23, SC-28.

Посилення заходів:

(1) КОНФІДЕНЦІЙНІСТЬ ТА ЦІЛІСНІСТЬ ПЕРЕДАЧІ - КРИПТОГРАФІЧНИЙ ЗАХИСТ

Реалізувати механізми криптографічного захисту для [*Вибір (один або більше): запобігання несанкціонованому розкриттю інформації; вияву зміни в*

*інформації*] під час передачі.

Рекомендації з реалізації: Шифрування захищає інформацію від несанкціонованого розкриття та модифікації під час передачі. Криптографічні механізми, які захищають конфіденційність і цілісність інформації під час передачі, є TLS та IPSec. Криптографічні механізми, що використовуються для захисту цілісності інформації включають криптографічні геш-функції, які застосовуються в цифрових підписів, контрольних сум і кодів автентифікації повідомлень.

Пов'язані заходи: SC-12, SC-13.

(2) КОНФІДЕНЦІЙНІСТЬ ТА ЦІЛІСНІСТЬ ПЕРЕДАЧІ - ПОПЕРЕДНЯ І ПОСТОБРОБКА

Підтримувати [*Вибір (один або більше): конфіденційність; цілісність*] інформації під час підготовки до передачі та під час приймання.

Рекомендації з реалізації: Інформація може бути ненавмисно або зловмисно розкрита або змінена під час підготовки до передачі або під час отримання, в тому числі під час агрегації, в пунктах трансформації протоколу, а також під час пакування та під час агрегації, в пунктах перетворення протоколу, а також під час пакування та розпакування. Таке несанкціоноване розкриття або такі несанкціоновані розкриття або модифікації ставлять під загрозу конфіденційність або цілісність інформації.

Пов'язані заходи: Немає.

(3) КОНФІДЕНЦІЙНІСТЬ ТА ЦІЛІСНІСТЬ ПЕРЕДАЧІ - КРИПТОГРАФІЧНИЙ ЗАХИСТ ПОВІДОМЛЕНЬ

Реалізувати криптографічні механізми захисту зовнішніх повідомлень, якщо вони не захищені [*Призначення: визначені організацією альтернативні фізичні заходи захисту*].

Рекомендації з реалізації: Криптографічний захист зовнішніх адрес повідомлень спрямований на захист від несанкціонованого розголошення інформації. До зовнішніх даних повідомлень належать заголовки повідомлень та інформація про маршрутизацію. Криптографічний захист запобігає використанню зовнішніх даних повідомлень і застосовується до внутрішніх і зовнішніх мереж або посилань, які можуть бути видимими для особи, які не є авторизованими користувачами. Інформація заголовка і маршрутизації іноді передається відкритим текстом (тобто незашифрованою), оскільки ця інформація не визначена організаціями як таку, що має значну цінність, або тому, що шифрування інформації може призвести до зниження продуктивності мережі або збільшення витрат. Альтернативні фізичні засоби контролю включають захищені системи розподілу.

Пов'язані заходи: SC-12, SC-13.

(4) КОНФІДЕНЦІЙНІСТЬ ТА ЦІЛІСНІСТЬ ПЕРЕДАЧІ - ПРИХОВУВАННЯ АБО РАНДОМІЗАЦІЯ КОМУНІКАЦІЇ

Впровадити криптографічні механізми для приховування або рандомізації

шаблонів комунікації, якщо вони не захищені [*Призначення: визначеними організацією альтернативними фізичними заходами безпеки*].

Рекомендації з реалізації: Приховування або рандомізація шаблонів комунікації спрямована на захист від несанкціонованого розголошення інформації. Моделі комунікації включають частоту, періоди, передбачуваність та обсяг. Зміни в моделях комунікації можуть виявити інформацію, що має розвідувальну цінність, особливо в поєднанні з іншою доступною інформацією, пов'язаною до місії та бізнес-функцій організації. Приховування або рандомізація комунікацій перешкоджає отриманню розвідувальної інформації на основі моделей комунікацій і стосується як внутрішніх, так і зовнішніх мереж або зв'язків, які можуть бути видимими для осіб які не є авторизованими користувачами. Шифрування зв'язків і передача в безперервному, фіксованому або випадковим чином, запобігає отриманню розвідувальних даних на основі шаблонів комунікацій системи. Альтернативні фізичні засоби контролю включають захищені системи розподілу.

Пов’язані заходи: SC-12, SC-13.

(5) КОНФІДЕНЦІЙНІСТЬ ТА ЦІЛІСНІСТЬ ПЕРЕДАЧІ - ЗАХИЩЕНА СИСТЕМА РОЗПОДІЛУ

Реалізація [*Призначення: визначена організацією захищена система розподілу*] до [*Вибір (один або більше): запобігання несанкціонованому розкриттю інформації; виявлення зміни інформації*] під час передачі.

Рекомендації з реалізації: Метою захищеної системи розповділу є запобігання, виявлення та/або ускладнення фізичного доступу до ліній зв’язку, які передають інформацію про національну безпеку.

Пов’язані заходи: Немає.

Посилання: [FIPS 140-3], [FIPS 197], [SP 800-52], [SP 800-77], [SP 800-81-2], [SP 800-113], [SP 800-177], [IR 8023].

## SC-9 КОНФІДЕНЦІЙНІСТЬ ПЕРЕДАЧІ

[Вилучено: Включено до SC-8].

## SC-10 ВІДКЛЮЧЕННЯ МЕРЕЖІ

Заходи захисту:

Завершити з’єднання з мережею, яке пов’язане із сеансом зв’язку в кінці сеансу або після [*Призначення: визначений організацією період часу*] бездіяльності.

Рекомендації з реалізації: Відключення мережі стосується внутрішніх і зовнішніх мереж. Припинення мережевих з’єднань, пов’язаних із певними сеансами зв’язку, включає скасування розподілу адрес TCP/IP або пар портів на рівні операційної системи та скасування розподілу мережевих призначень на рівні програми, якщо кілька сеансів програми використовують одне мережеве з’єднання на рівні операційної системи. Періоди бездіяльності можуть встановлюватися організаціями та включати

періоди часу за типом доступу до мережі або для певних доступів до мережі.

Пов’язані заходи: AC-17, SC-23.

Посилення заходів: Немає.

Посилання: Немає.

## SC-11 ДОВІРЕНИЙ КАНАЛ ЗВ’ЯЗКУ

Заходи захисту:

a. Надати [*Вибір: фізично; логічно*] ізольований надійний канал зв’язку для зв’язку між користувачем і довіреними компонентами системи.

b. Дозволити користувачам запросити довірений канал зв’язку для обміну даними між користувачем і наступними функціями безпеки системи, включно з, як мінімум, автентифікацією та повторною автентифікацією: [*Призначення: визначені організацією функції безпеки*].

Рекомендації з реалізації: Довірені шляхи - це механізми, за допомогою яких користувачі можуть спілкуватися (використовуючи пристрої введення наприклад, клавіатуру) безпосередньо з функціями безпеки систем з необхідними гарантіями для підтримки політик безпеки. Механізми довірених шляхів можуть бути активовані лише користувачами або функціями безпеки систем організації. Відповіді користувачів, які відбуваються через довірені шляхи, захищені від модифікації та розкриття ненадійним додаткам. Організації використовують довірені шляхи для надійних з'єднань з високим ступенем захисту між функціями безпеки систем і користувачами, в тому числі під час входу в систему користувачами. Початкові реалізації довірених шляхів використовували позасмуговий сигнал для ініціювання шляху, наприклад, за допомогою клавіші <BREAK>, яка не передає символи, які можуть бути підроблені. У пізніших реалізаціях використовувалася комбінація клавіш, яку не можна було перехопити (наприклад, клавіші <CTRL> + <ALT> + <DEL>). Такі комбінації клавіш, залежать від конкретної платформи і можуть не забезпечити реалізацію довіреного шляху в кожному конкретному випадку. Застосування довірених шляхів зв'язку забезпечується спеціальною реалізацією, яка відповідає концепції еталонного монітора.

Пов’язані заходи: AC-16, AC-25, SC-12, SC-23.

Посилення заходів:

(1) ДОВІРЕНИЙ КАНАЛ ЗВ’ЯЗКУ - ЛОГІЧНА ІЗОЛЯЦІЯ

(a) Забезпечити надійний канал зв’язку, який незаперечно відрізняється від інших каналів зв’язку.

(b) Ініціювати надійний канал зв’язку для зв’язку між наступними функціями безпеки системи та користувачем [*Призначення: визначені організацією функції безпеки*].

Рекомендації з реалізації: Незаперечний шлях зв’язку дозволяє системі ініціювати довірений шлях, що вимагає, щоб користувач міг безпомилково розпізнати джерело зв’язку як довірений компонент системи. Наприклад, довірений шлях може відображатися в області дисплея, до якої інші програми не можуть отримати доступ, або ґрунтуватися на наявності ідентифікатора, який неможливо підробити.

Пов’язані заходи:Немає.

Посилання: [OMB A-130].

## SC-12 ВСТАНОВЛЕННЯ ТА УПРАВЛІННЯ КРИПТОГРАФІЧНИМИ КЛЮЧАМИ

Заходи захисту:
Встановити та управляти криптографічними ключами для криптографічних засобів, які використовуються в системі відповідно до [*Призначення: визначені організацією вимоги до генерації, поширення, зберігання, доступу та знищення ключів*].

Рекомендації з реалізації: Управління криптографічними ключами та їх створення може здійснюватися за допомогою ручних процедур або автоматизованих механізмів з підтримкою ручних процедур. Організації визначають вимоги до управління ключами відповідно до чинного законодавства, наказів, розпоряджень, директив положеннями, політиками, стандартами та настановами, а також визначають відповідні опції, параметри та рівні. Організації керують довірчими сховищами, щоб гарантувати, що лише затверджені довірчі прив’язки є частиною таких довірчих сховищ.

Пов’язані заходи: AC-17, AU-9, AU-10, CM-3, IA-3, IA-7, SA-4, SA-9, SC-8, SC-11, SC-13, SC-17, SC-20, SC-37, SC-40, SI-3, SI-7.

Посилення заходів:

(1) ВСТАНОВЛЕННЯ ТА УПРАВЛІННЯ КРИПТОГРАФІЧНИМИ КЛЮЧАМИ - ДОСТУПНІСТЬ

Підтримувати доступність інформації в разі втрати користувачами криптографічних ключів.

Рекомендації з реалізації: Депонування ключів шифрування є поширеною практикою для забезпечення їхньої доступності на випадок у випадку втрати ключа. Забута парольна фраза - приклад втрати криптографічного ключа.

Пов’язані заходи: Немає.

(2) ВСТАНОВЛЕННЯ ТА УПРАВЛІННЯ КРИПТОГРАФІЧНИМИ КЛЮЧАМИ - СИМЕТРИЧНІ КЛЮЧІ

Встановити, контролювати та розповсюджувати симетричні криптографічні ключі, використовуючи [*Вибір: стандартизовані; узгоджені уповноваженим органом*] технології та процеси управління ключами.

Рекомендації з реалізації: [SP 800-56A], [SP 800-56B] та [SP 800-56C] надають настанови щодо криптографічних схем створення ключів та методів отримання ключів. [SP 800-57-1], [SP 800-57-2] та [SP 800-57-3] надають настанови щодо керування криптографічними ключами.

Пов’язані заходи: Немає.

(3) ВСТАНОВЛЕННЯ ТА УПРАВЛІННЯ КРИПТОГРАФІЧНИМИ КЛЮЧАМИ - АСИМЕТРИЧНІ КЛЮЧІ

Виробляти, керувати та поширювати асиметричні криптографічні ключі, використовуючи [*Вибір: затверджені уповноваженим органом технології та*

*процеси управління ключами; посилені сертифікати відкритого ключа; попередньо визначений «ключовий» матеріал; кваліфіковані сертифікати відкритого ключа та надійні апаратні засоби цифрового підпису (токени), які захищають особистий ключ користувача; сертифікати, видані відповідно до визначених організацією вимог*].

Рекомендації з реалізації: [SP 800-56A], [SP 800-56B] та [SP 800-56C] надають настанови щодо криптографічних схем створення ключів та методів отримання ключів. [SP 800-57-1], [SP 800-57-2] та [SP 800-57-3] надають настанови щодо керування криптографічними ключами.

Пов'язані заходи: Немає.

(4) ВСТАНОВЛЕННЯ ТА УПРАВЛІННЯ КРИПТОГРАФІЧНИМИ КЛЮЧАМИ - СЕРТИФІКАТИ PKI

[Вилучено: Включено до SC-12 (3)].

(5) ВСТАНОВЛЕННЯ ТА УПРАВЛІННЯ КРИПТОГРАФІЧНИМИ КЛЮЧАМИ - СЕРТИФІКАТИ PKI/АПАРАТНІ ТОКЕНИ

[Вилучено: Включено до SC-12 (3)].

(6) ВСТАНОВЛЕННЯ ТА УПРАВЛІННЯ КРИПТОГРАФІЧНИМИ КЛЮЧАМИ - ФІЗИЧНИЙ КОНТРОЛЬ КЛЮЧІВ

Підтримуйте фізичний контроль криптографічних ключів, коли збережену інформацію шифрують зовнішні постачальники послуг.

Рекомендації з реалізації: Для організацій, які використовують зовнішніх постачальників послуг (наприклад, постачальників хмарних служб або центрів обробки даних), фізичний контроль криптографічних ключів надає додаткову гарантію того, що інформація, яка зберігається такими зовнішніми постачальниками, не підлягає несанкціонованому розкриттю чи зміні.

Пов'язані заходи: Немає.

Посилання: [FIPS 140-3], [SP 800-56A], [SP 800-56B], [SP 800-56C], [SP 800-57-1], [SP 800-57-2], [SP 800-57-3], [SP 800-63-3], [IR 7956], [IR 7966].

## SC-13 КРИПТОГРАФІЧНИЙ ЗАХИСТ

Заходи захисту:

a. Визначити [*Призначення: використання криптографічних засобів, визначених організацією*];

b. Впровадити [*Завдання: визначені організацією види криптографії для кожного визначеного криптографічного використання*].

Рекомендації з реалізації: Криптографія може використовуватися для підтримки різноманітних рішень у сфері безпеки, включаючи захист секретної інформації та контрольованої несекретної інформації, надання та впровадження цифрових підписів

та впровадження цифрових підписів, а також забезпечення поділу інформації, коли уповноважені особи мають необхідні дозволи, але не мають необхідного формального доступу. Криптографія також може використовуватися для підтримки генерації випадкових чисел і гешування. Криптографія впроваджується відповідно до чинних законів, наказів, директив, положень, політиками, стандартами та рекомендацій.

Пов'язані заходи: AC-2, AC-3, AC-7, AC-17, AC-18, AC-19, AU-9, AU-10, CM-11, CP-9, IA-3, IA-5, IA-7, MA-4, MP-2, MP-4, MP-5, SA-4, SA-8, SA-9, SC-8, SC-12, SC-20, SC-23, SC-28, SC-40, SI-3, SI-7.

Посилення заходів: Немає.

(1) КРИПТОГРАФІЧНИЙ ЗАХИСТ - СТАНДАРТНА КРИПТОГРАФІЯ

[Вилучено: Включено до SC-13].

(2) КРИПТОГРАФІЧНИЙ ЗАХИСТ - ЗАТВЕРДЖЕНА УПОВНОВАЖЕНИМ ОРГАНОМ КРИПТОГРАФІЯ

[Вилучено: Включено до SC-13].

(3) КРИПТОГРАФІЧНИЙ ЗАХИСТ - ОСОБИ БЕЗ ОФІЦІЙНИХ ПОВНОВАЖЕНЬ

[Вилучено: Включено до SC-13].

(4) КРИПТОГРАФІЧНИЙ ЗАХИСТ - ЦИФРОВІ ПІДПИСИ

[Вилучено: Включено до SC-13].

Посилання: FIPS Publication 140-3.

## SC-14 ЗАХИСТ ГРОМАДСЬКОГО ДОСТУПУ

[Вилучено: Включено до AC-2, AC-3, AC-5, AC-6, SI-3, SI-4, SI-5, SI-7, SI-10].

## SC-15 СПІЛЬНІ ОБЧИСЛЮВАЛЬНІ ПРИСТРОЇ ТА ЗАСТОСУНКИ

Заходи захисту:

a. Заборонити віддалену активацію спільних обчислювальних пристроїв (хмар) та застосунків з такими виключеннями: [*Призначення: визначені організацією виключення, у яких дозволена віддалена активація*].

b. Надати явну вказівку щодо використання користувачами фізично присутніми пристроями.

Рекомендації з реалізації: Обчислювальні пристрої та програми для спільної роботи включають пристрої та програми для віддалених зустрічей, мережеві дошки, камери та мікрофони. Явна індикація використання включає сигнали для користувачів, коли активуються пристрої та програми для спільної роботи.

Пов'язані заходи: AC-21, SC-42.

Посилення заходів:

(1) СПІЛЬНІ ОБЧИСЛЮВАЛЬНІ ПРИСТРОЇ - ФІЗИЧНЕ ЧИ ЛОГІЧНЕ ВІДКЛЮЧЕННЯ

Надавати [*Вибір (один або кілька): фізичний; логічний*] відключення обчислювальних пристроїв для спільної роботи у спосіб, який підтримує зручність використання.

Рекомендації з реалізації: Якщо не вдасться від'єднатися від обчислювальних пристроїв для спільної роботи, це може призвести до компроментації інформації, що належить організації. Надання простих методів від'єднання від таких пристроїв після спільного обчислювального сеансу гарантує, що учасники виконують від'єднання без необхідності проходити через складні та виснажливі процедури. Відключення від обчислювальних пристроїв для спільної роботи може бути ручним або автоматичним

Пов'язані заходи: Немає.

(2) СПІЛЬНІ ОБЧИСЛЮВАЛЬНІ ПРИСТРОЇ - БЛОКУВАННЯ ТРАФІКУ ВХІДНИХ І ВИХІДНИХ ПОВІДОМЛЕНЬ

[Вилучено: Включено до SC-7].

(3) СПІЛЬНІ ОБЧИСЛЮВАЛЬНІ ПРИСТРОЇ - ВІДКЛЮЧЕННЯ ТА ВИДАЛЕННЯ В БЕЗПЕЧНИХ РОБОЧИХ ЗОНАХ

Відключати або видаляти спільні обчислювальні пристрої та застосунки з [*Призначення: визначених організацією систем або компонентів системи*] у [*Призначення: визначені організацією безпечні робочі зони*].

Рекомендації з реалізації: Нездатність вимкнути або видалити спільні обчислювальні пристрої та програми з систем або компонентів системи може призвести до компрометації інформації, зокрема прослуховування розмов. Прикладом захищеної робочої зони є конфіденційна інформаційна система (SCIF).

Пов'язані заходи: Немає.

(4) СПІЛЬНІ ОБЧИСЛЮВАЛЬНІ ПРИСТРОЇ - ЧІТКА ІДЕНТИФІКАЦІЯ ПОТОЧНИХ УЧАСНИКІВ

Забезпечити явну ідентифікацію поточних учасників [*Призначення: визначені організацією онлайн-зустрічі та телеконференції*].

Рекомендації з реалізації: Явне вказування поточних учасників запобігає неавторизованим особам брати участь у спільних обчислювальних сеансах без відома інших учасників.

Пов'язані заходи: Немає.

Посилання: Немає.

## SC-16 ПЕРЕДАЧА АТРИБУТІВ БЕЗПЕКИ ТА ПРИВАТНОСТІ

Заходи захисту:
Пов’язувати [*Призначення: визначені організацією атрибути безпеки та приватності*] з інформацією, яка передається між системами та компонентами системи.

Рекомендації з реалізації: Атрибути безпеки та конфіденційності можуть бути явно або неявно пов’язані з інформацією, що міститься в системах організації або компонентах системи. Атрибути — це абстракції, які представляють основні властивості або характеристики об’єкта стосовно захисту інформації або управління інформацією, що дозволяє ідентифікувати особу. Атрибути зазвичай асоціюються з внутрішніми структурами даних, включаючи записи, буфери та файли в системі. Атрибути безпеки та конфіденційності використовуються для реалізації політики контролю доступу та контролю потоку інформації; відображати спеціальні інструкції щодо розповсюдження, управління чи розповсюдження, включаючи дозволене використання особистої інформації; або підтримувати інші аспекти політики інформаційної безпеки та конфіденційності. Атрибути конфіденційності можуть використовуватися окремо або в поєднанні з атрибутами безпеки.

Пов’язані заходи: AC-3, AC-4, AC-16.

Посилення заходів:

(1) ПЕРЕДАЧА АТРИБУТІВ БЕЗПЕКИ ТА ПРИВАТНОСТІ - ПЕРЕВІРКА ЦІЛІСНОСТІ

Перевіряти цілісність переданих атрибутів безпеки та приватності.

Рекомендації з реалізації: Частиною перевірки цілісності переданої інформації є забезпечення того, що атрибути безпеки та конфіденційності, пов’язані з такою інформацією, не були змінені несанкціонованим чином. Несанкціонована зміна атрибутів безпеки або конфіденційності може призвести до втрати цілісності переданої інформації.

Пов’язані заходи: AU-10, SC-8.

(2) ПЕРЕДАЧА АТРИБУТІВ БЕЗПЕКИ ТА ПРИВАТНОСТІ - МЕХАНІЗМ АНТИСПУФІНГУ

Впровадити механізми антиспуфінгу, щоб запобігти фальсифікації зловмисниками атрибутів безпеки, які вказують на успішне застосування процесу безпеки.

Рекомендації з реалізації: Деякі вектори атак діють шляхом зміни атрибутів безпеки інформаційної системи для навмисного та зловмисного впровадження недостатнього рівня безпеки в системі. Зміна атрибутів спонукає організації більша частина функцій безпеки працює і саме так, як вони були реалізовано.

Пов’язані заходи: SI-3, SI-4, SI-7.

(3) ПЕРЕДАЧА АТРИБУТІВ БЕЗПЕКИ ТА ПРИВАТНОСТІ - КРИПТОГРАФІЧНА ПРИВ’ЯЗКА

Впровадити [*Призначення: визначені організацією механізми чи методи*] для прив’язки атрибутів безпеки та конфіденційності до переданої інформації.

Рекомендації з реалізації: Криптографічні механізми та методи можуть

забезпечити безпеку та прив’язку атрибутів конфіденційності до переданої інформації, щоб допомогти забезпечити цілісність такої інформації.

Пов’язані заходи: AC-16, SC-12, SC-13.

Посилання: [OMB A-130].

## SC-17 СЕРТИФІКАТИ ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧІВ

Заходи захисту:

a. Випускати сертифікати відкритого ключа відповідно до [*Призначення: визначеної організацією політики сертифікації*];

b. Отримувати сертифікати відкритого ключа від затвердженого постачальника послуг.

Рекомендації з реалізації: Сертифікати інфраструктури відкритих ключів (PKI) - це сертифікати, видимі за межами систем організації, а також сертифікати, пов'язані з внутрішніми операціями систем, як-от специфічні для додатків часові сервіси. У криптографічних системах з ієрархічною структурою, довірений постачальник - це довірине джерело (наприклад, центр сертифікації). Прикладом довіреного постачальника є кореневий сертифікат для системи PKI. ховище сертифікатів підтримує список довірених кореневих сертифікатів.

Пов’язані заходи: AU-10, IA-5, SC-12.

Посилення заходів: Немає.

Посилання: [SP 800-32], [SP 800-57-1], [SP 800-57-2], [SP 800-57-3], [SP 800-63-3].

## SC-18 МОБІЛЬНИЙ КОД

Заходи захисту:

a. Визначати прийнятні та неприйнятні мобільні коди та технології мобільних кодів.

b. Проводити авторизацію, відстежувати та контролювати використання мобільного коду всередині системи.

Рекомендації з реалізації: Мобільний код включає в себе будь-яку програму, додаток або контент, який може бути переданий через мережу (наприклад, вбудований в електронний лист, документ або веб-сайт) і виконується на віддаленій системі. Рішення щодо використання мобільного коду в системах організації приймаються на основі потенційної можливості коду завдати шкоди системам у разі зловмисного використання. Мобільний код включає в себе Java-аплети, JavaScript, HTML5, WebGL та VBScript. Обмеження щодо використання та інструкції з реалізації застосовуються як до вибору та використання мобільного коду, встановленого на серверах, так і до серверах, так і до мобільного коду, що завантажується та виконується на окремих робочих станціях і пристроях, включаючи ноутбуки та смартфони. Політика та процедури щодо мобільного коду стосуються конкретні дії, що вживаються для запобігання розробці, придбанню та впровадженню неприйнятного мобільного коду мобільного коду в системах організації, включаючи вимогу, щоб мобільний код був підписаний цифровим підписом довіреним джерелом.

Пов’язані заходи: AU-2, AU-12, CM-2, CM-6, SI-3.

Посилення заходів:

(1) МОБІЛЬНИЙ КОД - ІДЕНТИФІКАЦІЯ НЕПРИЙНЯТНОГО КОДУ ТА ВЖИВАННЯ ВИПРАВНИХ ДІЙ

Визначити [*Призначення: визначений організацією неприйнятний мобільний код*] та вжити [*Призначення: визначені організацією виправні дії*].

Рекомендації з реалізації: Коригувальні дії при виявленні неприйнятного мобільного коду включають блокування, карантин або сповіщення адміністраторів. Блокування включає запобігання передачі файлів обробки текстів із вбудованими макросами, якщо такі макроси визначено як неприйнятні для мобільного коду.

Пов’язані заходи: Немає.

(2) МОБІЛЬНИЙ КОД - ПРИДБАННЯ, РОЗРОБКА ТА ВИКОРИСТАННЯ

Переконатися, що придбання, розробка та використання мобільного коду, який буде розгорнуто в системі, відповідає вимогам [*Призначення: визначені організацією вимоги до мобільного коду*].

Рекомендації з реалізації: Немає.

Пов’язані заходи: Немає.

(3) МОБІЛЬНИЙ КОД - ЗАПОБІГАННЯ ЗАВАНТАЖЕННЮ ТА ВИКОНАННЮ

Запобігати завантаженню та виконанню [*Призначення: визначений організацією неприйнятний мобільний код*].

Рекомендації з реалізації: Немає.

Пов’язані заходи: Немає.

(4) МОБІЛЬНИЙ КОД - ЗАПОБІГАННЯ АВТОМАТИЧНОМУ ВИКОНАННЮ

Запобігати автоматичному виконанню мобільного коду в [*Призначення: визначені організацією програмні застосунки*] та забезпечити виконання [*Призначення: визначені організацією дії*] перед виконанням коду.

Рекомендації з реалізації: Дії, які виконуються перед виконанням мобільного коду, включають запити користувачів перед відкриттям вкладень електронної пошти або натисканням вебпосилань. Запобігання автоматичному виконанню мобільного коду включає вимкнення функцій автоматичного виконання для компонентів системни, які використовують портативні пристрої зберігання даних, такі як компакт-диски, цифрові універсальні диски та пристрої універсальної послідовної шини.

Пов’язані заходи: Немає.

(5) МОБІЛЬНИЙ КОД - ДОЗВІЛ ВИКОНАННЯ ТІЛЬКИ В ОБМЕЖЕНИХ СЕРЕДОВИЩАХ

Допускати виконання дозволеного мобільного коду лише на обмежених віртуальних машинних середовищах.

Рекомендації з реалізації: Дозвіл на виконання мобільного коду лише в обмежених середовищах віртуальних машин допомагає запобігти впровадженню шкідливого коду в інші системи та системні компоненти.

Пов'язані заходи: SC-44, SI-7.

Посилання: [SP 800-28].

## SC-19 ІНТЕРНЕТ-ПРОТОКОЛ ГОЛОСОВОГО ЗВ'ЯЗКУ

[Вилучено: Залежить від технології; розглядається як будь-яка інша технологія або протокол].

## SC-20 БЕЗПЕЧНА СЛУЖБА ІМЕН/АДРЕС (УПОВНОВАЖЕНЕ ДЖЕРЕЛО)

Заходи захисту:

a. Надати додаткові дані автентифікації та перевірки цілісності джерела даних разом з офіційними даними розпізнавання імен, які система повертає у відповідь на запити дозволу імен/адрес.

b. Надати засоби для вказання статусу безпеки дочірніх зон і (якщо дочірня зона підтримує служби безпечного дозволу) забезпечити перевірку ланцюга довіри між батьківськими та дочірніми доменами при роботі в складі розподіленого ієрархічного простору імен.

Рекомендації з реалізації: Надання авторитетної вихідної інформації дозволяє зовнішнім клієнтам, у тому числі віддаленим Інтернет-клієнтам, отримати гарантії автентифікації походження та перевірки цілісності для інформації про перетворення імен хостів/сервісів у мережеві адреси, отриманої за допомогою служби. Системи, які надають послуги з перетворення імен та адрес, включають систему доменних імен (DNS) сервери. Додаткові артефакти включають цифрові підписи DNS Security Extensions (DNSSEC) та криптографічні ключі. Достовірні дані включають записи ресурсів DNS. Засоби для вказівки статусу безпеки дочірніх зон є використання ресурсних записів підписувачів делегування в DNS. Системи, які використовують технології, відмінні від DNS, для зіставлення між іменами хостів і служб та мережевими адресами, надають інші засоби для забезпечення автентичності та цілісності відповідей дані.

Пов'язані заходи: AU-10, SC-8, SC-12, SC-13, SC-21, SC-22.

Посилення заходів:

(1) БЕЗПЕЧНА СЛУЖБА ІМЕН/АДРЕС (УПОВНОВАЖЕНЕ ДЖЕРЕЛО) - ДОЧІРНІЙ ПІДПРОСТІР

[Вилучено: включено до SC-20].

(2) БЕЗПЕЧНА СЛУЖБА ІМЕН/АДРЕС (УПОВНОВАЖЕНЕ ДЖЕРЕЛО) - ДЖЕРЕЛО ДАНИХ І ЦІЛІСНІСТЬ

Забезпечити справжність джерела походження та цілісність запитів внутрішніх імен/адрес.

Рекомендації з реалізації: Немає.

Пов’язані заходи: Немає.

Посилання: [FIPS 140-3], [FIPS 186-4], [SP 800-81-2].

## SC-21 БЕЗПЕЧНА СЛУЖБА ІМЕН/АДРЕС (РЕКУРСИВНИЙ АБО КЕШУВАЛЬНИЙ ПЕРЕТВОРЮВАЧ)

Заходи захисту:

Зробити запит та виконати перевірку автентичності джерела даних і перевірку цілісності даних у відповідях на дозвіл імен/адрес, які система отримує від уповноважених джерел.

Рекомендації з реалізації: Кожен клієнт сервісів виконує цю перевірку самостійно, або має аутентифіковані канали зв'язку з довіреними провайдерами валідації. Системи, які надають імена та адрес для локальних клієнтів включають рекурсивне вирішення або кешування доменних імен системи доменних імен (DNS). Клієнтські DNS або виконують перевірку підписів DNSSEC, або клієнти використовують автентифіковані канали для зв'язку з рекурсивними вирішувачами, які виконують таку перевірку. Системи які використовують технології, відмінні від DNS, для зіставлення імен хостів, служб і мережевих адресами, надають деякі інші засоби, що дозволяють клієнтам перевіряти автентичність і цілісність даних відповідно.

Пов’язані заходи: SC-20, SC-22.

Посилення заходів: Немає.

(1) БЕЗПЕЧНА СЛУЖБА ІМЕН/АДРЕС (РЕКУРСИВНИЙ АБО КЕШУВАЛЬНИЙ ПЕРЕТВОРЮВАЧ) - ДЖЕРЕЛО ДАНИХ ТА ЦІЛІСНІСТЬ

[Вилучено: Включено до SC-21].

Посилання: [SP 800-81-2].

## SC-22 АРХІТЕКТУРА ТА ЗАБЕЗПЕЧЕННЯ СЛУЖБИ ІМЕН/АДРЕС

Заходи захисту:

Переконатися, що системи, які спільно надають послуги розпізнавання імен/адрес для організації, є відмовостійкими та забезпечують поділ внутрішніх і зовнішніх ролей.

Рекомендації з реалізації: Системи, які надають послуги з визначення імен та адрес, включають в себе сервери доменних імен (DNS). Щоб усунути єдині точки відмови в системах і підвищити надмірність, організації використовують щонайменше два авторитетних сервери системи доменних імен - один налаштований як один з яких налаштований як основний сервер, а інший - як додатковий. Крім того, організації зазвичай розгортають сервери у двох географічно відокремлених мережевих підмережах (тобто не розташованих в одному фізичному приміщенні). Для розділення ролей DNS-сервери з внутрішніми ролями виконують лише такі функції обробляють

запити на дозвіл імен і адрес, що надходять зсередини організації (тобто від внутрішніх клієнтів). DNS-сервери із зовнішніми ролями обробляють лише інформацію про дозвіл імен та адрес запити від клієнтів ззовні організації (тобто із зовнішніх мереж, включно з Інтернетом). Інтернет). Організації визначають клієнтів, які можуть отримати доступ до авторитетних DNS-серверів у певних ролях (наприклад, за діапазонами адрес і явними списками).

Пов’язані заходи: SC-2, SC-20, SC-21, SC-24.

Посилення заходів: Немає.

Посилання: [SP 800-81-2].

## SC-23 АВТЕНТИФІКАЦІЯ СЕСІЇ

Заходи захисту: Забезпечити автентифікацію сеансів зв’язку.

Рекомендації з реалізації: Захист автентичності сеансу стосується захисту зв'язку на рівні сеансу а не на рівні пакетів. Такий захист створює підстави для впевненості на обох кінцях сеансу зв'язку в постійній ідентичності інших сторін і достовірності переданої інформації, що передається. Захист автентичності включає в себе захист від атак "людини посередині", перехоплення сеансу зв'язку та введення неправдивої інформації в сеанс зв'язку.

Пов’язані заходи: AU-10, SC-8, SC-10, SC-11.

Посилення заходів:

(1) АВТЕНТИФІКАЦІЯ СЕСІЇ - АНУЛЮВАННЯ ІДЕНТИФІКАТОРА СЕАНСУ ЗВ’ЯЗКУ ПРИ ВИХОДІ ІЗ СИСТЕМИ

Анулювати ідентифікатор сеансу зв’язку після виходу користувача або іншого припинення сеансу зв’язку.

Рекомендації з реалізації: Анулювання ідентифікатора сеансу під час виходу з системи обмежує здатність зловмисників перехоплювати та продовжувати використовувати раніше дійсні ідентифікатори сеансу.

Пов’язані заходи: Немає.

(2) АВТЕНТИФІКАЦІЯ СЕСІЇ - ІНІЦІЙОВАНІ КОРИСТУВАЧЕМ ВИХОДИ ТА ПОВІДОМЛЕННЯ

[Вилучено: Включено до SC-21(1)].

(3) АВТЕНТИФІКАЦІЯ СЕСІЇ - УНІКАЛЬНІ ІДЕНТИФІКАТОРИ СЕАНСІВ З РАНДОМІЗАЦІЄЮ

Створювати унікальний ідентифікатор сеансу зв’язку для кожного сеансу зв’язку за допомогою [*Призначення: визначені організацією вимоги до випадковостей*] та розпізнавати лише ідентифікатори сеансів зв’язку, які генеруються системою.

Рекомендації з реалізації: Створення унікальних ідентифікаторів сеансу

обмежує можливість зловмисників повторно використовувати раніше дійсні ідентифікатори сеансу. Використання концепції випадковості в генерації унікальних ідентифікаторів сеансу захищає від атак грубої сили для визначення ідентифікаторів майбутніх сеансів.

Пов'язані заходи: AC-10, SC-12, SC-13.

(4) АВТЕНТИФІКАЦІЯ СЕСІЇ - УНІКАЛЬНІ ІДЕНТИФІКАТОРИ СЕАНСІВ З РАНДОМІЗАЦІЄЮ

[Вилучено: Включено до SC-23 (3)].

(5) АВТЕНТИФІКАЦІЯ СЕСІЇ - ДОЗВОЛЕНІ УПОВНОВАЖЕНІ ІЗ СЕРТИФІКАЦІЇ

Дозволяти використання лише [*Призначення: визначених організацією уповноважених із сертифікації*] для перевірки встановлення захищених сеансів.

Рекомендації з реалізації: Довіра до центрів сертифікації для встановлення безпечних сеансів включає використання сертифікатів безпеки транспортного рівня (TLS). Ці сертифікати, після перевірки їхніми відповідними центрами сертифікації, полегшують встановлення захищених сеансів між вебклієнтами та вебсерверами.

Пов'язані заходи: SC-12, SC-13.

Посилання: [SP 800-52], [SP 800-77], [SP 800-95], [SP 800-113].

## SC-24 УВЕДЕННЯ У ВІДОМИЙ СТАН

Заходи захисту:

Увести систему в [*Призначення: визначений організацією відомий стан системи*] у разі [*Призначення: визначені організацією типи збоїв системи*] зі збереженням [*Призначення: визначена організацією інформація про стан системи*] при збої.

Рекомендації з реалізації: Відмова у відомому стані вирішує проблеми безпеки відповідно місії та бізнес-потреб організацій. Відмова у відомому стані запобігає втраті конфіденційності, цілісності або доступності інформації в разі збоїв в роботі систем організації або їх компонентів. або компонентів системи. Відмова у відомому безпечному стані допомагає запобігти виходу систем з ладу до стану, який може призвести до травмування людей або знищення майна. Збереження інформації про стан системи полегшує перезапуск системи та повернення до робочого режиму з меншим порушенням місії та бізнес-процесів.

Пов'язані заходи: CP-2, CP-4, CP-10, CP-12, SA-8, SC-7, SC-22, SI-13.

Посилення заходів: Немає.

Посилання: Немає.

## SC-25 ТОНКІ ВУЗЛИ

Заходи захисту:

Використовувати [*Призначення: визначені організацією системні компоненти*] з

мінімальною функціональністю та зберіганням інформації.

Рекомендації з реалізації: Розгортання компонентів системи з мінімальною функціональністю зменшує потребу в захисті кожної кінцевої точки і може зменшити вразливість інформації, систем і сервісів до атак. До таких компонентів належать бездискові вузли та технології тонких клієнтів.

Пов'язані заходи: SC-30, SC-44.

Посилення заходів: Немає.

Посилання: Немає.

## SC-26 ПРИМАНКА ДЛЯ ЗЛОВМИСНИКІВ (DECOYS)

Заходи захисту:
Вносити в систему компоненти, які спеціально призначені як об'єкти атак, з метою виявлення, відбиття й аналізу таких атак.

Рекомендації з реалізації: Приманки (пастки або сітки обману) створюються для залучення супротивників і відволікання їх уваги супротивників і відволікання атак від операційних систем, які підтримують місію та бізнес-функції організації. Використання приманок вимагає певних допоміжних заходів ізоляції, щоб гарантувати, що відвернутий шкідливий код не заразить системи організації.

Пов'язані заходи: RA-5, SC-7, SC-30, SC-35, SC-44, SI-3, SI-4.

Посилення заходів: Немає.

(1) ПРИМАНКА ДЛЯ ЗЛОВМИСНИКІВ (HONEYPOTS) - ВИЯВЛЕННЯ ШКІДЛИВОГО КОДУ

[Вилучено: Включено до SC-35].

Посилання: Немає.

## SC-27 НЕЗАЛЕЖНІ ВІД ПЛАТФОРМИ ЗАСТОСУНКИ

Заходи захисту:

Внести до системи: [*Призначення: визначені організацією незалежні від платформи застосунки*].

Рекомендації з реалізації: Платформи - це комбінації апаратних, програмних і апаратно-програмних компонентів, що використовуються для виконання програмних застосунків. Платформи включають операційні системи, базову комп'ютерну архітектуру комп'ютера або і те, і інше. Платформонезалежні програми - це програми з можливістю виконуватися на різних платформах. Такі програми сприяють перенесенню та відтворенню на різних платформах. Можливість перенесення додатків і відтворення на різних платформах підвищують доступність критично важливих функцій в організаціях в ситуаціях, коли системи з певними операційними системами піддаються атакам.

Пов'язані заходи: SC-29.

Посилення заходів: Немає.

Посилання: Немає.

## SC-28 ЗАХИСТ ІНФОРМАЦІЇ В СТАНІ СПОКОЮ

Заходи захисту:
Забезпечити [*Вибір (один або кілька): конфіденційність; цілісність*] [*Призначення: визначена організацією інформація*] в стані спокою.

Рекомендації з реалізації: Інформація в стані спокою – це інформація, яка не обробляється чи передається, а знаходиться в компонентах системи. До таких компонентів належать внутрішні або зовнішні жорсткі диски, мережеві пристрої зберігання чи бази даних. Однак захист інформації, що знаходиться в стані спокою, зосереджується не на типі пристрою зберігання чи частоті доступу, а скоріше на стані інформації. Інформація в стані спокою стосується конфіденційності та цілісності інформації та охоплює інформацію користувача та системну інформацію. Інформація, пов'язана з системою, яка потребує захисту, включає конфігурації або набори правил для брандмауерів, систем виявлення та запобігання вторгненням, маршрутизаторів фільтрації та інформацію про автентифікацію. Організації можуть використовувати різні механізми для забезпечення конфіденційності та захисту цілісності, включаючи використання криптографічних механізмів і сканування спільних файлів. Захист цілісності може бути досягнутий, наприклад, реалізацією технологій WORM (write-once-read-many). Якщо належного захисту інформації, що знаходиться в стані спокою, неможливо досягти інакше, організації можуть використовувати інші засоби контролю, включаючи часте сканування для виявлення зловмисного коду в стані спокою, а також безпечне зберігання в автономному режимі замість онлайн-сховища.

Пов'язані заходи: AC-3, AC-6, AC-19, CA-7, CM-3, CM-5, CM-6, CP-9, MP-4, MP-5, PE-3, SC-8, SC-12, SC-13, SC-34, SI-3, SI-7, SI-16.

Посилення заходів:

(1) ЗАХИСТ ІНФОРМАЦІЇ В СТАНІ СПОКОЮ - КРИПТОГРАФІЧНИЙ ЗАХИСТ

Впровадити криптографічні механізми для запобігання несанкціонованому розкриттю та модифікації [*Призначення: визначена організацією інформація*] у стані спокою на [*Призначення: визначені організацією компоненти системи*].

Рекомендації з реалізації: Вибір криптографічних механізмів базується на необхідності захисту конфіденційності та цілісності інформації. Міцність механізму відповідає категорії безпеки або класифікації інформації. Організації мають можливість шифрувати інформацію на компонентах системи чи носіях або шифрувати структури даних, зокрема файли, записи чи поля.

Пов'язані заходи: AC-19, SC-12, SC-13.

(2) ЗАХИСТ ІНФОРМАЦІЇ В СТАНІ СПОКОЮ - АВТОНОМНЕ СХОВИЩЕ

Видаляти [*Призначення: визначена організацією інформація*] з онлайнового сховища та зберігати її в автономному(off-line) режимі в безпечному місці.

Рекомендації з реалізації: Видалення інформації, що належить організації, з онлайн-сховища в офлайн-сховище усуває можливість отримання особами

неавторизованого доступу до інформації через мережу. Тому організації можуть вибрати переміщення інформації в офлайн-сховище замість захисту такої інформації в онлайн-сховищі.

Пов'язані заходи: Немає.

(3) ЗАХИСТ ІНФОРМАЦІЇ В СТАНІ СПОКОЮ - КРИПТОГРАФІЧНІ КЛЮЧІ

Забезпечити захищене зберігання криптографічних ключів [*Вибір: [Призначення: гарантії, визначені організацією]; апаратно-захищене сховище ключів*].

Рекомендації з реалізації: Модуль довіреної платформи (TPM) є прикладом апаратно-захищеного сховища даних, яке можна використовувати для захисту криптографічних ключів.

Пов'язані заходи: SC-12, SC-13.

Посилання: [OMB A-130], [SP 800-56A], [SP 800-56B], [SP 800-56C], [SP 800-57-1], [SP 800-57- 2], [SP 800-57-3], [SP 800-111], [SP 800-124].

## SC-29 ГЕТЕРОГЕННІСТЬ

Заходи захисту:
Використовувати різноманітний набір інформаційних технологій для [*Призначення: визначені організацією системні компоненти*] при впровадженні системи.

Рекомендації з реалізації: Збільшення різноманітності інформаційних технологій в системах організації зменшує вплив потенційної експлуатації або компрометації конкретних технологій. Така різноманітність захищає від загальних збоїв, в тому числі від збоїв, спричинених атаками на ланцюги постачання. Різноманітність інформаційних технологій також зменшує ймовірність того, що засоби які супротивник використовує для компрометації одного компоненту системи, будуть ефективні проти інших компонентів системи, тим самим ще більше збільшуючи фактор роботи супротивника для успішного завершення атаки компонентів системи, таким чином ще більше збільшуючи фактор роботи противника для успішного завершення запланованих атак. Збільшення різноманітності може призвести до ускладнення і збільшення витрат на управління, що може зрештою призвести до помилок і несанкціонованих конфігурацій.

Пов'язані заходи: AU-9, PL-8, SC-27, SC-30, SR-3.

Посилення заходів:

(1) ГЕТЕРОГЕННІСТЬ - МЕТОДИ ВІРТУАЛІЗАЦІЇ

Використовувати методи віртуалізації для підтримки розгортання різноманітних операційних систем і програм, що змінюються [*Призначення: визначена організацією частота*].

Рекомендації з реалізації: Хоча часті зміни в операційних системах і програмах можуть створювати значні проблеми з керуванням конфігураціями, зміни можуть призвести до збільшення коефіцієнта роботи зловмисників для проведення успішних атак. Зміна віртуальних операційних систем або додатків,

на відміну від зміни фактичних операційних систем або додатків, забезпечує віртуальні зміни, які перешкоджають успіху зловмисника, одночасно зменшуючи зусилля з керування конфігурацією. Методи віртуалізації можуть допомогти в ізоляції ненадійного програмного забезпечення або програмного забезпечення сумнівного походження в обмежених середовищах виконання.

Пов'язані заходи: Немає.

Посилання: Немає.

## SC-30 МАСКУВАННЯ ТА ХИБНИЙ НАПРЯМ

Заходи захисту:
Використовувати [*Призначення: визначені організацією методи маскування та хибного напряму*] для [*Призначення: визначені організацією системи*] у [*Призначення: визначений організацією період часу*], щоб заплутати та ввести в оману зловмисників.

Рекомендації з реалізації: Методи приховування і перенацілювання можуть значно зменшити можливості супротивника (тобто вікно можливостей і доступну поверхню атаки) для ініціювання і завершення атак. Наприклад, методи віртуалізації надають організаціям можливість маскувати системи, що потенційно зменшує ймовірність успішних атак без витрат на використання декількох платформ. Зростання використання методів приховування і методів перенаправлення - в тому числі випадковості, невизначеності і віртуалізації - може достатньо заплутати і ввести в оману супротивників, а отже, підвищити ризик виявлення та/або викриття обману. Методи приховування та дезорієнтації можуть надати додатковий час для виконання основної місії та бізнес-функцій. Застосування методів приховування та введення в оману може збільшити складність системи та витрати на управління, необхідні для її функціонування.

Пов'язані заходи: AC-6, SC-25, SC-26, SC-29, SC-44, SI-14.

Посилення заходів:

(1) МАСКУВАННЯ ТА ХИБНИЙ НАПРЯМ - МЕТОДИ ВІРТУАЛІЗАЦІЇ

[Вилучено: Включено до SC-29(1)].

(2) МАСКУВАННЯ ТА ХИБНИЙ НАПРЯМ - ВИПАДКОВІСТЬ

Використовувати [*Призначення: визначені організацією методи*], щоб ввести фактор випадковості в операції та активи організації.

Рекомендації з реалізації: Випадковість вносить підвищений рівень невизначеності для супротивників щодо дій, які організації вживають для захисту своїх систем від атак. Такі дії можуть перешкоджати спроможності супротивника правильно націлюватись на інформаційні ресурси організацій, які підтримують критичні місії або бізнес-функції. Невизначеність також може змусити супротивника вагатися перед початком або продовженням атак. Техніки дезорієнтації включають в себе випадковість виконання певних рутинних дій у різний час доби, використання різних інформаційних технологій, використання різних постачальників, а також ротацію ролей та обов'язків персоналу організації.

Пов'язані заходи: Немає.

(3) МАСКУВАННЯ ТА ХИБНИЙ НАПРЯМ - ЗМІНА МІСЦЯ ОБРОБКИ ТА ЗБЕРІГАННЯ

Змінювати місце [*Призначення: визначених організацією обробки та/або зберігання*] у [*Вибір:* [*Призначення: визначені організацією моменти часу*]; *випадкових часових інтервалах*]].

Рекомендації з реалізації: Противник націлений на критичні місії та бізнес-функції, а також на системи, які підтримують ці місії та бізнес-функції намагаючись при цьому мінімізувати викриття їхнього існування та методів роботи. Статичний, однорідний і детермінований характер систем організації, на які спрямовані атаки, робить такі системи більш вразливими до атак з меншими витратами і зусиллями з боку противника для досягнення успіху. Зміна місць обробки та зберігання даних (також відома як захист від рухомих цілей) спрямована на боротьбу з сучасними постійними загрозами за допомогою таких методів, як віртуалізація, розподілена обробка та реплікація. Це дозволяє організаціям переміщати компоненти системи (наприклад, обробку, зберігання), які підтримують критично важливі місії та бізнес-функції. Зміна місць обробки даних та/або місць зберігання вносить певну невизначеність у цілеспрямовані дії супротивника. Невизначеність у виборі цілей збільшує робочий фактор противника і робить компрометації або порушення систем організації більш складними і трудомісткими. Це також збільшує ймовірність того, що супротивники можуть ненавмисно розкрити певні аспекти своїх методів під час спроб знайти критичні організаційні ресурси.

Пов’язані заходи: Немає.

(4) МАСКУВАННЯ ТА ХИБНИЙ НАПРЯМ - НЕПРАВДИВА ІНФОРМАЦІЯ

Використовувати реалістичну, але неправдиву інформацію в [*Призначення: визначені організацією компоненти системи*] про її стан безпеки або положення.

Рекомендації з реалізації: Використання неправдивої інформації має на меті ввести в оману потенційних супротивників щодо характеру та обсягу заходів захисту, впроваджених в організації. Таким чином, зловмисники можуть застосовувати некоректні та неефективні методи атак. Один з методів введення в оману зловмисників полягає в тому, що організації розміщують неправдиву інформацію щодо конкретних заходів захисту, розгорнутих у зовнішніх системах, які, як відомо, є об'єктами атак з боку зловмисників. Іншим методом є використання оманливих мереж, які імітують реальні аспекти систем організації, але використовують, наприклад, застарілі конфігурації програмного забезпечення.

Пов’язані заходи: Немає.

(5) МАСКУВАННЯ ТА ХИБНИЙ НАПРЯМ - МАСКУВАННЯ КОМПОНЕНТІВ СИСТЕМИ

Використовувати [*Призначення: визначені організацією методи*], щоб приховати або замаскувати [*Призначення: визначені організацією компоненти системи*].

Рекомендації з реалізації: Приховуючи, маскуючи або приховуючи критичні компоненти системи, організації можуть зменшити ймовірність того, що

супротивник націлиться на ці ресурси і успішно скомпрометує їх. ці ресурси. Потенційні засоби для приховування, маскування або приховування компонентів системи включають конфігурацію маршрутизаторів, використання методів шифрування або віртуалізації.

Пов’язані заходи: Немає.

Посилання: Немає.

## SC-31 АНАЛІЗ ПРИХОВАНОГО КАНАЛУ

Заходи захисту:

a. Проводити аналіз прихованого каналу, щоб визначити ті аспекти комунікацій у системі, які володіють потенційними можливостями для реалізації прихованих каналів [*Вибір (один або кілька): зберігання; синхронізації*].

b. Оцінювати максимальну пропускну здатність цих каналів.

Рекомендації з реалізації: Розробники мають найкращі можливості для виявлення потенційних місць у системах, які можуть призвести до прихованих каналів. Аналіз прихованих каналів має сенс тоді, коли існує потенціал для несанкціонованих інформаційних потоків через сфери безпеки, наприклад, у випадку систем, які містять інформацію, що підлягає експортному контролю, і мають зв'язок із зовнішніми мережами (тобто з мережами, які не контролюються організаціями). Аналіз прихованих каналів також корисний для багаторівневих захищених систем, систем з декількома рівнями безпеки та міждоменних систем.

Пов’язані заходи: AC-3, AC-4, SI-11.

Посилення заходів:

(1) АНАЛІЗ ПРИХОВАНОГО КАНАЛУ - ТЕСТУВАННЯ ПРИХОВАНИХ КАНАЛІВ ДЛЯ ЕКСПЛУАТАЦІЇ

Тестувати підмножини визначених прихованих каналів, щоб визначити, які канали можна використовувати.

Рекомендації з реалізації: Немає.

Пов’язані заходи: Немає.

(2) АНАЛІЗ ПРИХОВАНОГО КАНАЛУ - МАКСИМАЛЬНА ПРОПУСКНА ЗДАТНІСТЬ

Зменшувати максимальну пропускну здатність для визначених прихованих каналів [*Вибір (один або більше); зберігання; синхронізації*] до [*Призначення: визначене організацією значення*].

Рекомендації з реалізації: Повне усунення прихованих каналів, особливо прихованих каналів синхронізації, зазвичай неможливе без значного впливу на продуктивність.

Пов’язані заходи: Немає.

(3) АНАЛІЗ ПРИХОВАНОГО КАНАЛУ - ВИМІРЮВАННЯ ПРОПУСКНОЇ ЗДАТНОСТІ В РОБОЧИХ СЕРЕДОВИЩАХ

Вимірювати пропускну здатність [*Призначення: визначена організацією підмножина визначених прихованих каналів*] в операційному середовищі системи.

Рекомендації з реалізації: Вимірювання пропускної здатності прихованого каналу в певних робочих середовищах допомагає організаціям визначити, скільки інформації може бути приховано до того, як такий витік негативно вплине на місію або бізнес-функції. Пропускна здатність прихованого каналу може суттєво відрізнятися при вимірюванні в налаштуваннях, які не залежать від конкретних робочих середовищ, включаючи лабораторії чи середовища розробки системи.

Пов'язані заходи: Немає.

Посилання: Немає.

## SC-32 ПОДІЛ СИСТЕМИ НА ЧАСТИНИ

Заходи захисту:
Розділити систему на [*Призначення: визначені організацією системні компоненти*], що розміщені в окремих фізичних доменах або середовищах на основі [*Призначення: визначені організацією умови для фізичного поділу компонентів*].

Рекомендації з реалізації: Поділ системи на частини є частиною стратегії поглибленого захисту. Організації визначають ступінь фізичного поділу компонентів системи. Параметри фізичного подулу включають фізично відмінні компоненти в окремих стійках в одній кімнаті, критичні компоненти в окремих кімнатах і географічне розділення критичних компонентів. Категорія безпеки може керувати вибором кандидатів для поділу домену. Керовані інтерфейси обмежують або забороняють доступ до мережі та потік інформації між компонентами розділеної системи.

Пов'язані заходи: AC-4, AC-6, SA-8, SC-2, SC-3, SC-7, SC-36.

Посилення заходів:

(1) ПОДІЛ СИСТЕМИ НА ЧАСТИНИ - ВІДОКРЕМЛЕНІ ФІЗИЧНІ ДОМЕНИ ДЛЯ ПРИВІЛЕЙОВАНИХ ФУНКЦІЙ

Розділіть привілейовані функції на окремі фізичні домени.

Рекомендації з реалізації: Привілейовані функції, які працюють в одному фізичному домені, можуть являти собою єдину точку збою, якщо цей домен стає скомпрометованим або виникає відмова в обслуговуванні.

Пов'язані заходи: Немає.

Посилання: [FIPS 199], [IR 8179].

## SC-33 ПІДГОТОВКА ЦІЛІСНОСТІ ПЕРЕДАЧІ

[Вилучено: Включено до SC-8].

## SC-34 НЕЗМІНЮВАНІ ВИКОНАВЧІ ПРОГРАМИ

Заходи захисту:
У [*Призначення: визначені організацією системні компоненти*]:

a. Завантажити та виконати операційне середовище з апаратного носія, що працює в режимі лише для зчитування.

b. Завантажити та виконати [*Призначення: визначені організацією застосунки*] з апаратного носія, що працює в режимі лише для зчитування.

Рекомендації з реалізації: Операційне середовище системи містить код, у якому працюють програми, зокрема операційні системи, виконавчі програми або монітори віртуальних машин (тобто гіпервізори). Воно може також включати певні програми, які працюють безпосередньо на апаратних платформах. Апаратно-закріплені, носії, призначені лише для читання, включають компакт-диски, що записуються (CD-R) та цифрові універсальні диски, що записуються (DVD-R), а також одноразові програмовані носії, призначені лише для читання. Використання немодифікованої пам'яті забезпечує цілісність програмного забезпечення з моменту створення образу, доступного лише для читання. Використання перепрограмованої пам'яті, доступної тільки для читання, може бути прийнято як носій тільки для читання за умови, що цілісність може бути адекватно захищена з моменту початкового запису до вставки пам'яті в систему, а також за наявності надійних апаратних засобів захисту від перепрограмування пам'яті під час встановлення в системах організації.

Пов’язані заходи: AC-3, SI-7, SI-14.

Посилення заходів:

(1) НЕЗМІНЮВАНІ ВИКОНАВЧІ ПРОГРАМИ - ВІДСУТНІСТЬ СХОВИЩА, ДОСТУПНОГО ДЛЯ ЗАПИСУ ІНФОРМАЦІЇ

Використовує [Призначення: визначені організацією системні компоненти] без можливості запису в сховище, яке є постійним при перезапуску компонента або вмикання/вимикання.

Рекомендації з реалізації: Заборона записуваного сховища усуває можливість вставлення зловмисного коду через постійне записуване сховище у призначені компоненти системи. Обмеження стосується фіксованих і знімних носіїв, причому останні розглядаються або безпосередньо, або як спеціальні обмеження, що накладаються через контроль доступу для мобільних пристроїв.

Пов’язані заходи: AC-19, MP-7.

(2) НЕЗМІНЮВАНІ ЗДІЙСНЮВАНІ ПРОГРАМИ - ЗАХИСТ ЦІЛІСНОСТІ НА НОСІЇ, ПРИДАТНОМУ ТІЛЬКИ ДЛЯ ЧИТАННЯ

Захищати цілісність інформації перед її зберіганням на носії, придатному тільки для читання та контролювати носій після того, як така інформація була записана.

Рекомендації з реалізації: Заходи захисту запобігають заміні носіїв у системах

або перепрограмуванню програмованих носіїв, доступних лише для читання, до інсталяції в системи. Контроль захисту цілісності включає поєднання запобігання, виявлення та реагування.

Пов'язані заходи: CM-3, CM-5, CM-9, MP-2, MP-4, MP-5, SC-28, SI-3.

(3) НЕЗМІНЮВАНІ ПРОГРАМИ, ЩО ВИКОНУЮТЬСЯ - АПАРАТНИЙ ЗАХИСТ

[Вилучено: Перенесено до SC-51].

## SC-35 РОЗПІЗНАВАННЯ ПРИМАНОК ДЛЯ ЗЛОВМИСНИКІВ (HONEYCLIENT)

Заходи захисту:

Ввімкнути системні компоненти, які активно намагаються ідентифікувати мережевий шкідливий код та шкідливі вебсайти.

Рекомендації з реалізації: Зовнішня ідентифікація шкідливого коду відрізняється від приманок в SC-26 тим, що компоненти активно досліджують мережі, включаючи Інтернет, у пошуках шкідливого коду що міститься на зовнішніх вебсайтах. Як і у випадку з приманками, використання зовнішньої ідентифікації шкідливого коду використання зовнішніх методів ідентифікації шкідливого коду вимагає певних допоміжних заходів ізоляції, щоб гарантувати, що будь-який шкідливий код, виявлений під час пошуку виявлений під час пошуку і згодом виконаний шкідливий код не заразить системи організації. Віртуалізація є поширеним методом досягнення такої ізоляції.

Пов'язані заходи: SC-7, SC-26, SC-44, SI-3, SI-4.

Посилення заходів: Немає.

Посилання: Немає.

## SC-36 РОЗПОДІЛЕНА ОБРОБКА ТА ЗБЕРІГАННЯ

Заходи захисту:

Розподіліть наведені нижче компоненти обробки та зберігання в кількох [*Вибір: фізичні локації; логічні домени*]: [*Призначення: компоненти обробки та зберігання, визначені організацією*].

Рекомендації з реалізації: Розподіл обробки та зберігання між кількома фізичними локаціями або логічними доменами забезпечує певний ступінь резервування або накладання для організацій. Надлишковість і накладення збільшують робочий фактор супротивників, що негативно впливає на організаційні операції, активи та осіб. Використання розподіленої обробки та зберігання не передбачає єдиного первинного місця обробки або зберігання. Таким чином, це дозволяє паралельно обробляти та зберігати.

Пов'язані заходи: CP-6, CP-7, PL-8, SC-32.

Посилення заходів:

(1) РОЗПОДІЛЕНА ОБРОБКА ТА ЗБЕРІГАННЯ - МЕТОДИ ОПИТУВАННЯ

(a) Використовувати методи опитування для виявлення потенційних збоїв, помилок або компрометації до [*Призначення: визначені організацією розподілені компоненти обробки та зберігання*]

(b) Вживати [*Призначення: визначені організацією заходи*] у відповідь на виявлені збої, помилки або компрометації.

Рекомендації з реалізації: Розподілену обробку та/або зберігання можна використовувати для зменшення можливостей зловмисників скомпрометувати конфіденційність, цілісність або доступність інформації та систем організації. Однак розподіл компонентів обробки та зберігання не заважає зловмисникам скомпрометувати один або кілька компонентів. Опитування порівнює результати обробки та/або вміст зберігання з розподілених компонентів і згодом підраховує результати. Опитування визначає потенційні несправності, компрометації або помилки в компонентах розподіленої обробки та зберігання.

Пов'язані заходи: SI-4.

(2) РОЗПОДІЛЕНА ОБРОБКА ТА ЗБЕРІГАННЯ - СИНХРОНІЗАЦІЯ

Синхронізуйте такі дублікати систем або компонентів системи: [*Призначення: визначені організацією дублікати систем або компонентів системи*].

Рекомендації з реалізації: SC-36 і CP-9(6) вимагають дублювання систем або компонентів системи у розподілених місцях. Синхронізація дубльованих і надлишкових служб і даних допомагає гарантувати, що інформація, що міститься в розподілених розташуваннях, може бути використана в місії або бізнес-функціях організацій, якщо це необхідно.

Пов'язані заходи: CP-9.

Посилання: [SP 800-160-2].

## SC-37 ПОЗАСМУГОВІ КАНАЛИ

Заходи захисту:

Використовувати [*Призначення: визначені організацією позасмугові канали*] для фізичного доставлення або електронної передачі [*Призначення: визначена організацією інформація, системні компоненти або пристрої*] до [*Призначення: визначені організацією особи або системи*].

Рекомендації з реалізації: Позасмугові канали включають локальний доступ до систем. Використання позасмугових каналів протиставляється використанню внутрішньосмугових каналів (тобто тих самих каналів), якими передається звичайний операційний трафік. Позасмугові канали не мають такої ж вразливості та незахищеності, як внутрішньосмугові. Тому порушення конфіденційності, цілісності або доступності внутрішньосмугових каналів не призведе до компрометації або негативного впливу на позасмугові канали. Організації можуть використовувати позасмугові канали для доставки або передачі елементів організації, включаючи автентифікатори та облікові дані; криптографічні ключі; управлінську інформацію; резервні копій системи та даних; змін в управлінні конфігурацією апаратного, мікропрограмного чи програмного забезпечення; оновлень безпеки; інформації про технічне обслуговування; та оновлень захисту від зловмисного оновлення захисту.

Пов’язані заходи: AC-2, CM-3, CM-5, CM-7, IA-2, IA-4, IA-5, MA-4, SC-12, SI-3, SI-4, SI-7.

Посилення заходів:

(1) ПОЗАСМУГОВІ КАНАЛИ - ЗАБЕЗПЕЧЕННЯ ДОСТАВЛЕННЯ ТА ПЕРЕДАЧІ

Впровадити [*Призначення: визначені організацією заходи безпеки*], щоб забезпечити, що тільки [*Призначення: визначені організацією особи або системи*] отримують [*Призначення: визначену організацією інформацію, компоненти системи або пристрої*].

Рекомендації з реалізації: Методи, що застосовується організаціями для забезпечення того, щоб лише визначені системи або особи отримували певну інформацію, системні компоненти або пристрої, включають надсилання автентифікаторів через затверджену кур'єрську службу, але з вимогою до одержувачів показати певну форму посвідчення особи з фотографією, видане урядом, як умову отримання.

Пов’язані заходи: Немає.

Посилання: [SP 800-57-1], [SP 800-57-2], [SP 800-57-3].

## SC-38 БЕЗПЕКА ОПЕРАЦІЙ

Заходи захисту:

Впровадити [*Призначення: визначені організацією заходи з безпеки операцій*] для захисту ключової організаційної інформації протягом усього життєвого циклу розробки системи.

Рекомендації з реалізації: Операційна безпека (OPSEC) - це систематичний процес, за допомогою якого потенційні супротивники можуть бути позбавлені інформації про можливості та наміри організації шляхом виявлення, контролю та захисту загальнодоступної інформації, яка безпосередньо стосується планування та виконання чутливих видів діяльності організації. Процес OPSEC складається з п'яти етапів: ідентифікація критично важливої інформації, аналіз загроз, аналіз вразливостей, оцінка ризиків і застосування відповідних контрзаходів. Заходи захисту OPSEC застосовуються до систем і середовищ організації, в яких ці системи функціонують. Заходи захисту OPSEC захищають конфіденційність інформації, в тому числі обмежують обмін інформацією з постачальниками, потенційними постачальниками та іншими позаорганізаційними елементами та особами. Інформація, критична для місії та бізнес-функцій організації, включає ідентифікаційні дані користувачів, постачальників, процеси ланцюга чання функціональні вимоги, вимоги безпеки, специфікації проектування системи, протоколи тестування та оцінки, а також деталі впровадження заходів захисту.

Пов’язані заходи: CA-2, CA-7, PL-1, PM-9, PM-12, RA-2, RA-3, RA-5, SA-12, SC-7, SR-3, SR-7.

Посилення заходів: Немає.

Посилання: Немає.

## SC-39 ІЗОЛЯЦІЯ ПРОЦЕСУ

Заходи захисту:

Підтримувати окремий домен виконання для кожного процесу, що виконується в системі.

Рекомендації з реалізації: Системи можуть підтримувати окремі домени виконання для кожного процесу, що виконується, шляхом призначення кожному процесу окремого адресного простору. Кожен процес системи має окрему адресу, щоб зв'язок між процесами здійснювався у спосіб, контрольований за допомогою функцій безпеки і один процес не міг модифікувати виконуваний код іншого процесу. Підтримка окремих доменів виконання для процесів, що виконуються, може бути досягнута, наприклад, реалізацією окремих адресних просторів. Технології ізоляції процесів, включаючи пісочницю або віртуалізацію, логічно відокремлюють програмне забезпечення та мікропрограму від іншого програмного забезпечення, мікропрограми та даних. Ізоляція процесів допомагає обмежити доступ потенційно ненадійного програмного забезпечення до інших ресурсів системи. Можливість підтримувати окремі домени виконання, доступна у комерційних операційних системах, які використовують багатопроцесорні технології.

Пов’язані заходи: AC-3, AC-4, AC-6, AC-25, SA-8, SC-2, SC-3, SI-16.

Посилення заходів:

(1) ІЗОЛЯЦІЯ ПРОЦЕСУ - АПАРАТНЕ РОЗДІЛЕННЯ

Впровадити механізми апаратного розділення для розділення процесів.

Рекомендації з реалізації: Апаратне розділення процесів системи, як правило, менш схильне до компрометації, ніж програмне розділення, що забезпечує більшу гарантію того, що розділення буде дотримано. Апаратні механізми розділення включають апаратну пам'ять керування.

Пов’язані заходи: Немає.

(2) ІЗОЛЯЦІЯ ПРОЦЕСУ - ІЗОЛЯЦІЯ ПОТОКІВ

Підтримувати окремий домен виконання для кожного потоку в [*Призначення: визначена організацією багатопотокова обробка*].

Рекомендації з реалізації: Немає.

Пов’язані заходи: Немає.

Посилання: [SP 800-160-1].

## SC-40 ЗАХИСТ БЕЗДРОТОВОГО З’ЄДНАННЯ

Заходи захисту:

Забезпечити захист зовнішніх і внутрішніх [*Призначення: визначені організацією бездротові з’єднання*] від [*Призначення: визначені організацією типи атак з параметрами сигналів або посилання на джерела для таких атак*].

Рекомендації з реалізації: Цей захід захисту застосовується до внутрішніх і зовнішніх бездротових комунікаційних ліній. Порушники можуть використовувати параметри

сигналу бездротових посилань, якщо такі посилання недостатньо захищені. Цей захід безпеки зменшує вплив атак на бездротові системи. Існує багато способів використання параметрів сигналу бездротового з'єднання для отримання інформації, заборони обслуговування або підробки користувачів системи. Захист бездротових з'єднань зменшує вплив атак, які є унікальними для бездротових систем. Якщо організації покладаються на комерційних постачальників послуг для послуг передачі як товарних одиниць, а не як повністю виділених послуг, може бути неможливо реалізувати захист бездротового зв'язку в тій мірі, яка необхідна для задоволення вимог організаційної безпеки

Пов'язані заходи: AC-18, SC-5.

Посилення заходів:

(1) ЗАХИСТ БЕЗДРОТОВОГО З'ЄДНАННЯ - ЕЛЕКТРОМАГНІТНІ ПЕРЕШКОДИ

Впровадити криптографічні механізми, що забезпечують [*Призначення: визначений організацією рівень захисту*] від впливу навмисних електромагнітних перешкод.

Рекомендації з реалізації: Впровадження криптографічних механізмів захисту від електромагнітних перешкод захищає системи від навмисного глушіння, яке може призвести до припинення або погіршення зв'язку, гарантуючи, що форми хвиль бездротового розширення спектру, які використовуються для захисту від завад, не можуть бути передбачуваними для сторонніх осіб. Впровадження криптографічних механізмів також може одночасно зменшити вплив ненавмисного глушіння через перешкоди від легальних передавачів, які використовують той самий спектр. Вимоги місії, прогнозовані загрози, концепція операцій, а також закони, виконавчі накази, директиви, положення, політики та стандарти визначають рівні доступності бездротового зв'язку.

Пов'язані заходи: SC-12, SC-13, PE-21.

(2) ЗАХИСТ БЕЗДРОТОВОГО З'ЄДНАННЯ - ЗМЕНШЕННЯ ПОТЕНЦІАЛУ ВИЯВЛЕННЯ

Впровадити криптографічні механізми для зменшення потенціалу виявлення бездротових з'єднань до [*Призначення: визначений організацією рівень зниження*].

Рекомендації з реалізації: Впровадження криптографічних механізмів для зменшення можливості виявлення використовується для прихованого зв'язку та захисту бездротових передавачів від геолокації. Це також гарантує, що форми хвиль розширеного спектру, які використовуються для досягнення низької ймовірності виявлення, не можуть бути передбачуваними сторонніми особами. Вимоги місії, прогнозовані загрози, концепція операцій, а також чинні закони, виконавчі накази, директиви, положення, політики та стандарти визначають рівні, до яких бездротові з'єднання неможливо виявити.

Пов'язані заходи: SC-12, SC-13.

(3) ЗАХИСТ БЕЗДРОТОВОГО З'ЄДНАННЯ - ІМІТАЦІЙНИЙ АБО МАНІПУЛЯТИВНИЙ ОБМІН ПОВІДОМЛЕННЯМИ

Впровадити криптографічні механізми для визначення та відхилення бездротових передач, які є навмисними спробами досягти імітаційного або маніпулятивного обміну повідомленнями на основі параметрів сигналу.

Рекомендації з реалізації: Реалізація криптографічних механізмів для виявлення та відхилення імітаційних або маніпулятивних комунікацій гарантує, що параметри сигналу бездротової передачі непередбачувані для сторонніх осіб. Така непередбачуваність зменшує ймовірність обману імітаційних або маніпулятивних комунікацій на основі лише параметрів сигналу.

Пов'язані заходи: SC-12, SC-13, SI-4.

(4) ЗАХИСТ БЕЗДРОТОВОГО З'ЄДНАННЯ - ВИЗНАЧЕННЯ ПАРАМЕТРІВ СИГНАЛУ

Впровадити криптографічні механізми для запобігання визначенню [*Призначення: визначені організацією бездротові передавачі*] за допомогою параметрів сигналу передавача.

Рекомендації з реалізації: Впровадження криптографічних механізмів для запобігання ідентифікації бездротових передавачів захищає від унікальної ідентифікації бездротових передавачів з метою розвідувального використання, гарантуючи, що анти-відбитки змін параметрів сигналу не можуть бути передбачуваними неавторизованими особами. Він також забезпечує анонімність, коли це необхідно. Методи радіодактилоскопії ідентифікують унікальний сигнал параметрів сигналу передавачів, щоб зняти з них відбитки пальців з метою відстежування та місії або ідентифікації користувача.

Пов'язані заходи: SC-12, SC-13.

Посилання: Немає.

## SC-41 ДОСТУП ДО ПОРТІВ ТА ПРИСТРОЇВ ВВЕДЕННЯ/ВИВЕДЕННЯ

Заходи захисту:

[*Вибір: фізично або логічно*] відключити або видалити [*Призначення: визначені організацією, порти підключення або пристрої введення/виводу*] у [*Призначення: визначені організацією системи або системні компоненти*].

Рекомендації з реалізації: До портів підключення належать USB порти та Firewire (IEEE 1394). До пристроїв введення/виведення (вводу/виводу) належать, наприклад, компакт-диски (CD) та цифрові відеодиски (DVD). Вимкнення або видалення таких портів підключення та пристроїв вводу/виводу допомагає запобігти несанкціонованому пересуванню інформації та введенню шкідливого коду в системи з цих портів або пристроїв. Фізичне відключення або видалення портів і/або пристроїв є сильнішим заходом.

Пов'язані заходи: AC-20, MP-7.

Посилення заходів: Немає.

Посилання: Немає.

## SC-42 МОЖЛИВОСТІ ДАТЧИКА ТА ДАНІ

Заходи захисту:

a. Заборонити дистанційну активацію можливостей зондування навколишнього середовища в системах організації або компонентах системи за такими виключеннями: [*Призначення: визначені організацією виключення, в яких допускається дистанційна активація датчиків*].

b. Забезпечити явну вказівку використання датчика для [*Призначення: визначений організацією клас користувачів*].

Рекомендації з реалізації: Цей захід безпеки часто застосовується до типів систем або компонентів системи, які характеризуються як мобільні пристрої, наприклад, смартфони та планшети. Ці системи часто містять датчики, які можуть збирати та записувати дані щодо місця перебування. До датчиків, вбудованих у мобільні пристрої, належать, наприклад, камери, мікрофони, механізми глобальної системи позиціювання (GPS) та акселерометри. Хоча датчики на мобільних пристроях забезпечують важливу функцію, такі пристрої можуть потенційно забезпечити порушників цінною інформацією про людей та організації. Наприклад, дистанційна активація функції GPS на мобільному пристрої може забезпечити порушнику можливість відстежувати конкретні пересування людини.

Пов'язані заходи: SC-15.

Посилення заходів:

(1) МОЖЛИВОСТІ ДАТЧИКА ТА ДАНІ - ЗВІТУВАННЯ ПЕРЕД УПОВНОВАЖЕНИМИ АБО ПОСАДОВИМИ ОСОБАМИ

Переконатися, що система налаштована таким чином, щоб дані або інформація, зібрані [*Призначення: визначеними організацією датчиками*], повідомлялися лише уповноваженим або посадовим особам.

Рекомендації з реалізації: У ситуаціях, коли датчики активуються уповноваженими особами, існує ймовірність, що дані або інформація, зібрана датчиками, буде надіслана неавторизованим особам.

Пов'язані заходи: Немає.

(2) МОЖЛИВОСТІ ДАТЧИКА ТА ДАНІ - ДОЗВОЛЕНЕ ВИКОРИСТАННЯ

Застосуйте такі заходи, щоб дані або інформація, зібрана [*Призначення: датчики, визначені організацією*], використовувалася лише для авторизованих цілей: [*Призначення: заходи, визначені організацією*].

Рекомендації з реалізації: Інформація, зібрана датчиками для певної дозволеної мети, може бути використана з несанкціонованою метою. Наприклад, датчики GPS, які використовуються для підтримки навігації за дорожнім рухом, можуть бути використані з метою відстеження переміщень людей. Заходи щодо пом'якшення такої діяльності включають додаткове навчання, щоб гарантувати, що уповноважені особи не зловживають своїми повноваженнями, а у випадку, коли дані датчиків зберігаються зовнішніми сторонами, договірні обмеження на використання таких даних.

Пов’язані заходи: PT-2.

(3) МОЖЛИВОСТІ ДАТЧИКА ТА ДАНІ - ЗАБОРОНА ВИКОРИСТАННЯ ПРИСТРОЇВ

[Вилучено: включено до SC-42].

(4) МОЖЛИВОСТІ ДАТЧИКА ТА ДАНІ - ПОВІДОМЛЕННЯ ПРО ЗБІР

Впровадити наступні заходи для повідомлення осіб про збір персональних даних [*Призначення: визначеними організацією датчиками*]: [*Призначення: визначені організацією заходи*].

Рекомендації з реалізації: Усвідомлення того, що датчики організації збирають дані, дозволяє людям більш ефективно долучатися до управління своєю приватністю. Заходи можуть включати звичайні письмові повідомлення та конфігурації датчиків, які прямо чи опосередковано інформують людей через інші пристрої про те, що датчик збирає інформацію. Зручність та ефективність повідомлення є важливими мірами.

Пов’язані заходи: PT-1, PT-4, PT-5.

(5) МОЖЛИВОСТІ ДАТЧИКА ТА ДАНІ - МІНІМІЗАЦІЯ ЗБОРУ

Впровадити [*Призначення: визначені організацією датчики*], які налаштовані на мінімізацію збору непотрібних персональних даних.

Рекомендації з реалізації: Політики контролю за санкціонованим використанням можуть бути застосовані до інформації після її збору, мінімізація збору непотрібної інформації зменшує ризик конфіденційності в точці входу в систему і зменшує ризик збоїв у контролі політики. Конфігурації датчиків передбачають приховування людських рис, наприклад, розмиття або пікселізацію зображення.

Пов’язані заходи: SA-8, SI-12.

Посилання: [OMB A-130], [SP 800-124].

## SC-43 ОБМЕЖЕННЯ ВИКОРИСТАННЯ

Заходи захисту:

a. Встановити обмеження на використання та рекомендації щодо впровадження для [*Призначення: визначених організацією компонентів системи*].

b. Проводити авторизацію, спостереження та контроль використання таких компонентів у системі.

Рекомендації з реалізації: Цей захід безпеки застосовується до всіх компонентів системи, включно з дротовими та бездротовими периферійними компонентами (наприклад, копіювальними апаратами, принтерами, сканерами). Обмеження щодо використання та вказівки щодо впровадження мають базуватися на ймовірнісному оцінюванні можливості завдання шкоди системі.

Пов’язані заходи: AC-18, AC-19, CM-6, SC-7, SC-18.

Посилення заходів: Немає.

Посилання: [OMB A-130], [SP 800-124].

## SC-44 ЕКРАНОВАНІ КАМЕРИ

Заходи захисту:

Впровадити екрановані камери в [*Призначення: визначену організацією систему, компонент системи або місце розташування*].

Рекомендації з реалізації: Екрановані камери, також відомі як динамічні середовища виконання, дозволяють організаціям відкривати вкладення електронної пошти, запускати ненадійні або підозрілі програми та виконувати запити Universal Resource Locator безпечно в ізольованому середовищі. Ці захищені та ізольовані середовища виконання забезпечують спосіб визначення того, чи містять асоційовані застосунки або програми шкідливий код. Цей захід безпеки призначений для швидкого виявлення шкідливого коду та зменшення ймовірності того, що код поширяться в користувальницьких середовищах (або повністю запобігає такому розповсюдженню).

Пов'язані заходи: SC-7, SC-25, SC-26, SC-30, SC-35, SI-3, SI-7, SC-18, SC-39.

Посилення заходів: Немає.

Посилання: Немає.

## SC-45 СИНХРОНІЗАЦІЯ СИСТЕМИ З ЧАСОМ

Заходи захисту: Синхронізація системного годинника в системі та компонентах системи і між ними.

Рекомендації з реалізації: Синхронізація часу годинників системи необхідна для правильного виконання багатьох служб системи, включаючи процеси ідентифікації та автентифікації, сертифікати та обмеження часу доби як частину контролю доступу. Відмова в обслуговуванні або неможливість відхилити облікові дані, термін дії яких закінчився, може призвести до відсутності належної синхронізації годинника в системі та компонентах системи і між ними. Час зазвичай виражається всесвітнім координованим часом (UTC), сучасним продовженням середнього часу за Гринвічем (GMT) або місцевим часом із зміщенням від UTC. Деталізація вимірювань часу стосується ступеня синхронізації між системними годинниками та еталонними годинниками, наприклад годинниками, що синхронізуються в межах сотень мілісекунд або десятків мілісекунд. Організації можуть визначати різні параметри часу для компонентів системи. Служба часу може бути критичною для інших можливостей безпеки, таких як контроль доступу, ідентифікація та автентифікація, залежно від характеру механізмів, які використовуються для підтримки можливостей.

Пов'язані заходи: AC-3, AU-8, IA-2, IA-8.

Посилення заходів:

(1) СИНХРОНІЗАЦІЯ СИСТЕМИ З ЧАСОМ - СИНХРОНІЗАЦІЯ З АВТОРИТЕТНИМ ДЖЕРЕЛОМ ЧАСУ

a) Порівняйте внутрішні системні годинники [*Призначення: частота, визначена організацією*] з [*Призначення: визначене організацією авторитетне джерело часу*];

b) Синхронізувати внутрішні системні годинники з офіційним джерелом часу, коли різниця в часі перевищує [*Призначення: період часу, визначений організацією*].

Рекомендації з реалізації: Синхронізація внутрішнього системного годинника з авторитетним джерелом забезпечує однаковість позначок часу для систем із кількома системними годинниками та систем, підключених через мережу.

Пов'язані заходи: Немає.

(2) СИНХРОНІЗАЦІЯ СИСТЕМИ З ЧАСОМ - ВТОРИННЕ АВТОРИТЕТНЕ ДЖЕРЕЛО ЧАСУ

a) Визначте вторинне авторитетне джерело часу, яке знаходиться в іншому географічному регіоні, ніж основне авторитетне джерело часу;

b) Синхронізуйте внутрішні системні годинники з вторинним авторитетним джерелом часу, якщо основне авторитетне джерело часу недоступне.

Рекомендації з реалізації: Може знадобитися інформація про геолокацію, щоб визначити, що вторинне авторитетне джерело часу знаходиться в іншому географічному регіоні.

Пов'язані заходи: Немає.

Посилання: [IETF 5905].

## SC-46 ЗАБЕЗПЕЧЕННЯ ВИКОНАННЯ МІЖДОМЕННОЇ ПОЛІТИКИ

Заходи захисту:

Впровадити механізм примусового виконання політики [*Вибір: фізично; логічно*] між фізичними та/або мережевими інтерфейсами для підключених доменів безпеки.

Рекомендації з реалізації: Для логічних механізмів застосування політики організації уникають створення логічного шляху між інтерфейсами, щоб запобігти можливості обійти механізм застосування політики. Для фізичних механізмів примусового виконання політики може знадобитися надійність фізичної ізоляції, що забезпечується фізичною реалізацією примусового виконання політики, щоб запобігти присутності логічних прихованих каналів, що проникають у область безпеки.

Пов'язані заходи: AC-4, SC-7.

Посилення заходів: Немає.

Посилання: [SP 800-160-1].

## SC-47 АЛЬТЕРНАТИВНИЙ ШЛЯХ ЗВ'ЯЗКУ

Заходи захисту:

Встановіть [*Призначення: альтернативні шляхи зв'язку, визначені організацією*] для організаційного управління та контролю операцій системи.

Рекомендації з реалізації: Ворожий інцидент, може порушити встановлені шляхи зв'язку, які використовуються для операцій системи, організаційного командування та контролю. Альтернативні шляхи зв'язку зменшують ризик того, що всі шляхи зв'язку

постраждають від одного і того ж інциденту. Проблема ускладнюється тим, що нездатність посадових осіб організації отримати своєчасну інформацію про збої або своєчасно вказати оперативним елементам шлях зв'язку після інциденту може вплинути на здатність організації своєчасно реагувати на такі інциденти. Встановлення альтернативних шляхів зв'язку для цілей командування та управління, включаючи призначення альтернативних осіб, які приймають рішення, якщо основні особи, які приймають рішення, недоступні, і встановлення обсягу та обмежень їхніх дій, може значно полегшити здатність організації продовжувати роботу та вживати відповідних заходів під час інциденту.

Пов'язані заходи: CP-2, CP-8.

Посилення заходів: Немає.

Посилання: [SP 800-34], [SP 800-61], [SP 800-160-2].

## SC-48 ПЕРЕМІЩЕННЯ ДАТЧИКА

Заходи захисту:
Перенесіть [*Призначення: датчики та можливості моніторингу, визначені організацією*] до [*Призначення: місця, визначені організацією*] за таких умов або обставин: [*Призначення: умови або обставини, визначені організацією*].

Рекомендації з реалізації: Зловмисники можуть обирати різні шляхи та використовувати різні підходи, коли вони просуваються організацією (включно з її системами), щоб досягти своєї мети, або намагаються викрасти інформацію з організації. Організація часто має лише обмежений набір можливостей моніторингу та виявлення, і вони можуть бути зосереджені на критичних або можливих шляхах проникнення чи ексфільтрації. Використовуючи шляхи зв'язку, які організація зазвичай не контролює, супротивник може збільшити свої шанси на досягнення бажаних цілей. Перемістивши свої датчики або можливості моніторингу в нові місця, організація може перешкодити здатності супротивника досягти своїх цілей. Переміщення датчиків або можливостей моніторингу може здійснюватися на основі інформації про загрози, отриманої організацією, або випадковим чином, щоб збити з пантелику супротивника та ускладнити йому прохід через систему чи організацію.

Пов'язані заходи: AU-2, SC-7, SI-4.

Посилення заходів:

(1) ДИНАМІЧНЕ ПЕРЕМІЩЕННЯ СЕНСОРІВ ТА МОНІТОРИНГ МОЖЛИВОСТЕЙ

Динамічно перемістіть [*Призначення: датчики та можливості моніторингу, визначені організацією*] до [*Призначення: місця, визначені організацією*] за таких умов або обставин: [*Призначення: умови або обставини, визначені організацією*].

Рекомендації з реалізації: Немає.

Пов'язані заходи: Немає.

Посилання: [SP 800-160-2].

## SC-49 ПРИМУСОВЕ АПАРАТНЕ РОЗДІЛЕННЯ ТА ПОЛІТИКА ЗАБЕЗПЕЧЕННЯ ВИКОНАННЯ

Заходи захисту:
Впровадити механізми апаратного поділу та застосування політики між [*Призначення: домени безпеки, визначені організацією*].

Рекомендації з реалізації: Власникам систем може знадобитися додаткова потужність механізму та надійність, щоб забезпечити розділення доменів і застосування політики для певних типів загроз і робочих середовищ. Апаратне примусове розділення та застосування політики забезпечують більшу міцність механізму, ніж програмне розділення.

Пов'язані заходи: AC-4, SA-8, SC-50.

Посилення заходів: Немає.

Посилання: [SP 800-160-1].

## SC-50 ПРИМУСОВЕ ПРОГРАМНЕ РОЗДІЛЕННЯ ТА ПОЛІТИКА ЗАБЕЗПЕЧЕННЯ ВИКОНАННЯ

Заходи захисту:
Впровадити програмне розділення та механізми застосування політики між [*Призначення: домени безпеки, визначені організацією*].

Рекомендації з реалізації: Власникам систем може знадобитися додаткова потужність механізму для забезпечення розділення доменів і забезпечення виконання політики для певних типів загроз і операційних середовищ.

Пов'язані заходи: AC-3, AC-4, SA-8, SC-2, SC-3, SC-49.

Посилення заходів: Немає.

Посилання: [SP 800-160-1].

## SC-51 АПАРАТНИЙ ЗАХИСТ

Заходи захисту:

a. Використовуйте апаратний захист від запису для [*Призначення: системні мікропрограмні компоненти, визначені організацією*];

b. Запровадити спеціальні процедури для [*Призначення: уповноважені особи, визначені організацією*], щоб вручну вимкнути захист від запису апаратного забезпечення для модифікацій мікропрограми та повторно ввімкнути захист від запису перед поверненням до робочого режиму.

Рекомендації з реалізації: Немає.

Пов'язані заходи: Немає.

Посилення заходів: Немає.

Посилання: Немає.

## 10.19 Клас заходів захисту SI — ЦІЛІСНІСТЬ СИСТЕМИ ТА ІНФОРМАЦІЇ

### SI-1 ПОЛІТИКА ТА ПРОЦЕДУРИ ЦІЛІСНОСТІ ІНФОРМАЦІЇ

Заходи захисту:

a. Розробити, задокументувати та поширити серед [*Призначення: визначеного організацією персоналу або посадових осіб*]:

1. Політику цілісності системи та інформації, яка:

(a) містить мету, сферу застосування, ролі, обов'язки, відповідальність керівництва, координацію між організаційними підрозділами та систему контролю відповідності (complaince);

(b) відповідає чинному законодавству, виконавчим наказам, директивам, нормам, політикам, стандартам і керівним принципам.

2. Процедури, що сприяють впровадженню політики цілісності системи та інформації, а також пов'язані з нею заходи цілісності системи та інформації.

a. Призначити [*Призначення: визначена організацією посадова особа*] для управління політикою та процедурами цілісності системи та інформації.

b. Переглядати й оновлювати:

1. поточну політику цілісності системи та інформації [*Призначення: визначена організацією частота*];

2. поточні процедури цілісності системи та інформації [*Призначення: визначена організацією частота*].

Рекомендації з реалізації: Цей захід захисту стосується встановлення політики та процедур для ефективного здійснення заходів і їх посилень у класі SI. При розробці таких політик та процедур важливо враховувати стратегію управління ризиками. Для забезпечення цілісності систем та інформації необхідна взаємодія програм забезпечення безпеки та приватності при створенні відповідних політик та процедур. Якщо на рівні організації наявні достатньо ефективні політики та процедури забезпечення безпеки та приватності, їх можна використовувати для всіх місій та систем організації. Для забезпечення безпеки та приватності важливо розглянути можливість створення процедур для програм забезпечення, процесів місій або бізнесу та систем в цілому. Політика може бути частиною загальної політики з безпеки та приватності, або представлена кількома політиками, що відображають складну архітектуру організацій. Для кожного з цих аспектів можна створити відповідні процедури, які описують впровадження політик та заходів захисту. Ці процедури повинні мати чіткі напрямки і описувати, як їх виконувати відповідно до конкретної фізичної чи посадової особи, яка є об'єктом такої процедури. Процедури можуть бути описані у планах забезпечення безпеки та приватності систем, в одному або декількох окремих документах. Події, що можуть призвести до оновлення політики та процедур забезпечення цілісності систем та інформації включають відомості, отримані в ході оцінки або аудиту, випадки порушення безпеки або несанкціонованого доступу, а також у зв'язку зі змінами в законодавстві, директивах, політиках, стандартах та настановах. Повторення заходів захисту не може бути політикою або процедурою

організації. Організація повинна мати якісну та структуровану політику та процедури щодо забезпечення безпеки та приватності, які охоплюють не лише заходи захисту, а й інші аспекти безпеки, такі як збір, зберігання та обробка даних, контроль доступу, здійснення моніторингу тощо. Простий перелік заходів захисту не може забезпечити повної безпеки та приватності.

Пов’язані заходи: PM-9, PS-8, SA-8, SI-12.

Посилення заходів: Немає.

Посилання: [OMB A-130], [SP 800-12], [SP 800-100].

## SI-2 ВИПРАВЛЕННЯ ДЕФЕКТІВ

Заходи захисту:

a. Виявляти, виправляти та повідомляти про недоліки системи.

b. Перед установкою перевірити програмне забезпечення та оновлення вбудованого програмного забезпечення, що пов’язані з усуненням дефектів, на ефективність та можливі побічні ефекти.

c. Інсталювати оновлення програмного забезпечення та оновлення вбудованого програмного забезпечення в межах [*Призначення:визначений організацією певний період часу*] випуску оновлень.

d. Внести виправлення помилок в процес управління конфігурацією організації.

Рекомендації з реалізації: Потреба у виправленні помилок системи застосовується до всіх типів програмного та апаратного забезпечення. Організації визначають системи, що постраждали від програмних помилок, включаючи потенційні вразливості, що виникають через ці помилки, та повідомляють цю інформацію призначеному персоналу організації, який відповідає за інформаційну безпеку та приватність. Оновлення, пов'язані з безпекою, включають усунення помилок, пакети обслуговування та підписи на зловмисний код. Організації також вирішують питання, пов'язані з помилками, які виявлені під час оцінки, постійного моніторингу, дій у випадку інцидентів та обробки помилок системи. Шляхом включення виправлення помилок до процесу керування конфігурацією можна відстежувати та підтверджувати виконання необхідних заходів з виправлення.

Оновлення програмного та апаратного забезпечення, що впливає на безпеку, здійснюється у терміни, визначені організацією, тривалість яких може відрізнятися залежно від різноманітних факторів ризику, включаючи категорію безпеки системи, критичність оновлення (тобто ступінь вразливості, пов'язаної з виявленою помилкою), рівня прийняття організацією можливих ризиків, місію, яку підтримує система, або середовище загроз. Деякі види виправлень помилок потребують більш детального тестування, ніж інші. Організації визначають тип тестування, необхідний для конкретного типу діяльності з виправлення дефектів, а також змін, які підлягають конфігураційному управлінню. У деяких ситуаціях організації можуть прийняти рішення, що тестування оновлень програмного або апаратного забезпечення не є необхідним або практичним, наприклад, при впровадженні простих оновлень сигнатур шкідливого коду. Приймаючи рішення про тестування, організації враховують

наявність оновлення програмного або апаратного забезпечення, які впливають на безпеку, отриманого з авторизованих джерел з відповідними цифровими підписами.

Пов'язані заходи: CA-5, CM-3, CM-4, CM-5, CM-6, CM-8, MA-2, RA-5, SA-8, SA-10, SA-11, SI-3, SI-5, SI-7, SI-11.

Посилення заходів:

(1) ВИПРАВЛЕННЯ ДЕФЕКТІВ - ЦЕНТРАЛІЗОВАНЕ УПРАВЛІННЯ

[Вилучено: включено до PL-9].

(2) ВИПРАВЛЕННЯ ДЕФЕКТІВ - АВТОМАТИЗОВАНЕ ВИПРАВЛЕННЯ ДЕФЕКТІВ

Впровадити автоматизовані механізми [*Призначення: визначена організацією частота*] для визначення стану компонентів системи стосовно усунення дефектів.

Рекомендації з реалізації: Автоматизовані механізми можуть відстежувати і визначати стан відомих дефектів компонентів системи.

Пов'язані заходи: CA-7, SI-4.

(3) ВИПРАВЛЕННЯ ДЕФЕКТІВ - ЧАС ДЛЯ УСУНЕННЯ ДЕФЕКТІВ ТА ОРІЄНТИРИ ДЛЯ КОРИГУВАЛЬНИХ ДІЙ

(a) Вимірювати час між виявленням та виправленням дефектів.

(b) Встановити [*Призначення: визначені організацією орієнтири*] для вжиття коригувальних дій.

Рекомендації з реалізації: Організації визначають середній час, необхідний для виправлення дефектів системи після їх виявлення та подальше встановлення часових рамок для здійснення коригувальних дій. Бенчмарки можуть бути встановлені за типом дефекту або ступенем потенційної вразливості, якщо дефект може бути використаний.

Пов'язані заходи: Немає.

(4) ВИПРАВЛЕННЯ ДЕФЕКТІВ - АВТОМАТИЧНІ ЗАСОБИ УПРАВЛІННЯ ВИПРАВЛЕННЯМИ

Використовуйте автоматизовані інструменти управління виправленнями, щоб полегшити усунення дефектів для наступних компонентів системи: [*Призначення: системні компоненти, визначені організацією*].

Рекомендації з реалізації: Використання автоматизованих інструментів для підтримки управління патчами допомагає забезпечити своєчасність та повноту операцій зі встановлення патчів в системах.

Пов'язані заходи: Немає.

(5) ВИПРАВЛЕННЯ ДЕФЕКТІВ - АВТОМАТИЧНЕ ОНОВЛЕННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Встановлювати [*Призначення: визначене організацією відповідне оновлення програмного забезпечення та вбудованого програмного забезпечення*] автоматично на [*Призначення: визначені організацією компоненти системи*].

Рекомендації з реалізації: З метою забезпечення цілісності та доступності системи організації запроваджують методологію використання автоматичних оновлень. Організації збалансовують потребу в негайному встановленні оновлень з необхідністю збереження управління конфігураціями та контролю можливих наслідків для місії або операцій, які можуть виникнути внаслідок таких автоматичних оновлень.

Пов'язані заходи: Немає.

(6) ВИПРАВЛЕННЯ ДЕФЕКТІВ - ВИДАЛЕННЯ ПОПЕРЕДНІХ ВЕРСІЙ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Видаляти попередні версії [*Призначення: визначені організацією компоненти програмного забезпечення та вбудованого програмного забезпечення*] після інсталяції оновлених версій.

Рекомендації з реалізації: Попередні версії програмного забезпечення або компонентів мікропрограмного забезпечення, які не видаляються із системи після встановлення оновлень, можуть використовуватися порушниками. Деякі продукти можуть автоматично видаляти попередні версії програмного забезпечення та мікропрограмного забезпечення із системи.

Пов'язані заходи: Немає.

Посилання: [OMB A-130], [FIPS 140-3], [FIPS 186-4], [SP 800-39], [SP 800-40], [SP 800-128], [IR 7788].

## SI-3 ЗАХИСТ ВІД ШКІДЛИВОГО КОДУ

Заходи захисту:

a. Впровадити механізми захисту від шкідливого коду [*Вибір (один або кілька): на основі підпису; не на основі підпису*] на вході та виході системи для виявлення та знищення шкідливого коду.

b. Автоматично оновлювати механізми захисту від шкідливого коду, коли доступні нові випуски відповідно до політики та процедур управління конфігурацією.

c. Налаштовувати механізми захисту від шкідливого коду для:

1. Виконання періодичного сканування системи [*Призначення: визначена організацією частота*] і сканування файлів у реальному часі із зовнішніх джерел у [*Вибір (один або кілька); кінцевій точці; точці входу/виходу в мережу*], коли файли завантажуються, відкриваються або виконуються відповідно до політики організації.

2. [*Вибір (один або кілька): Блокування шкідливого коду; Відправлення шкідливого коду в карантин; Надсилання попередження адміністратору; [Призначення: визначена організацією дія*]] у відповідь на виявлення шкідливого коду.

d. Фіксувати отримання помилкових спрацьовувань під час виявлення й усунення шкідливого коду та, як наслідок, потенційного впливу на доступність системи.

Рекомендації з реалізації: До пунктів входу та виходу системи належать брандмауери, сервери віддаленого доступу, робочі станції, сервери електронної пошти, вебсервери, проксі-сервери, ноутбуки та мобільні пристрої. До шкідливого коду належать, наприклад, віруси, троянські коні та шпигунські програми. Шкідливий код також може бути замаскований у різних форматах, що містяться в стислих чи прихованих файлах, або в стеганоконтейнерах. Шкідливий код може проникати в системи різними способами, зокрема електронною поштою, через мережу Інтернет або через портативні пристрої (це можливо реалізувати, використовуючи наявні вразливості систем). Атаки на систему за допомогою зловмисного коду відбуваються через використання її вразливостей. Але існує багато технологій та методів, які можуть допомогти мінімізувати наслідки від зловмисного коду або взагалі їх усунути.
Механізми захисту від шкідливого коду включають технології на основі сигнатур і без використання сигнатур. Механізми без використання сигнатур включають методи виявлення на основі штучного інтелекту, які застосовують сигнатури для виявлення, аналізу та опису характеристик або поведінки шкідливого коду, і забезпечують контроль над таким кодом, для якого ще не існують сигнатури або його діючі сигнатури є неефективними. Шкідливий код, для якого діючі сигнатури ще не існують або можуть бути неефективними, може бути представленим як поліморфний шкідливий код (тобто код, що змінює сигнатури при реплікації). Механізми, що не базуються на сигнатурах, також включають технології на основі репутації. Крім вищезазначених технологій, можливі ефективні засоби запобігання виконанню несанкціонованого коду включають широко розповсюджене управління конфігурацією, контроль цілісності програмного забезпечення та програмне забезпечення для запобігання використанню небезпечного коду. Шкідливий код, такий як логічні бомби, використання вразливостей за допомогою створення бекдорів та інші типи атак, можуть бути виявлені в комерційному програмному забезпеченні, а також в програмному забезпеченні, розробленому під конкретні потреби, що може негативно вплинути на діяльність організації.
Якщо шкідливий код не можна виявлити за допомогою методів або технологій виявлення, організації використовують інші заходи захисту, такі як безпечні методи розробки програмного коду, управління та контроль конфігурацій системи, процеси довіреного здійснення закупівель та моніторинг, щоб переконатися, що програмне забезпечення виконує лише ті функції, для яких воно було призначене. В залежності від виявленого шкідливого коду, організації визначають подальші заходи реагування. На приклад, організації можуть встановлювати різні заходи реагування відповідно до виявлення шкідливого коду в різні моменти: під час періодичного сканування, при завантаженні підозрілих файлів або у разі виявлення зловмисного коду при спробі відкрити чи виконати файл.

Пов’язані заходи: AC-4, AC-19, CM-3, CM-8, IR-4, MA-3, MA-4, PL-9, RA-5, SC-7, SC-26, SC-28, SC-23, SC-44, SI-2, SI-4, SI-7, SI-8, SI-15.

Посилення заходів:

(1) ЗАХИСТ ВІД ШКІДЛИВОГО КОДУ - ЦЕНТРАЛІЗОВАНЕ УПРАВЛІННЯ

[Вилучено: включено до PL-9].

(2) ЗАХИСТ ВІД ШКІДЛИВОГО КОДУ - АВТОМАТИЧНІ ОНОВЛЕННЯ

[Вилучено: Включено до SI-3].

(3) ЗАХИСТ ВІД ШКІДЛИВОГО КОДУ - НЕПРИВІЛЕЙОВАНІ КОРИСТУВАЧІ

[Вилучено: Включено до AC-6(10)].

(4) ЗАХИСТ ВІД ШКІДЛИВОГО КОДУ - ОНОВЛЕННЯ ТІЛЬКИ ПРИВІЛЕЙОВАНИМИ КОРИСТУВАЧАМИ

Здійснювати оновлення механізмів захисту від шкідливого коду лише привілейованими користувачами.

Рекомендації з реалізації: Захисні механізми для шкідливого коду зазвичай класифікуються як програмне забезпечення, пов'язане з безпекою, і оновлюються тільки персоналом організації з відповідними привілеями доступу.

Пов’язані заходи: CM-5.

(5) ЗАХИСТ ВІД ШКІДЛИВОГО КОДУ - ПОРТАТИВНІ ПРИСТРОЇ ЗБЕРІГАННЯ ДАНИХ

[Вилучено: Включено до MP-7].

(6) ЗАХИСТ ВІД ШКІДЛИВОГО КОДУ - ТЕСТУВАННЯ ТА ВЕРИФІКАЦІЯ

(a) Перевіряти механізми захисту від шкідливого коду [*Призначення: визначена організацією частота*] шляхом введення в систему відомого доброякісного, нерозповсюджуваного тестового прикладу.

(b) Переконатися, що відбувається виявлення тестового прикладу та відповідного повідомлення про інциденти.

Рекомендації з реалізації: Немає.

Пов’язані заходи: CA-2, CA-7, RA-5.

(7) ЗАХИСТ ВІД ШКІДЛИВОГО КОДУ - ВИЯВЛЕННЯ БЕЗ ПІДПИСУ

[Вилучено: Включено до SI-3].

(8) ЗАХИСТ ВІД ШКІДЛИВОГО КОДУ - ВИЯВЛЕННЯ НЕАВТОРИЗОВАНИХ КОМАНД

a) Виявляти [*Призначення: визначені організацією неавторизовані команди операційної системи*] за допомогою інтерфейсу програмування прикладних програм ядра ОС на [*Призначення: визначені організацією системні апаратні компоненти*]

b) [*Вибір (один або більше): видати попередження; перевірити виконання команди; запобігти виконанню команди*].

Рекомендації з реалізації: Виявлення неавторизованих команд можна

використовувати для критичних інтерфейсів, що не базуються на ядрі операційної системи, включаючи інтерфейси з віртуальними машинами та привілейованими додатками. Неавторизовані команди операційної системи включають команди для функцій ядра з процесів системи, які не мають відповідного дозволу на виконання, а також команди для функцій ядра, які, навіть якщо вони є доцільними для процесів, можуть викликати підозру. Організації можуть визначити шкідливі команди, які потрібно виявляти. Це можна зробити шляхом використання різних параметрів, таких як тип команди, клас команди чи конкретний випадок команди. Крім того, організації можуть визначати компоненти обладнання за їх типом, самим компонентом, розташуванням в мережі чи комбінацією цих параметрів. Для різних типів, класів чи випадків шкідливих команд можуть бути вибрані різні заходи.

Пов'язані заходи: AU-2, AU-6, AU-12.

(9) ЗАХИСТ ВІД ШКІДЛИВОГО КОДУ - АВТЕНТИФІКАЦІЯ ВІДДАЛЕНИХ КОМАНД

[Вилучено: Включено до AC-17 (10)].

(10) ЗАХИСТ ВІД ШКІДЛИВОГО КОДУ - АНАЛІЗ ШКІДЛИВОГО КОДУ

(a) Використовувати [*Призначення: визначені організацією інструменти та методи*] для аналізу характеристик і поведінки шкідливого коду.

(b) Вносити результати аналізу шкідливого коду в процес реагування на інциденти та виправлення дефектів організації.

Рекомендації з реалізації: Використання спеціальних інструментів для аналізу шкідливого коду дозволяє організаціям отримати детальні знання про методи і прийоми зловмисників, а також про функціональність та мету конкретних випадків шкідливого коду. Це знання допомагає ефективніше захищати організацію від поточних та майбутніх загроз. Для аналізу шкідливого коду можна використовувати метод реверсної інженерії або моніторинг поведінки коду під час виконання.

Пов'язані заходи: Немає.

Посилання: [SP 800-83], [SP 800-125B], [SP 800-177].

## SI-4 МОНІТОРИНГ СИСТЕМИ

Заходи захисту:

a. Здійснювати моніторинг системи для виявлення:

1. атак та індикаторів потенційних атак відповідно до [*Призначення: встановлені організацією цілі моніторингу*];

2. Неавторизованих локальних, мережевих та віддалених підключень.

b. Визначати несанкціоноване використання системи через [*Призначення: визначені організацією методи та техніки*].

c. Застосовувати можливості внутрішнього моніторингу або розгортати пристрої моніторингу:

1. стратегічно в рамках системи для збору необхідної для організації суттєвої інформації;

2. у спеціальних місцях у системі для відстеження конкретних видів транзакцій, що мають інтерес для організації.

d. Захищати інформацію, отриману від засобів моніторингу вторгнень, від несанкціонованого доступу, модифікації та видалення.

e. Регулювати рівень активності системного моніторингу при зміні ризику для операцій і активів організації, фізичних осіб, інших організацій або держави.

f. Отримувати за результатами моніторингу системи юридичний висновок щодо діяльності.

g. Надавати [*Призначення: визначена організацією інформація про моніторинг системи*] до [*Призначення: визначений організацією персонал або посадові особи] [Вибір (один або кілька): за необхідності; [Призначення: визначена організацією частота*]].

Рекомендації з реалізації: Система моніторингу охоплює зовнішній та внутрішній моніторинг. До зовнішнього моніторингу належить спостереження за подіями, що відбуваються на межах системи. До внутрішнього моніторингу належить спостереження за подіями, що відбуваються всередині системи. Організації можуть контролювати системи засобами діяльності аудиту в режимі реального часу або спостерігаючи за іншими системними аспектами, такими як структури доступу, характеристики доступу тощо. Метою моніторингу є інформування про визначені події та управління ними. Моніторинг системи може здійснюватися за допомогою різноманітних інструментів і методів, включно з, наприклад, системами виявлення вторгнень, системами запобігання вторгненням, програмним забезпеченням захисту від шкідливого коду, засобами сканування, програмним забезпечення для моніторингу записів аудиту та програмним забезпеченням мережевого моніторингу.

Залежно від того, як налаштована система безпеки, розподіл та конфігурація пристроїв моніторингу можуть вплинути на швидкість передачі даних на ключових внутрішніх та зовнішніх точках мережі, а також в інших місцях мережі через затримки у передачі даних. Якщо виникає необхідність в керуванні швидкістю передачі даних, такі пристрої розміщують стратегічно та встановлюють як частину загальної системи безпеки для всієї організації. Стратегічні місця для розташування пристроїв моніторингу включають обрані граничні точки та місця, розташовані біля ключових серверів та серверних ферм, які є важливими для підтримки критичних додатків. Зазвичай пристрої моніторингу використовуються на керованих інтерфейсах, що пов'язані зі заходами захисту SC-7 та AC-17. Інформація, яка підлягає збору, залежить від моніторингових цілей організації та можливостей систем для їх досягнення. До конкретних типів транзакцій, які викликають зацікавленість, входить трафік протоколу передачі гіпертексту (HTTP), який обходить HTTP-проксі. Моніторинг системи є необхідною складовою програм постійного моніторингу та реагування на інциденти в організації, при цьому результати моніторингу виступають джерелом інформації для цих програм. Вимоги до моніторингу системи, включаючи необхідність певних видів моніторингу системи, можуть бути згадані в інших заходах захисту (AC-2g, AC-2(7), AC-2(12)(a), AC-17(1), AU13, AU-13(1), AU-13(2), CM-3f,

CM-6d, MA-3a, MA-4a, SC-5(3)(b), SC-7a, SC-7(24)(b), SC-18b, SC43b). Рівень моніторингу системи може бути змінений в залежності від інформації, наданої правоохоронними органами, розвідувальних служб або інших джерел. Законність процесу моніторингу системи визначається відповідно до чинних законів, виконавчих наказів, директив, правил, стандартів та рекомендацій..

Пов'язані заходи: AC-2, AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, AU-13, AU-14, CA-7, CM-3, CM-6, CM-8, CM-11, IA-10, IR-4, MA-3, MA-4, PL-9, PE-3, PM-12, PM-24, RA-5, SA-18, SC-7, SC-18, SC-26, SC-31, SC-35, SC-36, SC-37, SI-3, SI-6, SI-7, SR-9, SR-10.

Посилення заходів:

(1) МОНІТОРИНГ СИСТЕМИ - ЗАГАЛЬНОСИСТЕМНА СИСТЕМА ВИЯВЛЕННЯ ВТОРГНЕНЬ (IDS)

Підключати та налаштовувати окремі засоби виявлення вторгнень у загальну систему виявлення вторгнень.

Рекомендації з реалізації: Послідовне поєднання окремих засобів виявлення вторгнень у систему в систему загального виявлення вторгнень забезпечує додаткове охоплення та ефективні можливості виявлення. Інформація, яка міститься в одному засобі виявлення вторгнень, може бути широко розповсюджена в організації, що робить систему загального виявлення більш стійкою та потужною.

Пов'язані заходи: CM-6.

(2) МОНІТОРИНГ СИСТЕМИ - АВТОМАТИЗОВАНІ ЗАСОБИ ТА МЕХАНІЗМИ АНАЛІЗУ В РЕАЛЬНОМУ ЧАСІ

Впровадити автоматизовані засоби та механізми для підтримки аналізу подій у режимі, близькому до реального часу.

Рекомендації з реалізації: Автоматизовані засоби та механізми включають засоби та механізми моніторингу подій, які базуються на хостах, сховищах, мережевих чи транспортних пристроях, або технології управління інформацією та подіями безпеки (SIEM), які забезпечують аналіз в режимі реального часу попереджень та повідомлень, що генеруються системами організації. Автоматизовані засоби та механізми моніторингу можуть створювати небажані ризики конфіденційності, оскільки вони можуть підключатися до зовнішніх систем, які не мають прямого зв'язку з моніторинговою системою організації. Відповідно, порівняння записів цих систем може створювати зв'язки з непередбачуваними наслідками. Організації оцінюють та документують ці ризики у своїй оцінці впливу на приватність та готують рішення, які відповідають їхньому плану програми приватності.

Пов'язані заходи: PM-23, PM-25.

(3) МОНІТОРИНГ СИСТЕМИ - АВТОМАТИЗОВАНІ ЗАСОБИ ТА МЕХАНІЗМИ ІНТЕГРАЦІЇ

Впровадити автоматизовані засоби та механізми для інтеграції інструментів і механізмів виявлення вторгнень у механізми контролю доступу та контролю

потоків.

Рекомендації з реалізації: Використання автоматизованих засобів і механізмів інтеграції засобів та механізмів виявлення вторгнень у механізми контролю доступу та потоку сприяє швидкому реагуванню на атаки, дозволяючи переконфігурувати ці механізми для усунення атаки.

Пов’язані заходи: PM-23, PM-25.

(4) МОНІТОРИНГ СИСТЕМИ - ТРАФІК ВХІДНИХ І ВИХІДНИХ КОМУНІКАЦІЙ

a) Визначити критерії незвичайної або несанкціонованої діяльності або умов для вхідного та вихідного комунікаційного трафіку;

b) Проводити моніторинг вхідного та вихідного комунікаційного трафіку [*Призначення: визначена організацією частота*] для виявлення незвичайних або несанкціонованих дій чи умов.

Рекомендації з реалізації: Виявлення незвичайних або несанкціонованих активностей в системі, пов'язаних з вхідним і вихідним трафіком комунікації, може відображати наявність ризику в області кібербезпеки, так як ці дії можуть вказувати на присутність зловмисного коду або несанкціонованого використання легітимного коду або облікових даних. Ці ризики можуть мати наслідки, такі як поширення вірусів та несанкціоноване виведення інформації за межі системи. Виявлення таких ризиків допомагає виявити потенційно скомпрометовані системи чи компоненти системи.

Пов’язані заходи: Немає.

(5) МОНІТОРИНГ СИСТЕМИ - СИСТЕМНІ СПОВІЩЕННЯ

Попереджати [*Призначення: визначені організацією персонал або посадові особи*], коли виникають наступні системні ознаки компрометації або потенційної компрометації: [*Призначення: визначені організацією показники компрометації*].

Рекомендації з реалізації: Інформація про можливі загрози може бути отримана з різних джерел, включаючи записи аудиту, механізми захисту від шкідливих програм, системи виявлення та запобігання вторгнень та захисні пристрої, такі як мережеві екрани, шлюзи та маршрутизатори. Ця інформація може бути автоматизованою та передаватися телефонним зв'язком, електронною поштою або текстовими повідомленнями. Особи, які можуть отримувати інформацію про загрози, включають адміністраторів систем, власників бізнесу або місії, власників систем, керівників інформаційних ресурсів, вищих посадовців з питань інформаційної безпеки, вищих посадовців з питань приватності, офіцерів з питань безпеки систем або приватності. Оповіщення, згенеровані системою, відрізняються від оповіщень, згенерованих організаціями в рамках SI-4(12), оскільки останній зосереджується на джерелах інформації, які знаходяться поза системою, наприклад, повідомлення про підозрілу діяльність та звіти про потенційні внутрішні загрози.

Пов’язані заходи: AU-4, AU-5, PE-6.

(6) МОНІТОРИНГ СИСТЕМИ - ЗАБОРОНА ДЛЯ НЕПРИВІЛЕЙОВАНИХ КОРИСТУВАЧІВ

[Вилучено: Включено до AC-6(10)].

(7) МОНІТОРИНГ СИСТЕМИ - АВТОМАТИЧНЕ РЕАГУВАННЯ НА ПІДОЗРІЛІ ПОДІЇ

a) Повідомляти [*Призначення: визначений організацією персонал реагування на інциденти (ідентифікований за іменем та/або посадою)*] про виявлені підозрілі події

b) Вжити наступні заходи після виявлення: [*Призначення: визначені організацією мінімально руйнівні дії для припинення підозрілих подій*].

Рекомендації з реалізації: До мінімально руйнівних дій належить ініціювання запитів на відповіді.

Пов’язані заходи: Немає.

(8) МОНІТОРИНГ СИСТЕМИ - ЗАХИСТ ІНФОРМАЦІЇ МОНІТОРИНГУ

[Вилучено: Включено до SI-4].

(9) МОНІТОРИНГ СИСТЕМИ - ТЕСТУВАННЯ ЗАСОБІВ І МЕХАНІЗМІВ МОНІТОРИНГУ

Тестувати інструменти та механізми моніторингу вторгнень з [*Призначення: визначена організацією частота*].

Рекомендації з реалізації: Тестування засобів і механізмів моніторингу необхідне для забезпечення їхнього правильного функціонування. Частота та глибина тестування залежить від типів засобів та механізмів, що використовуються організаціями, та методів їх впровадження.

Пов’язані заходи: Немає.

(10) МОНІТОРИНГ СИСТЕМИ - ВИДИМІСТЬ ЗАШИФРОВАНИХ КОМУНІКАЦІЙ

Вживати заходи, щоб [*Призначення: визначений організацією зашифрований трафік зв’язку*] було видно на [*Призначення: визначені організацією засоби та механізми моніторингу системи*].

Рекомендації з реалізації: Організації забезпечують баланс між потребою шифрування трафіку комунікацій для захисту конфіденційності даних та необхідністю зберігання видимості такого трафіку з точки зору моніторингу. Вони визначають, чи застосовується вимога щодо видимості внутрішнього зашифрованого трафіку, а також призначеного для зовнішніх адресатів, чи до підмножини типів трафіку.

Пов’язані заходи: Немає.

(11) МОНІТОРИНГ СИСТЕМИ - АНАЛІЗ АНОМАЛІЙ ТРАФІКУ КОМУНІКАЦІЙ

Проводити аналіз трафіку вихідних комунікацій на зовнішній межі системи та в

окремих [*Призначення: визначених організацією внутрішніх точках всередині системи*] для виявлення аномалій.

Рекомендації з реалізації: Визначені організацією внутрішні точки включають підмережі та підсистеми. Аномалії в системах організацій включають передачу великих файлів, тривалі постійні підключення, спроби отримати доступ до інформації з неочікуваних місць, використання незвичайних протоколів та портів, використання невідстежуваних мережевих протоколів (наприклад, використання IPv6 під час переходу з IPv4) та спроби зв'язку з підозрілими зовнішніми адресами.

Пов’язані заходи: Немає.

(12) МОНІТОРИНГ СИСТЕМИ - СТВОРЕНІ ОРГАНІЗАЦІЄЮ АВТОМАТИЗОВАНІ СПОВІЩЕННЯ

Впровадити автоматизовані механізми для оповіщення [*Призначення: визначені організацією персонал або посадові особи*], коли виникають такі ознаки невідповідної або незвичайної діяльності з наслідками для безпеки чи приватності: [*Призначення: визначені організацією заходи, які спричиняють сповіщення*].

Рекомендації з реалізації: До посадових осіб організації, які відповідають за обробку сповіщень, належать адміністратори систем, власники місій або бізнесу, власники систем, старша посадова особа з питань інформаційної безпеки, старша посадова особа з питань приватності, офіцер з інформаційної безпеки системи або офіцер з приватності. Повідомлення про попередження щодо безпеки генеруються організацією та передаються за допомогою автоматизованих засобів. Організація отримує інформацію для створення цих повідомлень від різних джерел, наприклад, звітів про підозрілу діяльність або потенційних внутрішніх загроз. Порівняно з повідомленнями, що генеруються організацією, повідомлення, які генеруються системою в рамках SI-4 (5), зосереджуються на джерелах інформації, які є внутрішніми для систем, такими як записи аудиту.

Пов’язані заходи: Немає.

(13) МОНІТОРИНГ СИСТЕМИ - АНАЛІЗ ТРАФІКУ ТА ШАБЛОНІВ ПОДІЙ

(a) Аналізувати трафік і шаблони подій для системи.

(b) Розробити профілі, що представляють загальну модель трафіку та шаблони подій.

(c) Використовувати профілі трафіку та подій у налаштуванні пристроїв моніторингу системи, щоб зменшити кількість помилкових позитивних і негативних спрацювань.

Рекомендації з реалізації: Розпізнавання та розуміння загальних зразків комунікаційного трафіку та подій допомагає організаціям надавати корисну інформацію пристроям моніторингу систем для більш ефективного виявлення підозрілого або аномального трафіку та подій. Така інформація може допомогти зменшити кількість помилкових спрацювань та недостовірних результатів під час моніторингу системи.

Пов’язані заходи: Немає.

(14) МОНІТОРИНГ СИСТЕМИ - ВИЯВЛЕННЯ БЕЗДРОТОВОГО ВТОРГНЕННЯ

Впровадити бездротову систему виявлення вторгнень, щоб визначати зловмисні бездротові пристрої та виявляти спроби атаки й потенційні компрометації або порушення системи.

Рекомендації з реалізації: Бездротові системи можуть випромінювати сигнали за межами об’єктів, що контролюються організацією. Організації мають активно проводити пошук несанкціонованих бездротових з’єднань, включно з ретельним скануванням несанкціонованих бездротових точок доступу. Сканування повинно проводитися не тільки на території системи, а також захоплювати області поза її межами для перешкоджання їх функціонуванню.

Пов’язані заходи: AC-18, IA-3.

(15) МОНІТОРИНГ СИСТЕМИ - ПЕРЕХІД ВІД БЕЗДРОТОВОГО ЗВ’ЯЗКУ ДО ПРОВІДНИХ МЕРЕЖ

Впровадити систему виявлення вторгнень для моніторингу трафіку бездротового зв’язку, коли трафік переходить від бездротових до провідних мереж.

Рекомендації з реалізації: Немає.

Пов’язані заходи: AC-18.

(16) МОНІТОРИНГ СИСТЕМИ - ЗІСТАВЛЕННЯ ІНФОРМАЦІЇ МОНІТОРИНГУ

Зіставляти інформацію з інструментів і механізмів моніторингу, що використовуються в системі.

Рекомендації з реалізації: Зіставлення інформації, отриманої за допомогою різних інструментів і механізмів моніторингу може забезпечити всебічний огляд діяльності системи. Зіставлення засобів моніторингу систем, які зазвичай працюють відокремлено один від одного, включаючи програмне забезпечення захисту від зловмисного коду, моніторинг хостів та мережевий моніторинг, може забезпечити організації загальний огляд моніторингу та виявити раніше невидимі шаблони атак. Розуміння можливостей та обмежень різноманітних інструментів та механізмів моніторингу та те, як максимально використовувати інформацію, яку вони генерують, може допомогти організаціям розробляти, виконувати та підтримувати ефективні програми моніторингу. Співставлення інформації моніторингу особливо важливо під час переходу від старих до нових технологій (наприклад, перехід від протоколів мережі IPv4 до IPv6).

Пов’язані заходи: AU-6.

(17) МОНІТОРИНГ СИСТЕМИ - ІНТЕГРОВАНА СИТУАЦІЙНА ОБІЗНАНІСТЬ

Зіставляти інформацію, отриману через моніторинг фізичної та кібердіяльності, а також діяльності ланцюга постачання, з метою досягнення інтегрованої, всеосяжної ситуаційної обізнаності.

Рекомендації з реалізації: Комбінування інформації з різних джерел дозволяє

отримати повну картину ситуації, що називається інтегрованою ситуаційною свідомістю. Це допомагає організаціям швидко виявляти складні атаки та вивчати застосовані методи та техніки за допомогою фізичного, кібернетичного моніторингу та моніторингу постачання. На відміну від SI-4(16), який фокусується на кібернетичному моніторингу, інтегрована ситуаційна свідомість включає кореляцію моніторингу не тільки в кібернетичній сфері, але і за її межами. Це означає, що за допомогою кореляції інформації з різних джерел можна виявляти атаки на організації, які здійснюються за декількома векторами.

Пов'язані заходи: AU-16, PE-6, SR-2, SR-4, SR-6.

(18) МОНІТОРИНГ СИСТЕМИ - АНАЛІЗ ТРАФІКУ ТА ПРИХОВАНОЇ ЕКСФІЛЬТРАЦІЇ

Аналізувати трафік вихідних комунікацій на зовнішній межі або периметрі системи та на [*Призначення: визначені організацією внутрішні точки всередині системи*] для виявлення прихованої ексфільтрації інформації.

Рекомендації з реалізації: До визначених організацією внутрішніх точок системи належать підмережі та підсистеми. До прихованих засобів, які можуть бути використані для ексфільтрації інформації, належать, наприклад, стеганоконтейнери.

Пов'язані заходи: Немає.

(19) МОНІТОРИНГ СИСТЕМИ - ОСОБИ, ЯКІ СТАНОВЛЯТЬ БІЛЬШИЙ РИЗИК

Здійснювати [*Призначення: визначений організацією додатковий моніторинг*] осіб, які були визначені [*Призначенням: визначеними організацією джерелами*], як такі, що становлять підвищений рівень ризику.

Рекомендації з реалізації: Інформація про особи, що становлять більший ризик, може бути отримана з різних джерел, наприклад, з кадрових записів, від правоохоронних організацій тощо. Моніторинг конкретних осіб має тісно координуватися з посадовими особами з правових питань, безпеки, приватності та кадрових ресурсів. Моніторинг має проводитися відповідно до чинного законодавства.

Пов'язані заходи: Немає.

(20) МОНІТОРИНГ СИСТЕМИ - ПРИВІЛЕЙОВАНІ КОРИСТУВАЧІ

Реалізувати [*Призначення: визначений організацією додатковий моніторинг*] привілейованих користувачів.

Рекомендації з реалізації: Привілейовані користувачі є великим ризиком для безпеки інформації, оскільки мають доступ до більш чутливої інформації, включаючи дані, пов'язані з безпекою. Це може призвести до серйозної шкоди для систем та організацій, тому додатковий моніторинг привілейованих користувачів є необхідним заходом ризик менеджменту. Це дозволить вчасно виявляти можливі зловживання та приймати відповідні заходи для запобігання потенційній шкоді.

Пов'язані заходи: AC-18.

(21) МОНІТОРИНГ СИСТЕМИ - ВИПРОБУВАЛЬНІ ТЕРМІНИ

Реалізувати [*Призначення: визначений організацією додатковий моніторинг*] осіб під час [*Призначення: визначений організацією випробувальний період*].

Рекомендації з реалізації: Під час періоду випробувального терміну працівники не мають статусу постійного працівника в організації і не мають доступу до конфіденційної інформації, що зберігається в системі. У зв'язку з цим, додатковий моніторинг може допомогти виявити будь-яку потенційно шкідливу діяльність або неприпустиму поведінку.

Пов’язані заходи: AC-18.

(22) МОНІТОРИНГ СИСТЕМИ - НЕСАНКЦІОНОВАНІ ПОСЛУГИ МЕРЕЖІ

Виявляти послуги мережі, які не були дозволені або схвалені [*Призначення: визначені організацією процеси авторизації або затвердження*] та здійснити [*Вибір (один або більше): перевірка; попередження* [*Призначення: визначених організацією персоналу чи посадових осіб*]].

Рекомендації з реалізації: До несанкціонованих послуг мережі належать, наприклад, отримання послуг у сервісно-орієнтованих архітектурах, які не пройшли відповідну перевірку та не отримали акредитацію і, таким чином, можуть бути ненадійними.

Пов’язані заходи: CM-7.

(23) МОНІТОРИНГ СИСТЕМИ - ПРИСТРОЇ НА ОСНОВІ ХОСТА

Реалізувати [*Призначення: визначені організацією механізми моніторингу на основі хоста*] на [*Призначення: визначені організацією компоненти системи*].

Рекомендації з реалізації: До компонентів системи, у яких може бути реалізований моніторинг на основі хоста, належать, наприклад, сервери, ноутбуки та мобільні пристрої. Організації можуть розглянути можливість використання механізмів моніторингу на основі хоста від багатьох розробників або постачальників продуктів.

Пов’язані заходи: AC-18, AC-19.

(24) МОНІТОРИНГ СИСТЕМИ - ІНДИКАТОРИ КОМПРОМЕТАЦІЇ

Досліджувати, збирати та поширювати серед [*Призначення: визначені організацією персонал або посадових осіб*] ознаки компрометації.

Рекомендації з реалізації: Індикатори компрометації (IOC) - це сліди, які залишають зловмисники під час вторгнення на системи організації на рівні хосту або мережі. IOC надають цінну інформацію про компрометовані системи. Індикатори компрометації можуть включати створення значень ключів реєстру, а для мережевого трафіку – елементи універсального ресурсу (URL) або протоколу, що свідчать про наявність зловживань на серверах управління зловмисним кодом. Швидке поширення та використання індикаторів компрометації може покращити інформаційну безпеку, скорочуючи час, під час якого система і організація залишаються вразливими перед експлойтами чи атаками. Інформація про показники загроз, сигнатури, тактики, техніки,

процедури та інші індикатори компрометації може бути доступна через урядові та неурядові організації.Пов’язані заходи: AC-18.

(25) МОНІТОРИНГ СИСТЕМИ - АНАЛІЗ МЕРЕЖЕВОГО ТРАФІКУ

Забезпечити видимість мережевого трафіку на зовнішніх і ключових внутрішніх інтерфейсах системи, щоб оптимізувати ефективність пристроїв моніторингу.

Рекомендації з реалізації: Шифрований трафік, асиметричні маршрутизаційні архітектури, обмеження пропускної здатності та затримки, а також перехід від старіших до новіших технологій (наприклад, перехід від мережевого протоколу IPv4 до IPv6) можуть призвести до сліпих зон для організацій при аналізі мережевого трафіку. Збір, дешифрування, передобробка та розподіл лише відповідного трафіку на пристрої моніторингу може покращити ефективність та використання пристроїв і оптимізувати аналіз трафіку.

Пов’язані заходи: Немає.

Посилання: [OMB A-130], [FIPS 140-3], [SP 800-61], [SP 800-83], [SP 800-92], [SP 800-94], [SP 800-137].

## SI-5 ПОПЕРЕДЖЕННЯ, РЕКОМЕНДАЦІЇ ТА ДИРЕКТИВИ З БЕЗПЕКИ

Заходи захисту:

a. Отримувати системні попередження безпеки, рекомендації та директиви від [*Призначення: визначені організацією зовнішні організації*] на постійній основі.

b. Генерувати внутрішні попередження безпеки, рекомендації та директиви (за необхідністю).

c. Поширювати попередження, рекомендації та директиви безпеки для: [*Вибір (один або кілька):* [*Призначення: визначений організацією персонал або посадові особи]; [Призначення: визначені організацією елементи всередині організації]; [Призначення: визначені організацією зовнішні організації*]].

d. Впровадити директиви безпеки відповідно до встановлених термінів і повідомити організацію-емітента про ступінь невідповідності.

Рекомендації з реалізації: Команда CERT-UA генерує попередження та рекомендації щодо безпеки для підтримки поінформованості про ситуацію на державному рівні. Директиви з безпеки, які видаються уповноваженими органами, надають актуальну інформацію про стан речей на національному рівні. Дотримання вказівок таких директив допомагає знизити можливі негативні наслідки для конкретних систем.Пов’язані заходи: PM-15, RA-5, SI-2.

Посилення заходів:

(1) ПОПЕРЕДЖЕННЯ, РЕКОМЕНДАЦІЇ ТА ДИРЕКТИВИ З БЕЗПЕКИ - АВТОМАТИЧНІ ПОПЕРЕДЖЕННЯ ТА РЕКОМЕНДАЦІЇ

Впровадити автоматизовані механізми, щоб зробити попередження та рекомендації з безпеки доступними для всієї організації.

Рекомендації з реалізації: З міркувань безпеки організації необхідно регулярно аналізувати зміни у системах та середовищі її діяльності, щоб ідентифікувати можливі ризики. Інформація про попередження та поради щодо забезпечення безпеки допомагає приймати рішення, які призведуть до зменшення ризиків на різних рівнях управління: на рівні управління, місії, бізнес-процесів, а також на рівні інформаційних систем. Керівництво організації має забезпечувати поширення цієї інформації на всіх рівнях організації, щоб забезпечити успішне виконання місії та бізнес-функцій організації.

Пов'язані заходи: Немає.

Посилання: [SP 800-40].

## SI-6 ПЕРЕВІРКА ФУНКЦІЙ БЕЗПЕКИ ТА ПРИВАТНОСТІ

Заходи захисту:

a. Перевіряти правильність роботи [*Призначення: визначені організацією функції безпеки та приватності*].

b. Виконувати перевірку [*Вибір (один або кілька):* [*Призначення: визначені організацією системні перехідні стани*]; *за командою користувача з відповідними повноваженнями*; [*Призначення: визначена організацією частота*]].

c. Повідомляти [*Призначення: визначені організацією персонал або посадові особи*] про невдалі перевірки безпеки та приватності.

d. [*Вибір (один або кілька): Вимкнути систему; Перезапустити систему; [Призначення: визначені організацією альтернативні дії*]], коли виявляються аномалії.

Рекомендації з реалізації: Прикладами перехідних станів системи можуть бути: запуск, перезапуск системи, відключення та переривання роботи. До сповіщень належать, наприклад, показники індикаторів обладнання, електронні сповіщення адміністраторам та повідомлення на локальних консолях комп'ютерів. Перевірка функцій приватності має на меті переконатись, що заходи, які забезпечують приватність, працюють належним чином та були затверджені відповідною посадовою особою, відповідальною за приватність в організації, або що відповідні атрибути приватності використовуються відповідно до очікувань. Це відрізняється від перевірки функцій безпеки, яка ставить за мету переконатись, що заходи безпеки відповідають вимогам та стандартам безпеки.

Пов'язані заходи: CA-7, CM-4, CM-6, SI-7.

Посилення заходів:

(1) ПЕРЕВІРКА БЕЗПЕКИ ТА ФУНКЦІЙ ПРИВАТНОСТІ - СПОВІЩЕННЯ ПРО НЕУСПІШНЕ ПРОХОДЖЕННЯ ТЕСТІВ З БЕЗПЕКИ

[Вилучено: Включено до SI-6].

(2) ПЕРЕВІРКА БЕЗПЕКИ ТА ФУНКЦІЙ ПРИВАТНОСТІ - АВТОМАТИЗОВАНА ПІДТРИМКА РОЗПОДІЛЕНОГО ТЕСТУВАННЯ

Впровадити автоматизовані механізми для підтримки управління розподіленого тестування функцій безпеки та приватності.

Рекомендації з реалізації: Використання автоматизованих засобів для керування розподіленим тестуванням функцій допомагає гарантувати, що воно буде проведено з високою точністю, повнотою, вчасністю та ефективністю.

Пов'язані заходи: SI-2

(3) ПЕРЕВІРКА БЕЗПЕКИ ТА ФУНКЦІЙ ПРИВАТНОСТІ - ПОВІДОМЛЕННЯ ПРО РЕЗУЛЬТАТИ ПЕРЕВІРКИ

Повідомляти про результати перевірки функцій безпеки та приватності [*Призначення: визначені організацією персонал або посадові особи*].

Рекомендації з реалізації: До осіб, які можуть бути зацікавлені в результатах перевірки функцій забезпечення безпеки та приватності, відносяться офіцери забезпечення безпеки систем, старші посадові особи з питань інформаційної безпеки організації та старші посадові особи організації з питань приватності.

Пов'язані заходи: SI-4, SR-4, SR-5.

Посилання: [OMB A-130].

## SI-7 ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ

Заходи захисту:

Впровадити інструменти перевірки цілісності для виявлення несанкціонованих змін [*Призначення: визначеного організацією програмного забезпечення, вбудованого програмного забезпечення та інформації*].

Рекомендації з реалізації: Несанкціоновані зміни програмного забезпечення, вбудованого програмного забезпечення та інформації можуть статися через помилки чи шкідливу діяльність. До програмного забезпечення належать: операційні системи (з ключовими внутрішніми компонентами, такими як ядра, драйвери); програмне забезпечення проміжного рівня та застосунки. До вбудованого програмного забезпечення належить, наприклад, базова система вводу-виводу (BIOS). До інформації належать: дані, персональні дані та метадані, що містять атрибути безпеки та приватності й пов'язані з інформацією. Механізмами перевірки цілісності можуть бути: перевірка паритетності; циклічна перевірка надмірності; криптографічні геші та пов'язані з ними інструменти, які можуть автоматично контролювати цілісність систем і розміщених програм.

Пов'язані заходи: AC-4, CM-3, CM-7, CM-8, MA-3, MA-4, RA-5, SA-8, SA-9, SA-10, SA-18, SA-19, SA-12, SC-8, SC-12, SC-13, SC-28, SC-37, SI-3, SR-3, SR-4, SR-5, SR-6, SR-9, SR-10, SR-11.

Посилення заходів:

(1) ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - ПЕРЕВІРКА ЦІЛІСНОСТІ

Виконати перевірку цілісності [*Призначення: визначені організацією програмне забезпечення, вбудоване програмне забезпечення та інформація*] [*Вибір (один або більше): під час запуску; під час* [*Призначення: визначені організацією перехідні стани або події, що стосуються безпеки*]; [*Призначення: визначена організацією частота*]].

Рекомендації з реалізації: До подій, що стосуються безпеки, належать, наприклад, виявлення нової загрози, встановлення нового апаратного, програмного забезпечення чи вбудованого програмного забезпечення. Перехідні стани включають запуск, перезапуск, вимкнення та припинення роботи системи

Пов'язані заходи: Немає.

(2) ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - АВТОМАТИЧНІ СПОВІЩЕННЯ ПРО ПОРУШЕННЯ ЦІЛІСНОСТІ

Впровадити автоматизовані інструменти, які надсилають повідомлення до [*Призначення: визначені організацією персонал або посадові особи*] після виявлення розбіжностей під час перевірки цілісності.

Рекомендації з реалізації: Використання автоматизованих інструментів для повідомлення про порушення цілісності та своєчасне повідомлення уповноважених посадових осіб є важливим фактором ефективного реагування на ризик. Для ефективного відстеження цих ризиків, має бути залучений персонал з різних відділів організації, таких як власники місії та бізнесу, керівники відділу інформаційної безпеки та приватності, системні адміністратори, розробники програмного забезпечення, інтегратори систем, а також офіцери з інформаційної безпеки та приватності.

Пов'язані заходи: Немає.

(3) ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - ІНСТРУМЕНТИ ЦІЛІСНОСТІ З ЦЕНТРАЛІЗОВАНИМ УПРАВЛІННЯМ

Впровадити інструменти перевірки цілісності з централізованим управлінням.

Рекомендації з реалізації: Застосування централізованої системи управління інструментами перевірки цілісності дозволяє забезпечити більшу стабільність та послідовність у застосуванні цих інструментів, що, в свою чергу, допомагає здійснювати більш повну перевірку цілісності.

Пов'язані заходи: AU-3, SI-2, SI-8.

(4) ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - УПАКОВКА З ІНДИКАЦІЄЮ ОЗНАК ЇЇ НЕСАНКЦІОНОВАНОГО РОЗКРИТТЯ

[Вилучено: Включено до SA-12].

(5) ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - АВТОМАТИЧНІ ВІДПОВІДІ ПРО ПОРУШЕННЯ ЦІЛІСНОСТІ

Автоматично [*Вибір (один або більше): вимкнути систему; перезапустити систему; реалізувати* [*Призначення: визначені організацією захисні заходи*]], коли виявляються порушення цілісності.

Рекомендації з реалізації: Організації можуть визначати різні перевірки цілісності за типом інформації. Приклади типів інформації містять у собі інформацію щодо: програмного забезпечення, вбудованого програмного забезпечення та дані користувача, дані про завантажувальну прошивку для певних типів машин. До конкретної інформації відноситься загрузочна прошивка для певних типів машин. У разі несанкціонованих змін в критичних файлах безпеки, системи організації автоматично виконують контрольні дії, такі як скасування змін, зупинка системи або відправлення сигналів аудиту.

Пов’язані заходи: Немає.

(6) ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - КРИПТОГРАФІЧНИЙ ЗАХИСТ

Запровадити криптографічні механізми для виявлення несанкціонованих змін програмного забезпечення, вбудованого програмного забезпечення та інформації.

Рекомендації з реалізації: Щоб захистити цілісність даних, можна використовувати криптографічні методи. До таких методів належать цифрові підписи та обчислення підписаних гешів, які створюються за допомогою асиметричної криптографії. Це дозволяє захистити ключ, що використовується для створення гешу, та використовувати публічний ключ для перевірки гешу. Крім того, організації, які використовують криптографію, повинні займатися керуванням криптографічними ключами.

Пов’язані заходи: SC-12, SC-13.

(7) ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - ІНТЕГРАЦІЯ ВИЯВЛЕННЯ І РЕАГУВАННЯ

Внести виявлення наступних несанкціонованих змін у можливості організації реагувати на інциденти: [*Призначення: визначені організацією відповідні зміни в системі*].

Рекомендації з реалізації: Це посилення заходу допомагає гарантувати, що виявлені події відстежуються, виправляються і записи про них доступні в архіві. Ведення архівних записів важливо як для виявлення та розрізнення протилежних дій протягом тривалого періоду, так і для можливих юридичних дій. Зміни, що стосуються безпеки, містять, наприклад, несанкціоновані зміни встановлених параметрів конфігурації або несанкціоноване підвищення привілеїв системи.

Пов’язані заходи: AU-2, AU-6, IR-4, IR-5, SI-4.

(8) ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - АУДИТ ВАЖЛИВИХ ПОДІЙ

При виявленні потенційного порушення цілісності провести аудит події та ініціювати такі дії: [*Вибір (один або більше): створити запис аудиту*; *сповістити поточного користувача*; *сповістити* [*Призначення: визначені організацією персонал або посадові особи*]; *виконати* [*Призначення: визначені організацією інші дії*]].

Рекомендації з реалізації: Організації вибирають дії щодо реагування на основні типи програмного забезпечення, конкретного програмного забезпечення або інформації, щодо яких можливі порушення цілісності.

Пов'язані заходи: AU-2, AU-6, AU-12.

(9) ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - ПЕРЕВІРКА ПРОЦЕСУ ЗАВАНТАЖЕННЯ

Перевіряти цілісність процесу завантаження [*Призначення: визначених організацією компонент системи*].

Рекомендації з реалізації: Забезпечення цілісності завантажувальних процесів є критично важливим для запуску компонентів системи у відомих, надійних станах. Механізми перевірки цілісності забезпечують рівень впевненості, що під час завантаження виконується лише довірений код.

Пов'язані заходи: SI-6.

(10) ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - ЗАХИСТ ЗАВАНТАЖУВАЛЬНОГО ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Реалізувати [*Призначення: визначені організацією заходи безпеки*] для захисту цілісності завантажувального вбудованого програмного забезпечення [*Призначення: визначені організацією компоненти системи*].

Рекомендації з реалізації: Несанкціоновані зміни завантажувального програмного забезпечення можуть вказувати на наявність складної направленої атаки. Ці типи направлених атак можуть призвести до відмови в обслуговуванні або внесення шкідливого коду. Компоненти системи можуть захищати цілісність завантажувального вбудованого програмного забезпечення, перевіряючи цілісність і достовірність усіх оновлень перед застосуванням.

Пов'язані заходи: SI-6.

(11) ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - ОБМЕЖЕНЕ СЕРЕДОВИЩЕ З ОБМЕЖЕНИМИ ПРИВІЛЕЯМИ

Вимагати, щоб [*Призначення: визначене організацією програмне забезпечення, встановлене користувачем*] виконувалося в обмеженому фізичному або віртуальному середовищі з обмеженими правами.

Рекомендації з реалізації: Організації мають визначати програмне забезпечення, яке може спричинити занепокоєння щодо його походження або наявності в ньому шкідливого коду. Для цього типу програмного забезпечення користувацькі установки мають відбуватися в обмежених середовищах.

Пов'язані заходи: CM-11, SC-44.

(12) ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - ПЕРЕВІРКА ЦІЛІСНОСТІ

Вимагати перевірки цілісності [*Призначення: визначене організацією програмне забезпечення, встановлене користувачем*] перед виконанням.

Рекомендації з реалізації: Організації мають перевіряти цілісність встановленого користувачем програмного забезпечення перед його використанням, щоб зменшити ймовірність виконання шкідливого коду або коду, що містить помилки внаслідок несанкціонованих модифікацій. При цьому організації враховують практичність методів перевірки цілісності програмного забезпечення, включаючи можливість отримання достовірних контрольних сум від розробників та продавців програмного забезпечення..

Пов'язані заходи: CM-11.

(13) ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - ВИКОНАННЯ КОДУ В ЗАХИЩЕНИХ СЕРЕДОВИЩАХ

[Вилучено: включено до CM-7(7)].

(14) ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - ДВІЙКОВИЙ АБО МАШИННО-ВИКОНУВАНИЙ КОД

[Вилучено: включено до CM-7(8)].

(15) ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - АВТЕНТИФІКАЦІЯ КОДУ

Запровадити криптографічні механізми для автентифікації [*Призначення: визначене організацією програмне забезпечення або компоненти вбудованого програмного забезпечення*] перед його встановленням.

Рекомендації з реалізації: Криптографічна автентифікація передбачає, наприклад, перевірку того, що програмне забезпечення або його компоненти були підписані цифровим підписом з використанням чинних і визнаних організаціями сертифікатів.

Пов'язані заходи: CM-5, SC-12, SC-13.

(16) ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - ТЕРМІН ВИКОНАННЯ ПРОЦЕСУ БЕЗ НАГЛЯДУ

Заборонити виконання процесів без нагляду впродовж більш ніж [*Призначення: визначений організацією період часу*].

Рекомендації з реалізації: Обмеження часу на виконання процесів без нагляду призначено для процесів, для яких можна визначити типові або нормальні періоди виконання та випадки, коли організації перевищують такі періоди. Нагляд включає в себе таймери в операційних системах, автоматизовані відповіді та ручний нагляд та реакцію при виникненні аномалій системного процесу.

Пов'язані заходи: Немає.

(17) ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ – САМОЗАХИСТ ПРОГРАМ ВІД САМОВІЛЬНОГО ВИКОНАННЯ

Впровадити [*Призначення: визначені організацією заходи захисту*] для забезпечення захисту програм на етапі виконання.

Рекомендації з реалізації: Інструментарій захисту програм під час їх виконання використовується для виявлення та блокування використання вразливостей програмного забезпечення, використовуючи інформацію, отриману від програми, що вже запущена. Захист від вразливостей на етапі виконання програм відрізняється від традиційних методів захисту на основі периметру, таких як використання програм захисту та брандмауерів, які можуть лише виявляти та блокувати атаки на основі мережевої інформації без контекстного розуміння. Технологія самозахисту додатків під час виконання може знизити сприйнятливість програмного забезпечення до атак шляхом моніторингу його вхідних даних і блокування тих вхідних даних, які можуть призвести до атак. Це також дозволяє здійснювати захист середовища виконання від небажаних змін та втручань. Коли виявляється загроза, технологія самозахисту додатка в режимі виконання може запобігти його несанкціонованому застосуванню, а також вжити інших заходів (наприклад, надіслати користувачеві попередження, завершити сеанс користувача, завершити роботу додатка або надіслати сповіщення персоналу організації). Рішення самозахисту додатка в режимі виконання можуть бути встановлені в режимі моніторингу або захисту.

Пов'язані заходи: SI-6.

Посилання: [OMB A-130], [FIPS 140-3], [SP 800-61], [SP 800-83], [SP 800-92], [SP 800-94], [SP 800-137].

## SI-8 ЗАХИСТ ВІД СПАМУ

Заходи захисту:

a. Впровадити механізми захисту від спаму в точках входу та виходу системи, щоб виявляти та протидіяти небажаним повідомленням.

b. Оновлювати механізми захисту від спаму, коли доступні нові механізми відповідно до організаційної політики та процедур управління конфігурацією.

Рекомендації з реалізації: До точок входу та виходу системи належать, наприклад,

брандмауери, сервери віддаленого доступу, сервери електронної пошти, вебсервери, проксі-сервери, робочі станції, ноутбуки та мобільні пристрої. Спам може передаватися різними способами, включно з, наприклад, електронною поштою, вкладеннями електронної пошти та вебдоступом.

Пов'язані заходи: PL-9, SC-5, SC-7, SC-38, SI-3, SI-4.

Посилення заходів:

(1) ЗАХИСТ ВІД СПАМУ - ЦЕНТРАЛІЗОВАНЕ УПРАВЛІННЯ

Централізовано управляти механізмами захисту від спаму.

Рекомендації з реалізації: Централізоване управління — це управління на рівні організації. Централізоване управління охоплює планування, реалізацію, оцінювання, надання дозволів та моніторинг визначених організацією заходів щодо захисту від спаму.

Пов'язані заходи: AU-3, CM-6, SI-2, SI-7.

(2) ЗАХИСТ ВІД СПАМУ - АВТОМАТИЧНІ ОНОВЛЕННЯ

Автоматично оновлювати механізми захисту від спаму [Призначення: з визначеною організацією частотою].

Рекомендації з реалізації: Використання автоматизованих механізмів для оновлення механізмів захисту від спаму допомагає забезпечити регулярне оновлення та надання найсучасніших можливостей та засобів захисту.

Пов'язані заходи: Немає.

(3) ЗАХИСТ ВІД СПАМУ - БЕЗПЕРЕРВНЕ НАВЧАННЯ

Запровадити механізми захисту від спаму з можливістю навчання для ефективнішого визначення законного трафіку зв'язку.

Рекомендації з реалізації: До механізмів навчання належать: фільтри, які реагують на входи користувачів, ідентифікуючи конкретний трафік або як спам, або як законний; оновляючи при цьому параметри алгоритму і, тим самим, точніше розділяючи типи трафіку.

Пов'язані заходи: Немає.

Посилання: [SP 800-45], [SP 800-177].

## SI-9 ОБМЕЖЕННЯ НА ВВЕДЕННЯ ІНФОРМАЦІЇ

[Вилучено: включено до AC-2, AC-3, AC-5, AC-6].

## SI-10 ПЕРЕВІРКА ВВОДУ ІНФОРМАЦІЇ

Заходи захисту: Перевіряти дійсність [*Призначення: визначена організацією введена інформація*].

Рекомендації з реалізації: Перевірка дійсності синтаксису входів системи передбачає, наприклад, перевірку набору символів, довжину, числовий діапазон і підтвердження, що входи відповідають заданим формату та вмісту. Наприклад, якщо організація встановлює, що числові значення в діапазоні від 1 до 100 є єдиними прийнятними значеннями для використання в певній програмі, тоді такі введення як "387", "abc" або "%K%" є неприпустимими та не приймаються системою як вхідні дані. Коректні введення можуть бути різними в залежності від галузі програмного забезпечення. Зазвичай програмні застосунки дотримуються чітко визначених протоколів, які використовують структуровані повідомлення (тобто команди або запити) для взаємодії між модулями програмного забезпечення або компонентами системи. Структуровані повідомлення можуть містити сирі або неструктуровані дані, які переплітаються з метаданими або інформацією управління. Якщо програмні застосунки використовують вхідні дані, які були надані зловмисником, для створення структурованих повідомлень без належного кодування таких повідомлень, тоді зловмисник може вставити шкідливі команди або спеціальні символи, які можуть призвести до того, що дані будуть сприйматися як контрольна інформація або метадані. Як наслідок, модуль або компонент, що отримує пошкоджений вивід, буде виконувати неправильні операції або неправильно інтерпретувати отримані дані. Як наслідок, модуль або компонент, що отримує пошкоджені вихідні дані, буде виконувати неправильні операції або неправильно інтерпретувати отримані дані. Відсіювання вхідних даних перед їх подальшою обробкою допомагає запобігти ненавмисному розумінню їх як команд. Перевірка вхідних даних забезпечує точні та правильні введення та запобігає атакам, таким як кросс-сайт скриптинг та різні типи атак з інтегруванням зловмисного коду.

Пов’язані заходи: Немає.

Посилення заходів:

(1) ПЕРЕВІРКА ВВОДУ ІНФОРМАЦІЇ - МОЖЛИВІСТЬ РУЧНОГО ПЕРЕВИЗНАЧЕННЯ

(a) Забезпечити можливість ручного перевизначення для вхідної перевірки [*Призначення: визначені організацією входи*].

(b) Обмежити використання можливостей ручного перевизначення лише для [*Призначення: визначені організацією уповноважені особи*].

(c) Перевіряти використання можливостей ручного перевизначення.

Рекомендації з реалізації: У певних ситуаціях, наприклад, під час подій, визначених в планах забезпечення безперервної роботи та відновлення функціонування організації, може знадобитися можливість ручного виправлення для перевірки введення даних. Такі керовані засоби використовуються лише в обмежених обставинах і з визначеними організацією вхідними даними.

Пов’язані заходи: AC-3, AU-2, AU-12.

(2) ПЕРЕВІРКА ВВОДУ ІНФОРМАЦІЇ - ПЕРЕГЛЯД ТА УСУНЕННЯ ПОМИЛОК

Переглядати та усувати помилки перевірки вводу інформації в межах [*Призначення: визначений організацією період часу*].

Рекомендації з реалізації: Усунення помилок перевірки вхідних даних містить, наприклад, виправлення помилок системи і повторне подання транзакцій з виправленим входом.

Пов’язані заходи: Немає.

(3) ПЕРЕВІРКА ВВОДУ ІНФОРМАЦІЇ - ПРОГНОЗОВАНА ПОВЕДІНКА

Перевіряти, що система поводиться передбачуваним і документованим способом при отриманні недійсних вхідних даних.

Рекомендації з реалізації: Поширеною вразливістю в системах організації є непередбачувана поведінка при надходженні невірних вхідних даних. Перевірка прогнозованості системи допомагає забезпечити правильну роботи цієї системи в разі отримання неправильних вхідних даних. Перевірка прогнозованості системи допомагає гарантувати, що система поводиться прогнозовано при отриманні невірних вхідних даних. Неправильні вхідні дані це ті, які стосуються вхідної інформації, визначеної організацією в базовому заході захисту (SI-10).

Пов’язані заходи: Немає.

(4) ПЕРЕВІРКА ВВОДУ ІНФОРМАЦІЇ - ЧАСОВІ ВЗАЄМОДІЇ

Враховувати часові взаємодії між компонентами системи при визначенні доречних відповідей для невідповідних вхідних даних.

Рекомендації з реалізації: Коли система обробляє неправильні вхідні дані через протокольні інтерфейси, важливо враховувати взаємодію між протоколами і часом. Наприклад, стандарти бездротових мереж 802.11 не взаємодіють добре з протоколами передачі TCP, коли відбувається втрата пакетів (це може бути через неправильне введення пакету). Протокол TCP припускає, що втрати пакетів відбуваються через перевантаження, але насправді вони можуть бути викликані шумом або колізіями на каналі у випадку втрат при відправленні через 802.11. Якщо TCP відповідає на втрату пакету, припускаючи перевантаження, то це призведе до неправильних дій, які можуть бути використані зловмисниками для створення невірних вхідних даних, використовуючи взаємодію між протоколами для досягнення негативних наслідків. Невірні вхідні дані - це ті, що пов'язані з інформаційними вхідними даними, визначеними організацією в базовому заході захисту (SI-10).

Пов’язані заходи: Немає.

(5) ПЕРЕВІРКА ВВОДУ ІНФОРМАЦІЇ - ОБМЕЖЕННЯ ВХІДНИХ ДАНИХ ДОВІРЕНИМИ ДЖЕРЕЛАМИ ТА ЗАТВЕРДЖЕНИМИ ФОРМАТАМИ

Обмежити використання вхідних даних лише [*Призначення: визначені організацією довірені джерела*] і/або [*Призначення: визначені організацією формати*].

Рекомендації з реалізації: Це посилення заходу застосовує концепцію білого списку до вхідної інформації. Визначення відомих надійних джерел для введення інформації та прийнятних форматів для таких входів може зменшити ймовірність зловмисної активності.

Пов’язані заходи: AC-3, AC-6.

(6) ПЕРЕВІРКА ВВОДУ ІНФОРМАЦІЇ - ПРОФІЛАКТИКА ВВОДУ ДАНИХ

Запобігайте впровадженню ненадійних даних.

Рекомендації з реалізації: Впровадженню ненадійних даних можна запобігти за допомогою параметризованого інтерфейсу або екрануванням виводу (кодування виводу). Параметризовані інтерфейси відокремлюють дані від коду, щоб впровадження зловмисних або ненавмисних даних не могли змінити семантику команд, що надсилаються. Екранування вихідних даних використовує певні символи, щоб повідомити аналізатору інтерпретатора, чи є дані довіреними. Запобігання впровадженню ненадійних даних стосується інформаційних вводів, визначених організацією в базовому контролі (SI-10).

Пов'язані заходи: AC-3, AC-6.

Посилання: [OMB A-130].

## SI-11 ОБРОБКА ПОМИЛОК

Заходи захисту:

a. Створити повідомлення про помилки, які надають інформацію, необхідну для реалізації виправних дій, без виявлення інформації, що може бути використана.

b. Показувати повідомлення про помилки лише [*Призначення: визначений організацією персонал або посадові особи*].

Рекомендації з реалізації: Організації мають розглядати структуру та зміст повідомлень про помилки. Процедури обробки та порядок управління помилками керуються організаційною політикою та експлуатаційними вимогами. Необхідно враховувати, що повідомлення про помилки можуть надавати прихований канал для передачі інформації. Під час виникнення помилок у системі може бути розкрита важлива інформація, така як деталі реалізації програми, помилково введений пароль, що може бути використаний як ім'я користувача, або конфіденційна інформація, така як номери рахунків або кредитних карток. Більше того, повідомлення про помилки можуть бути використані як прихований канал для передачі інформації.

Пов'язані заходи: AU-2, AU-3, SC-31, SI-2.

Посилення заходів: Немає.

Посилання: Немає.

## SI-12 УПРАВЛІННЯ ТА ЗБЕРЕЖЕННЯ ІНФОРМАЦІЇ

Заходи захисту:

Управляти та зберігати інформацію всередині системи та виводити інформацію із системи відповідно до чинного законодавства, виконавчих наказів, директив, правил, політик, стандартів, керівних принципів та експлуатаційних вимог.

Рекомендації з реалізації: Вимоги до управління та збереження інформації мають охоплювати весь життєвий цикл інформації (в тому числі тоді, коли інформація покидає систему). Інформація, що підлягає збереженню, може також містити політику, процедури, плани та інші види адміністративної інформації. Якщо в організації є офіс з управління записами, розгляньте можливість координації з персоналом з управління записами. Записи, створені з результатів реалізації контролю, які можуть потребувати управління та зберігання, включають, але не обмежуються: всі XX-1 заходи захисту,

AC-6(9), AT-4, AU-12, CA-2, CA-3, CA-5, CA-6, CA-7, CA-8, CA-9, CM-2, CM-3, CM-4, CM-6, CM-8, CM-9, CM-12, CM-13, CP-2, IR-6, IR-8, MA-2, MA-4, PE-2, PE-8, PE-16, PE-17, PL-2, PL-4, PL-7, PL-8, PM-5, PM-8, PM-9, PM-18, PM-21, PM-27, PM-28, PM-30, PM-31, PS-2, PS-6, PS-7, PT-2, PT-3, PT-7, RA-2, RA-3, RA-5, RA-8, SA-4, SA-5, SA-8, SA-10, SI-4, SR-2, SR-4, SR-8.

Пов'язані заходи: Всі XX-1 заходи захисту, AC-16, AU-5, AU-11, CA-2, CA-3, CA-5, CA-6, CA-7, CA-9, CM-5, CM-9, CP-2, IR-8, MP-2, MP-3, MP-4, MP-6, PA-1, PA-2, PA-3, PL-2, PL-4, PM-4, PM-8, PM-9, PS-2, PS-6, PT-2, PT-6, RA-2, RA-3, SA-5, SA-8, SR-2.

Посилення заходів:

(1) УПРАВЛІННЯ ТА ЗБЕРЕЖЕННЯ ІНФОРМАЦІЇ - ОБМЕЖЕННЯ ЕЛЕМЕНТІВ ПЕРСОНАЛЬНИХ ДАНИХ

Обмежити обробку персональних даних у життєвому циклі інформації до [*Призначення: визначені організацією елементи*], визначених в оцінюванні ризику приватності.

Рекомендації з реалізації: Обмеження використання персональних даних життєвого циклу, коли вони не потрібні для оперативних цілей, сприяє зниженню рівня ризику приватності, створеного системою. Життєвий цикл охоплює генерацію, збір, використання, обробку, зберігання, обслуговування, розповсюдження, розкриття та знищення інформації. Оцінки ризиків, а також відповідні закони, нормативні акти та політики можуть стати корисними вхідними даними для визначення того, які елементи персональних даних можуть створити ризик.

Пов'язані заходи: PM-25.

(2) УПРАВЛІННЯ ТА ЗБЕРЕЖЕННЯ ІНФОРМАЦІЇ - МІНІМІЗАЦІЯ ВИКОРИСТАННЯ ПЕРСОНАЛЬНИХ ДАНИХ ПІД ЧАС ТЕСТУВАННЯ, НАВЧАННЯ ТА ДОСЛІДЖЕННЯ

Використовувати [*Призначення: визначені організацією методи*] для мінімізації використання персональних даних для досліджень, тестування або навчання, відповідно до оцінки ризику приватності. Оцінки ризиків, а також відповідні закони, нормативні акти та політики можуть надати корисні вхідні дані для визначення технік, які слід використовувати та коли слід їх використовувати.

Рекомендації з реалізації: Організації можуть мінімізувати ризик для приватності особи, використовуючи такі методи, як деідентифікація або штучно згенеровані дані. Обмеження використання персональних даних протягом життєвого циклу, коли вони не потрібні для дослідження, тестування чи навчання, допомагає знизити рівень ризику приватності.

Пов'язані заходи: PM-22, PM-25, SI-19.

(3) УПРАВЛІННЯ ТА ЗБЕРЕЖЕННЯ ІНФОРМАЦІЇ - ВИДАЛЕННЯ ІНФОРМАЦІЇ

Використовуйте наступні методи, щоб позбутися, знищити або стерти інформацію після періоду зберігання: [*Призначення: методи, визначені організацією*].

Рекомендації з реалізації: Організації можуть мінімізувати ризики безпеки та конфіденційності, видаляючи інформацію, коли вона більше не потрібна. Утилізація або знищення інформації стосується оригіналів, а також копій і архівних записів, включаючи системні журнали, які можуть містити персональну інформацію.

Пов'язані заходи: Немає.

Посилання: [USC 2901], [OMB A-130].

## SI-13 ЗАПОБІГАННЯ ПРОГНОЗОВАНИМ ЗБОЯМ

Заходи захисту:

a. Визначити середній час до збою (MTTF) для [*Призначення: визначені організацією компоненти системи*] в певних середовищах роботи.

b. Надати замінні компоненти системи та засоби для заміни активних компонентів резервними компонентами відповідно до [*Призначення: визначені організацією критерії заміни*].

Рекомендації з реалізації: Хоча MTTF в першу чергу стосується надійності, запобігання прогнозованим збоям призначене для вирішення можливих відмов компонентів системи, які забезпечують функціональні можливості безпеки. Відсоток збоївв відображає особливості налаштувань, а не середні показники всієї галузі. Організації визначають критерії для заміни компонентів системи на основі значення MTTF з урахуванням можливих наслідків від збоїв компонентів. Передача відповідальності між активними та резервними компонентами не порушує безпеку, готовність до роботи та функціональні можливості безпеки. Збереження змінних стану системи також критично для забезпечення успішного процесу передачі. Резервні компоненти залишаються доступними протягом усього часу, за винятком проблем з обслуговування або невдалих спроб відновлення.

Пов'язані заходи: CP-2, CP-10, CP-13, MA-2, MA-6, SA-8, SC-6.

Посилення заходів:

(1) ЗАПОБІГАННЯ ПРОГНОЗОВАНИМ ЗБОЯМ - ВІДПОВІДАЛЬНІСТЬ ЗА ПЕРЕДАЧУ ФУНКЦІЙ КОМПОНЕНТІВ

Знімати з експлуатації системні компоненти шляхом передачі функцій на резервні компоненти не пізніше, ніж [*Призначення: визначена організацією частина або відсоток*] середнього часу до збоїв.

Рекомендації з реалізації: Передача обов'язків основного компонента системи іншим компонентам-замінникам до виходу з ладу основного компонента є важливим процесом, метою якого є зменшення ризику погіршення або ослаблення місії чи бізнес-функцій. Проведення таких передач на основі значення відсотку середнього часу до відмови дозволяє організаціям бути проактивними не дивлячись на готовності до ризику. Однак передчасна заміна компонентів системи може призвести до збільшення вартості операцій системи.

Пов'язані заходи: Немає.

(2) ЗАПОБІГАННЯ ПРОГНОЗОВАНИМ ЗБОЯМ - ТЕРМІН ВИКОНАННЯ ПРОЦЕСУ БЕЗ НАГЛЯДУ

[Вилучено: включено до SI-7 (16)].

(3) ЗАПОБІГАННЯ ПРОГНОЗОВАНИМ ЗБОЯМ - РУЧНА ПЕРЕДАЧА ФУНКЦІЙ КОМПОНЕНТІВ

Вручну ініціювати передачу функцій між активними та резервними компонентами системи, коли використання активного компонента досягає [*Призначення: визначений організацією відсоток*] від середнього часу до збоїв.

Рекомендації з реалізації: Наприклад, якщо MTTF для компонента системи становить 100 днів, а відсоток MTTF, визначений організацією, становить 90 відсотків, перенесення вручну відбудеться через 90 днів.

Пов'язані заходи: Немає.

(4) ЗАПОБІГАННЯ ПРОГНОЗОВАНИМ ЗБОЯМ - ВСТАНОВЛЕННЯ РЕЗЕРВНИХ КОМПОНЕНТІВ ТА ОПОВІЩЕННЯ

Якщо виявлено збої компонентів системи:

(a) переконатися, що резервні компоненти успішно та прозоро встановлені в межах [*Призначення: визначений організацією період часу*];

(b) [*Вибір (один або більше): Активувати* [*Призначення: визначений організацією сигнал*]; *Автоматично вимкнути систему; виконати* [*Призначення:визначена організацією дія*]].

Рекомендації з реалізації: При виявленні відмов компонентів має бути забезпечено автоматичне або ручне перемикання на компоненти в режимі очікування.

Пов'язані заходи: Немає.

(5) ЗАПОБІГАННЯ ПРОГНОЗОВАНИМ ЗБОЯМ - МОЖЛИВІСТЬ АВАРІЙНОГО ПЕРЕМИКАННЯ

Забезпечити [*Вибір: в режимі реального часу; близько до реального часу*] [*Призначення: визначена організацією можливість аварійного перемикання*] для системи.

Рекомендації з реалізації: Аварійне перемикання означає автоматичне перемикання на альтернативну систему в разі відмови первинної системи. Функціональність автоматичного перемикання включає в себе використання дзеркальних операцій системи на альтернативних оброблювальних майданчиках або періодичне копіювання даних на регулярні інтервали, що визначаються періодами часу відновлення організацій.

Пов'язані заходи: CP-6, CP-7, CP-9.

Посилання: Немає.

## SI-14 НЕСТІЙКІСТЬ

Заходи захисту:
Реалізувати нестійкі [*Призначення: визначені організацією компоненти системи та служби*], які ініціюються у відомих станах і завершуються [*Вибір (один або кілька): після закінчення сеансу використання; періодично з [Призначення: визначена організацією частота*]].

Рекомендації з реалізації: Впровадження нестійких компонентів і служб знижує ризики від розширених постійних загроз (APT), зменшуючи здатність зловмисників націлюватися (тобто вікно можливостей і доступну поверхню атаки) для ініціювання та завершення атак. Реалізуючи концепцію нестійкості для вибраних компонентів системи, організації можуть надати надійний обчислювальний ресурс із відомим станом на певний період часу, який не дає зловмисникам достатньо часу для використання вразливостей в системах організації або операційних середовищах. Оскільки APT є висококласною, складною загрозою щодо можливостей, намірів і націлювання, організації припускають, що протягом тривалого періоду відсоток атак буде успішним. Непстійкі системні компоненти та служби активуються за потреби з використанням захищеної інформації та припиняються періодично або в кінці сеансів. Ненаполегливість збільшує ефективність противників, які намагаються скомпрометувати або зламати організаційні системи.

Нестійкості можна досягти шляхом оновлення компонентів системи, періодичного повторного створення образів компонентів або використання різноманітних поширених методів віртуалізації. Нестійкі служби можуть бути реалізовані за допомогою методів віртуалізації як частини віртуальних машин або як нові екземпляри процесів на фізичних машинах (постійних або непостійних). Перевага періодичних оновлень компонентів системи і служб полягає в тому, що організаціям не потрібно спочатку визначати, чи відбулося компрометування компонентів або служб (те, що часто важко визначити). Оновлення вибраних компонентів системи і служб відбувається з достатньою частотою, щоб запобігти поширенню або передбачуваному впливу атак, але не так часто, щоб зробити систему нестабільною. Оновлення критичних компонентів і служб може проводитися періодично, щоб перешкодити зловмисникам використовувати оптимальні вікна вразливостей.

Пов'язані заходи: SC-30, SC-34, SI-21.

Посилення заходів:

(1) НЕСТІЙКІСТЬ - ОНОВЛЕННЯ З НАДІЙНИХ ДЖЕРЕЛ

Отримувати програмне забезпечення та дані, що використовуються під час оновлення компонента системи та служби з [*Призначення: визначені організацією довірені джерела*].

Рекомендації з реалізації: Довірені джерела включають програмне забезпечення та дані з одноразового запису, лише для читання або з вибраних офлайн-захищених сховищ.

Пов'язані заходи: Немає.

(2) НЕСТІЙКІСТЬ - НЕСТІЙКА ІНФОРМАЦІЯ

а) [Вибір: Оновити [Призначення: інформація, визначена організацією] [*Призначення: частота, визначена організацією*]; Генерувати

[*Призначення: інформацію, визначену організацією] на вимогу*];

b) Видаляти інформацію, яка більше не потрібна.

Рекомендації з реалізації: Зберігання інформації довше, ніж потрібно, робить її потенційною мішенню для досвідчених зловмисників, які шукають високоцінні активи для компрометації шляхом несанкціонованого розголошення, несанкціонованої модифікації або викрадання. Для інформації, пов'язаної з системою, непотрібне збереження надає розширену інформацію для противників, яка може допомогти в їх розвідці та боковому переміщенні через систему.

Пов'язані заходи: Немає.

(3) НЕСТІЙКІСТЬ - НЕСТІЙКІ ПІДКЛЮЧЕННЯ

Встановлювати підключення до системи на вимогу та завершувати підключення після [*Вибір: завершення запиту; період невикористання*].

Рекомендації з реалізації: Постійні підключення до систем можуть надати досвідченим зловмисникам шляхи для бокового переміщення через системи та потенційно розташувати себе ближче до цінних активів. Обмеження доступності таких зв'язків перешкоджає можливості зловмисника вільно пересуватися через організаційні системи.

Пов'язані заходи: SC-10.

Посилання: Немає.

## SI-15 ФІЛЬТРАЦІЯ ВИХІДНИХ ДАНИХ

Заходи захисту:
Перевіряти інформацію, що виходить з [*Призначення: визначені організацією програмні продукти та/або застосунки*], щоб переконатися, що інформація відповідає очікуваному змісту.

Рекомендації з реалізації: Певні типи атак, зокрема, SQL-ін'єкції, можуть виводити результати, які неочікувані або несумісні з очікуваними результатами програмного забезпечення або додатків. Фільтрування вихідних даних інформації спрямоване на виявлення зайвого вмісту, запобігання його відображенню, а потім сповіщення інструментів моніторингу, що було виявлено аномальну поведінку.

Пов'язані заходи: SI-3, SI-4, SI-11.

Посилення заходів: Немає.

## SI-16 ЗАХИСТ ПАМ'ЯТІ

Заходи захисту:
Виконати [*Призначення: визначені організацією заходи безпеки*] для захисту системної пам'яті від несанкціонованого коду, що виконується.

Рекомендації з реалізації: Деякі зловмисники запускають атаки з метою виконання коду в тих областях пам'яті, які не призначені або заборонені для виконання коду. Для захисту пам'яті використовуються різні методи, включаючи запобігання виконанню даних та випадкове розташування адресного простору. Контроль запобігання виконанню даних може здійснюватися як апаратним, так і програмним шляхом, причому апаратний контроль надає більшу ефективність захисту.

Пов'язані заходи: AC-25, SC-3, SI-7.

Посилення заходів: Немає.

Посилання: Немає.

## SI-17 ВІДМОВОСТІЙКІ ПРОЦЕДУРИ

Заходи захисту:
Виконати [*Призначення: визначені організацією відмовостійкі процедури*], коли настають [*Призначення: визначені організацією умови виявлення несправностей*].

Рекомендації з реалізації: Відмовостійкі процедури включають попередження персоналу операторів та надання конкретних інструкцій щодо подальших дій в разі втрати зв'язку між критичними компонентами системи або між компонентами системи та оперативними підрозділами. Ці подальші дії можуть включати в себе не здійснення жодних дій, відновлення налаштувань системи, зупинку процесів, перезапуск системи або зв'язок з визначеним персоналом організації.

Пов'язані заходи: CP-12, CP-13, SC-24, SI-13.

Посилення заходів: Немає.

Посилання: Немає.

## SI-18 ОПЕРАЦІЇ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ДАНИХ

Заходи захисту:

a. Перевіряти точність, актуальність, своєчасність і повноту персональної інформації протягом її життєвого циклу [*Завдання: частота, визначена організацією*];

b. Виправляти або видаляти неточну або застарілу персональну інформацію.

Рекомендації з реалізації: Операції з якістю персональних даних включають кроки, які організації вживають для підтвердження точності та актуальності такої інформації протягом її життєвого циклу. Життєвий цикл включає створення, збір, використання, обробку, зберігання, підтримку, поширення, розголошення та видалення персональних даних. Операції з якістю персональних даних включають редагування та підтвердження адрес під час їх збору або введення в системи з використанням інтерфейсів автоматизованих додатків для верифікації адрес. Перевірка якості персональних даних включає відстеження оновлень та змін даних протягом часу, що дозволяє організаціям знати, як і що було змінено у цих даних, якщо були виявлені помилки. Заходи, прийняті для захисту якості персональних даних, ґрунтуються на характері та контексті самої інформації, на тому, як вона має використовуватись, на тому, як вона була отримана, та

на можливих методах деідентифікації, які були використані. Заходи, прийняті для підтвердження точності персональних даних, які використовуються для прийняття рішень щодо прав, пільг або привілеїв осіб, підпадаючих під державні програми, можуть бути більш комплексними, ніж заходи, прийняті для підтвердження точності персональних даних, які використовуються для менш чутливих цілей.

Пов'язані заходи: PM-22, PM-24, PT-2, SI-4.

Посилення заходів:

(1) ОПЕРАЦІЇ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ДАНИХ - АВТОМАТИЧНА ПІДТРИМКА

Виправляйте або видаляйте персональну інформацію, яка є неточною або застарілою, неправильно визначено щодо впливу або неправильно деідентифікована за допомогою [*Призначення: автоматизовані механізми, визначені організацією*].

Рекомендації з реалізації: Використання автоматизованих механізмів для покращення якості даних може ненавмисно створювати ризики конфіденційності. Автоматизовані інструменти можуть з'єднуватися із зовнішніми чи іншими непов'язаними системами, а зіставлення записів між цими системами може створювати зв'язки з непередбачуваними наслідками. Організації оцінюють і документують ці ризики у своїх оцінках впливу на приватйність і приймають рішення, які узгоджуються з їхніми планами програми приватності.

Оскільки дані отримуються та використовуються протягом усього життєвого циклу інформації, важливо підтвердити точність і релевантність персональних даних. Автоматизовані механізми можуть розширити існуючі процеси та процедури якості даних і дозволити організації краще ідентифікувати та керувати персональними даними у великомасштабних системах. Наприклад, автоматизовані інструменти можуть значно покращити роботу з постійної нормалізації даних або виявлення неправильних даних. Автоматизовані інструменти також можна використовувати для покращення перевірки даних і виявлення помилок, які можуть неправильно змінити персональні дані або пов'язати такі дані з неправильною особою. Автоматизовані можливості підтримують процеси та процедури в масштабі та забезпечують більш детальне виявлення та виправлення помилок якості даних.

Пов'язані заходи: PM-18, RA-8.

(2) ОПЕРАЦІЇ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ДАНИХ - ТЕГУВАННЯ ДАНИХ

Використовуйте теги даних для автоматизації виправлення або видалення персональних данихпротягом їхжиттєвого циклу в системах організації.

Рекомендації з реалізації: Додавання тегів до даних, які дозволяють ідентифікувати особу, включає теги, які вказують на дозволи на обробку, повноваження на обробку, деідентифікацію, рівень впливу, етап життєвого циклу даних та дати збереження або останнього оновлення. Використання тегів даних для персональних даних може підтримувати використання засобів автоматизації для виправлення або видалення відповідної персональних даних.

Пов'язані заходи: AC-3, AC-16, SC-16.

(3) ОПЕРАЦІЇ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ДАНИХ - ЗБИРАННЯ

Збирайте персональні дані безпосередньо від особи.

Рекомендації з реалізації: Окремі особи або призначені ними представники можуть бути джерелами правильних персональних даних. Організації враховують контекстуальні фактори, які можуть спонукати людей надавати правильні дані, а не помилкові. Додаткові кроки можуть знадобитися для підтвердження зібраної інформації на основі характеру та контексту персональних даних, способу їх використання та отримання. Заходи, вжиті для перевірки точності персональних даних, які використовуються для визначення прав, пільг або привілеїв осіб за державними програмами, можуть бути більш комплексними, ніж заходи, вжиті для перевірки менш конфіденційних персональних даних.

Пов'язані заходи: Немає.

(4) ОПЕРАЦІЇ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ДАНИХ - ІНДИВІДУАЛЬНІ ЗАПИТИ

Виправляти або видаляти особисті дані за запитом окремих осіб або їх призначених представників.

Рекомендації з реалізації: Неточні персональні дані, яку зберігають організації, може спричинити проблеми для окремих осіб, особливо в тих бізнес-функціях, де така інформація може призвести до прийняття невідповідних рішень або відмови в наданні переваг і послуг особі. Навіть правильні дані за певних обставин можуть спричинити проблеми для людей та переважити переваги організації, яка зберігає такі дані. Організації на власний розсуд вирішують, чи потрібно виправляти чи видаляти персональні дані на основі обсягу запитів, бажаних змін, впливу змін, а також законів, нормативних актів і політики. Персонал організації консультується зі старшим представником агентства з конфіденційності та юрисконсультантом щодо відповідних випадків виправлення чи видалення.

Пов'язані заходи: Немає.

(5) ОПЕРАЦІЇ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ДАНИХ - ПОВІДОМЛЕННЯ ПРО ВИПРАВЛЕННЯ ЧИ ВИДАЛЕННЯ

Повідомити [*Призначення: визначені організацією одержувачі персональної інформації*] та окремих осіб про те, що персональну інформацію було виправлено або видалено.

Рекомендації з реалізації: Коли персональні дані виправляють або видаляють, організації вживають заходів для того, щоб усі авторизовані одержувачі такої інформації, а також особи, з якими пов'язані дані, або їхні призначені представники були поінформовані про таке виправлення або видалення.

Пов'язані заходи: Немає.

Посилання: [OMB M-19-15], [SP 800-188], [IR 8112].

## SI-19 ДЕІНДЕФІКАЦІЯ

Заходи захисту:

a. Видаліть такі елементи персональних даних з наборів даних: [*Призначення: визначені організацією елементи персональних даних*];

b. Оцініть [*Призначення: частота, визначена організацією*] ефективність деідентифікації.

Рекомендації з реалізації: Деідентифікація — це загальний термін для процесу усунення зв'язку між набором ідентифікаційних даних і суб'єктом даних. Багато наборів даних містять інформацію про осіб, за якою можна розрізняти або відстежувати особу, як-от ім'я, номер соціального страхування, дата та місце народження, дівоче прізвище матері або біометричні записи. Набори даних також можуть містити іншу інформацію, яка пов'язана або може бути зв'язана з особою, наприклад, медичну, освітню, фінансову інформацію та інформацію про роботу. Персональні дані видаляються з наборів даних навченим персоналом, якщо така інформація не є (або більше не потрібна) для вимог, ними передбаченими. Наприклад, якщо набір даних використовується лише для створення сукупної статистики, ідентифікатори, які не потрібні для створення цієї статистики, видаляються. Видалення ідентифікаторів покращує захист приватності, оскільки видалена інформація не може бути випадково розголошена чи використана неналежним чином. Згідно з чинними законами, нормативними актами чи політикою організації можуть підлягати певним визначенням або методам деідентифікації. Повторна ідентифікація є залишковим ризиком із деідентифікованими даними. Атаки повторної ідентифікації можуть бути різними, включаючи поєднання нових наборів даних або інші вдосконалення в аналітиці даних. Підтримання обізнаності про потенційні атаки та оцінка ефективності деідентифікації з плином часу підтримують управління цим залишковим ризиком.

Пов'язані заходи: MP-6, PM-22, PM-23, PM-24, RA-2, SI-12.

Посилення заходів:

(1) ДЕІДЕНТИФІКАЦІЯ - ЗБІР

Деідентифікуйте набір інформаційних даних після збирання, не збираючи персональні дані.

Рекомендації з реалізації: Якщо набір даних містить персональні дані, які не потрібні для подальшої обробки, набір даних має бути деіндентифікований після створення. Наприклад, якщо організація не має наміру використовувати номер соціального страхування заявника, то форми заявок не повинні вимагати заповнення такого поля.

Пов'язані заходи: Немає.

(2) ДЕІДЕНТИФІКАЦІЯ - АРХІВАЦІЯ

Заборонити архівування елементів персональних даних, якщо ці елементи в наборі даних не будуть потрібні після його архівування.

Рекомендації з реалізації: При архівації набору даних мають вказуватися цілі архівації. Якщо персональні дані, які містяться в наборі інформації, не потрібні для досягнення вказаних цілей архівування, то такі дані мають бути видалені з набору. Наприклад, якщо номери соціального страхування були зібрані для

зв’язку записів, але архівний набір даних більше не потребує таких зв’язків, елементи, які містять номери соціального страхування, мають видалятися перед архівуванням.

Пов’язані заходи: Немає.

(3) ДЕІДЕНТИФІКАЦІЯ - ВИДАЛЕННЯ

Видаляти елементи персональних даних з набору даних перед його випуском (публікацією), якщо ці елементи в наборі даних не повинні бути частиною даних, що публікуються.

Рекомендації з реалізації: Перед випуском (публікацією) набору даних уповноважена особа має визначити: чи містить такий набір елементи персональних даних, які не мають бути розголошені. У разі необхідності, набір даних має бути деідентифікований.

Пов’язані заходи: Немає.

(4) ДЕІДЕНТИФІКАЦІЯ - ВИДАЛЕННЯ, МАСКУВАННЯ, ШИФРУВАННЯ, ГЕШУВАННЯ АБО ЗАМІНА ПРЯМИХ ІДЕНТИФІКАТОРІВ

Видаляйте, маскуйте, шифруйте, гешуйте або замінюйте прямі ідентифікатори в наборі даних.

Рекомендації з реалізації: Є багато можливих методів видалення прямих ідентифікаторів з набору даних. Наприклад, стовпці в наборі даних, які містять прямий ідентифікатор, можуть бути видалені. Можуть бути застосовані методи маскування (прямий ідентифікатор перетворюється на повторюваний символ, наприклад, XXXXXX або 999999). Ідентифікатори можуть бути зашифровані або замість відкритого тексту може використовуватися його геш-значення (при цьому пов’язані записи залишаються пов’язаними). Також ідентифікатори можуть бути замінені на ключові слова.

Пов’язані заходи: SC-12, SC-13.

(5) ДЕІДЕНТИФІКАЦІЯ - СТАТИСТИЧНИЙ КОНТРОЛЬ РОЗКРИТТЯ

При здійсненні аналізу статистичних даних рекомендується проводити маніпулювання з числовими даними, таблицями співвідношень та статистичними результатами таким чином, щоб в результаті цього аналізу не можна було ідентифікувати жодну окрему особу або організацію.

Рекомендації з реалізації: Деякі види статистичного аналізу можуть призвести до розкриття інформації про осіб, навіть якщо надаються лише зведені статистичні дані.

Пов’язані заходи: Немає.

(6) ДЕІДЕНТИФІКАЦІЯ - ДИФЕРЕНЦІЙНА КОНФІДЕНЦІЙНІСТЬ

Запобігайте розголошенню персональної інформації, додаючи недетермінований шум до результатів математичних операцій перед повідомленням про результати.

Рекомендації з реалізації: Математичне визначення диференційованої приватності стверджує, що результат аналізу набору даних повинен бути приблизно однаковим до та після додавання або видалення одного запису даних (тобто запису про одну особу). У своїй найпростішій формі диференціальна приватність стосується лише систем онлайн-запитів. Однак вона також може використовуватися для отримання статистичних класифікаторів машинного навчання та синтетичних даних. Диференціальна приватність досягається коштом зниження точності результатів. Організації змушені кількісно оцінювати компроміс між захистом приватності та точністю і корисністю деіндентифікованого набору даних. Введення недетермінованого шуму передбачає додавання невеликих випадкових значень до результатів математичних операцій при аналізі набору даних.

Пов'язані заходи: SC-12, SC-13.

(7) ДЕІДЕНТИФІКАЦІЯ - ПЕРЕВІРЕНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

Виконувати деідентифікацію за допомогою перевірених алгоритмів і програмного забезпечення, затвердженого для використання в реалізації алгоритмів.

Рекомендації з реалізації: Алгоритми, які видаляють персональні дані з набору даних, можуть залишати інформацію, яку можна використовувати для ідентифікації осіб. Програмне забезпечення, що реалізує відповідний алгоритм, може містити помилки або навмисно введені закладки. З цих причин деідентифікація має проводиться лише з використанням сертифікованого програмного забезпечення.

Пов'язані заходи: Немає.

(8) ДЕІДЕНТИФІКАЦІЯ - МОТИВОВАНИЙ ПОРУШНИК

Виконати тест на мотивованого порушника на деідентифікованому наборі даних, щоб визначити, чи залишаються присутніми ідентифіковані дані або чи можуть дані бути повторно ідентифіковані.

Рекомендації з реалізації: Тест на вмотивованого зловмисника — це тест, під час якого окрема особа або група отримує випуск даних і визначені ресурси та намагається повторно ідентифікувати одну або більше осіб у деідентифікованому наборі даних. Такі тести визначають обсяг внутрішніх знань, обчислювальних, фінансових, ресурсів, даних та навичок, якими володіють зловмисники для проведення тестів. Мотивований тест на зловмисника може визначити, чи є деідентифікація недостатньою. Це також може бути корисним діагностичним інструментом для оцінки того, чи буде достатньо тільки деідентифікації.

Пов'язані заходи: Немає.

Посилання: [OMB A-130], [SP 800-188].

## SI-20 ПСУВАННЯ

Заходи захисту: Вбудуйте дані або можливості в такі системи або системні компоненти, щоб визначити, чи дані організації були викрадені або неналежним чином видалені з

організації: [*Призначення: визначені організацією системи або системні компоненти*].

Рекомендації з реалізації: Багато кібератак спрямовані на викрадення інформації, що належить організації або, якою вона володіє від імені інших організацій (наприклад, персональні данію). Крім того, інсайдерські атаки та помилкові процедури користувача можуть видалити інформацію із системи, яка порушує політику організації. Підходи до псування можуть варіюватися від пасивних до активних. Пасивний підхід псування може бути простим, як додавання фальшивих імен та адрес електронної пошти до внутрішньої бази даних. Якщо організація отримує пошту на одну з фальшивих адрес електронної пошти, вона знатиме, що базу даних було зламано. Крім того, організація знає, що електронний лист надіслала неавторизована особа, тому будь-які пакети, у такому листі, потенційно містять шкідливий код, і що такаособа потенційно могла отримати копію бази даних. Інший підхід до псування може включати вбудовування неправдивих даних або стеганографічних даних у файли, щоб дані можна було знайти за допомогою аналізу з відкритим кодом. Нарешті, підхід активного псування може включати вбудовування в дані програмного забезпечення, яке здатне «зателефонувати додому», таким чином повідомляючи організацію про його «захоплення», і, можливо, його місцезнаходження, а також шлях, яким його було викрадено або видалено.

Пов'язані заходи: AU-13.

Посилення заходів: Немає.

Посилання: [OMB A-130], [SP 800-160-2].

## SI-21 ОНОВЛЕННЯ ІНФОРМАЦІЇ

Заходи захисту: Оновлюйте [*Призначення: інформація, визначена організацією*] з [*Призначення: частота, визначена організацією*] або згенеруйте інформацію за запитом і видаліть її, коли в ній більше не буде потреби.

Рекомендації з реалізації: Зберігання інформації довше, ніж це необхідно, робить її більш привабливою мішенню для зловмисників. Зберігання інформації доступною протягом мінімального періоду часу, необхідного для підтримки місій або бізнес-функцій організації, зменшує можливість для зловмисників скомпрометувати, захопити та викрасти її.

Пов'язані заходи: SC-14.

Посилення заходів: Немає.

Посилання: [OMB A-130], [SP 800-160-2].

## SI-22 РІЗНОВИДИ ІНФОРМАЦІЇ

Заходи захисту:

a. Визначити наступні альтернативні джерела інформації для [*Завдання: основні функції та послуги, визначені організацією*]: [*Завдання: альтернативні, визначені організацією джерела інформації*];

b. Використовуйте альтернативне джерело інформації для виконання основних функцій або послуг на [*Призначення: визначені організацією системи або системні компоненти*], коли основне джерело інформації пошкоджено або недоступне.

Рекомендації з реалізації: Дії, які виконує системна служба або функція, часто пов'язані зі вхідною інформацією. Пошкодження, фальсифікація, модифікація або видалення такої інформації може вплинути на здатність служби належним чином виконувати свої дії. Маючи кілька джерел введення, служба або функція може продовжувати роботу, якщо одне з джерел пошкоджене або не доступне. Альтернативні джерела інформації можуть бути менш точними, ніж первинне джерело інформації. Але наявність таких альтернативних джерел інформації все одно може забезпечити достатній рівень якості для виконання важливих послуг чи функцій.

Пов'язані заходи: Немає.

Посилення заходів: Немає.

Посилання: [SP 800-160-2].

## SI-23 ФРАГМЕНТАЦІЯ ІНФОРМАЦІЇ

Заходи захисту на основі [*Призначення: обставини, визначені організацією*]:

a. Фрагментуйте таку інформацію: [*Призначення: інформація, визначена організацією*];

b. Розподіліть фрагментовану інформацію між такими системами або компонентами системи: [*Системи або компоненти системи, визначені організацією призначення*].

Рекомендації з реалізації: Однією з цілей вдосконаленої постійної загрози є вилучення цінної інформації. Після ексфільтрації організація, як правило, не може відновити втрачену інформацію. Тому організації можуть розділяти інформацію на різні елементи та розташовувати ці елементи інформації між кількома системами або системними компонентами та місцями розташуваннями. Такі дії збільшать об'єм роботи противнику для захоплення та викрадання потрібної інформації та підвищать ймовірність виявлення. Фрагментація інформації впливає на здатність організації отримувати доступ до інформації вчасно. Ступінь фрагментації залежить від впливу або рівня класифікації (та цінності) інформації, отриманої інформації про загрози та того, чи використовується псування даних (тобто отримана інформація псування даних або викрадання певної інформації може призвести до фрагментації решти інформації).

Пов'язані заходи: Немає.

Посилення заходів: Немає.

Посилання: [SP 800-160-2].

## 10.20 Клас заходів захисту SR — УПРАВЛІННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ

### SR-1 ПОЛІТИКА ТА ПРОЦЕДУРИ УПРАВЛІННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ

Заходи захисту:

a. Розробіть, задокументуйте та поширте [*Призначення: персонал або ролі, визначені організацією*]:

   1. [*Вибір (один або декілька): Рівень організації; Рівень місії/бізнес-процесу; рівень системи*] політика управління ризиками ланцюга постачання, яка:

      a) Розглядає мету, сферу діяльності, ролі, відповідальність, зобов'язання керівництва, координацію між організаційними підрозділами та відповідність;

      b) Відповідає чинним законам, виконавчим наказам, директивам, положенням, політикам, стандартам і вказівкам;

   2. Процедури для сприяння впровадженню політики управління ризиками ланцюга постачання та відповідних засобів контролю управління ризиками ланцюга постачання;

b. Призначити [*Призначення: посадова особа, визначена організацією*] для управління розробкою, документуванням і розповсюдженням політики та процедур управління ризиками ланцюга постачання;

c. Перегляньте та оновіть поточне управління ризиками ланцюга постачання:

   1. Політика [*Призначення: частота, визначена організацією*] та наступне [*Призначення: події, визначені організацією*];

   2. Процедури [*Призначення: частота, визначена організацією*] та наступні [*Призначення: події, визначені організацією*].

Рекомендації з реалізації: Політика та процедури управління ризиками ланцюга постачання стосуються заходів захисту в сімействі SR, а також заходів захисту, пов'язаних з ланцюгом постачання в інших сім'ях, які реалізуються в системах і організаціях. Стратегія управління ризиками є важливим фактором у встановленні такої політики та процедур. Політики та процедури сприяють забезпеченню безпеки та приватності, тому важливо, щоб програми безпеки та приватності були узгоджені при розробці політики та процедур управління ризиками ланцюга поставок. Політика та процедури програми безпеки та приватності на рівні організації мають вищий пріорітет і можуть усунути потребу в політиках і процедурах, що стосуються місії чи системи. Політика може бути включена як частина загальної політики безпеки та приватності або представлена декількома політиками, які відображають складний характер організацій. За потреби можна встановити процедури для програм безпеки та приватності, для місії чи бізнес-процесів, а також для систем. Процедури описують, як реалізуються політики або заходи захисту, і можуть бути спрямовані на особу або роль, які є об'єктом процедури. Процедури можуть бути задокументовані в планах захисту інформації та приватності, в одному чи кількох окремих документах. Події, які можуть спричинити оновлення політики та процедур управління ризиками ланцюга постачання, включають висновки оцінювання або аудиту, інциденти чи порушення

безпеки або зміни у чинних законах, розпорядженнях, директивах, постановах, політиках, стандартах і рекомендаціях. Просте повторне встановлення заходів захисту не є організаційною політикою чи процедурою.

Пов'язані заходи: PM-9, PM-30, PS-8, SI-12.

Посилення заходів: Немає.

Посилання: [FASC18], [41 CFR 201], [EO 13873], [CNSSD 505], [SP 800-12], [SP 800-30], [SP 800- 39], [SP 800-100], [SP 800-161].

## SR-2 ПЛАН УПРАВЛІННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ

Заходи захисту:

a. Розробіть план управління ризиками ланцюга постачання, пов'язаними з дослідженнями та розробкою, проектуванням, виробництвом, придбанням, доставкою, інтеграцією, експлуатацією та обслуговуванням, а також утилізацією таких систем, компонентів системи або послуг для системи: [*Призначення: системи, визначені організацією, системні компоненти або системні служби*];

b. Перегляньте та оновіть план управління ризиками ланцюга постачання [*Призначення: частота, визначена організацією*] або за потреби для усунення загроз;

c. Захистіть план управління ризиками ланцюга постачання від несанкціонованого розголошення та модифікації.

Рекомендації з реалізації: Залежність від продуктів, систем і послуг зовнішніх постачальників, а також характер відносин із цими постачальниками становлять зростаючий рівень ризику для організації. До загроз, які можуть збільшити ризики для безпеки чи приватності, належать несанкціоноване виробництво, використання підробок, крадіжки, використання зловмисного програмного та апаратного забезпечення, а також неналежні методи виробництва та розробки в ланцюжку постачання. Ризики ланцюга постачання можуть бути ендемічними або системними в системному елементі чи компоненті, системі, організації, чи на національному рівні. Управління ризиками в ланцюжку постачання є складним, багатогранним заходом, який вимагає скоординованих зусиль усієї організації для побудови довірчих відносин і спілкування з внутрішніми та зовнішніми зацікавленими сторонами. Діяльність з управління ризиками в ланцюжку постачання (SCRM) включає виявлення та оцінку ризиків, визначення відповідних заходів реагування на ризики, розробку планів SCRM для документування дій реагування та моніторинг ефективності щодо планів. План SCRM (на системному рівні) є специфічним для реалізації та забезпечує впровадження політики, вимог, обмеження та наслідків. Він може бути як окремим, так і включеним до системної безпеки та планів конфіденційності. План SCRM стосується управління, впровадження та моніторингу заходів захисту SCRM, а також розробки/підтримки систем у SDLC для підтримки місії та функцій.

Оскільки ланцюги постачання можуть суттєво відрізнятися між організаціями та всередині них, плани SCRM адаптовані до індивідуальних програм, організаційних та операційних умов. Спеціальні плани SCRM забезпечують основу для визначення того, чи технологія, послуга, компонент системи або система відповідають меті, і яким чином елементи керування потрібно адаптувати. Індивідуальні плани SCRM допомагають організаціям зосередити свої ресурси на найважливіших місіях і функціях на основі місії та бізнес-вимог і середовища ризику. Плани управління ризиками ланцюга

постачання включають допустимі ризики ланцюга постачання для організації, прийнятні стратегії зменшення таких ризиків або заходи захисту, процеси послідовної оцінки та моніторингу ризиків ланцюга постачання, підходи до впровадження та передачі плану, опис та обґрунтування вжитих заходів із зменшення ризиків у ланцюзі постачання, а також відповідні ролі та відповідальність. Нарешті, плани управління ризиками ланцюга постачання стосуються вимог щодо розробки надійних, безпечних, стійких до конфіденційності компонентів системи і систем, включаючи застосування принципів проектування безпеки, реалізованих як частина процесів розробки систем безпеки на основі життєвого циклу (див. SA- 8).

Пов'язані заходи: CA-2, CP-4, IR-4, MA-2, MA-6, PE-16, PL-2, PM-9, PM-30, RA-3, RA-7, SA-8, SI-4.

Посилення заходів:

(1) СТВОРЕННЯ КОМАНДИ УПРАВЛІННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ

Створіть команду з управління ризиками ланцюга постачання, що складається з [*Призначення: визначений організацією персонал, ролі та обов'язки*] для керівництва та підтримки наступних заходів SCRM: [*Призначення: діяльність з управління ризиками ланцюга постачання, визначена організацією*].

Рекомендації з реалізації: Щоб реалізувати плани управління ризиками ланцюга постачання, організації встановлюють скоординований командний підхід для виявлення та оцінки ризиків ланцюга постачання та управління цими ризиками за допомогою програмних і технічних методів. Командний підхід дозволяє організаціям проводити аналіз свого ланцюга постачання, спілкуватися з внутрішніми та зовнішніми партнерами чи зацікавленими сторонами та досягати широкого консенсусу щодо відповідних ресурсів для SCRM. Команда SCRM складається з організаційного персоналу з різноманітними ролями та обов'язками для керівництва та підтримки діяльності SCRM, включаючи управління ризиками, інформаційні технології, укладання контрактів, інформаційну безпеку, приватність, місію чи бізнес, юридичні питання, ланцюг постачання та логістику, придбання, безперервність бізнесу та інші відповідні функції. Члени команди SCRM залучені до різних аспектів SDLC і співпрацюють у процесах отримання, юридичних практиках, уразливостях, загрозах і векторах атак, а також розуміють технічні аспекти та залежності систем. Команда SCRM може бути продовженням процесів управління ризиками безпеки та приватності або бути включеною до складу команди управління організаційними ризиками.

Пов'язані заходи: Немає.

Посилання: [FASC18], [41 CFR 201], [EO 13873], [CNSSD 505], [SP 800-30], [SP 800-39], [SP-800- 160-1], [SP 800-161], [SP 800-181], [IR 7622], [IR 8272].

## SR-3 КОНТРОЛЬ ЛАНЦЮГА ПОСТАЧАННЯ І ПРОЦЕСІВ

Заходи захисту:

a. Встановлення процесу або процесів для виявлення та усунення слабких місць або недоліків в елементах і процесах ланцюга постачання [*Призначення:*

*визначена організацією система або компонент системи*] у координації з [*Завдання: персонал ланцюга постачання, визначений організацією*];

b. Використовуйте такі заходи захисту, щоб захистити систему, компонент системи або системну службу від ризиків ланцюга постачання та обмежити шкоду чи наслідки від подій, пов'язаних із ланцюгом постачання: [*Призначення: заходи захисту ланцюга постачання, визначені організацією*];

c. Задокументуйте обрані та впроваджені процеси та заходи захисту ланцюгом постачання у [*Вибір: плани безпеки та приватності; план управління ризиками ланцюга постачання;* [*Призначення: документ, визначений організацією*]].

Рекомендації з реалізації: Елементи ланцюга постачання включають організації або інструменти, що використовуються для дослідження, розробки, проектування, виробництва, придбання, постачання, інтеграції, експлуатації та обслуговування, а також утилізації систем і компонентів системи. Процеси ланцюга постачання включають процеси розробки обладнання, апаратного та програмного забезпечення; процедури доставки та обробки; програми безпеки персоналу та фізичної безпеки; засоби керування конфігурацією, методи та заходи для підтримки походження; або інші програми, процеси чи процедури, пов'язані з розробкою, придбанням, підтримкою та утилізацією систем і компонентів системи. Елементи та процеси ланцюга постачання можуть надаватися організаціями, системними інтеграторами або зовнішніми постачальниками. Слабкі місця або недоліки в елементах або процесах ланцюга постачання є потенційно вразливими місцями, якими можуть скористатися зловмисники, щоб завдати шкоди організації та вплинути на її здатність виконувати свої основні місії або функції. Персонал ланцюга постачання – це особи, які мають ролі та обов'язки в ланцюзі постачання.

Пов'язані заходи: CA-2, MA-2, MA-6, PE-3, PE-16, PL-8, PM-30, SA-2, SA-3, SA-4, SA-5, SA-8, SA-9, SA-10, SA-15, SC-7, SC-29, SC-30, SC-38, SI-7, SR-6, SR-9, SR-11.

Посилення заходів:

(1) КОНТРОЛЬ ЛАНЦЮГА ПОСТАЧАННЯ І ПРОЦЕСІВ - РІЗНІ БАЗИ ПОСТАЧАННЯ

Використовуйте різноманітний набір джерел для таких компонентів системи і служб: [*Призначення: системні компоненти та служби, визначені організацією*].

Рекомендації з реалізації: Різномінісття систем постачання, компонентів системи і послуг може зменшити ймовірність того, що зловмисники успішно ідентифікують ланцюжок постачання і націляться на нього, а також зменшити вплив події в ланцюзі постачання або компрометації. Вибір кількох постачальників для заміни компонентів може зменшити ймовірність того, що компонент, який необхідно замінити, стане недоступним. Залучення різноманітних розробників або постачальників логістичних послуг може зменшити вплив стихійного лиха чи іншої події в ланцюзі постачання. Організації проектують системи з використанням різноманітних матеріалів і компонентів.

Пов'язані заходи: Немає.

(2) КОНТРОЛЬ ЛАНЦЮГА ПОСТАЧАННЯ І ПРОЦЕСІВ - ОБМЕЖЕННЯ ШКОДИ

Використовуйте такі заходи захисту, щоб обмежити шкоду від потенційних супротивників, які ідентифікують ланцюг постачання організації і націлюються на нього: [*Призначення: заходи захисту, визначені організацією*].

Рекомендації з реалізації: Заходи захисту, які можна запровадити, щоб зменшити ймовірність того, що зловмисники успішно ідентифікують ланцюг постачання та націляться на нього, включають уникнення придбання нестандартних або нестандартизованих конфігурацій, використання схвалених списків постачальників із стабільною репутацією в галузі, дотримання попередньо узгоджених графіків технічного обслуговування, оновлення та виправлення. механізмів доставки, підтримання плану на випадок надзвичайних ситуацій в ланцюзі постачання, використання виключень із закупівель та різноманітних маршрутів доставки, мінімізація часу між прийняттям рішення про закупівлю та доставку.

Пов’язані заходи: Немає.

(3) КОНТРОЛЬ ЛАНЦЮГА ПОСТАЧАННЯ І ПРОЦЕСІВ - ПЕРЕНЕСЕННЯ ЗАХОДІВ ЗАХИСТУ УПРАВЛІННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ ДО СУБПІДРЯДНИКІВ

Переконайтеся, що заходи захисту, включені в контракти головних підрядників, також включені в контракти субпідрядників.

Рекомендації з реалізації: Для ефективного та цілісного управління ризиками в ланцюзі постачання важливо, щоб організації забезпечили включення заходів захисту та ризиків у ланцюгу постачання на всіх його рівнях. Це включає забезпечення того, щоб підрядники рівня 1 (основні) запровадили процеси для полегшення «перенесення» заходів захисту управління ризиками ланцюга постачання до субпідрядників. Заходи захисту, що підлягають включенню до угод, визначені в SR-3b.

Пов’язані заходи: SR-5, SR-8.

Посилання: [FASC18], [41 CFR 201], [EO 13873], [ISO 20243], [SP 800-30], [SP 800-161], [IR 7622].

## SR-4 ПОХОДЖЕННЯ

Заходи захисту: Документуйте, відстежуйте та підтримуйте справжнє походження таких систем, компонентів системи і пов’язаних даних: *[Призначення: системи, визначені організацією, системні компоненти та пов’язані дані*].

Рекомендації з реалізації: Кожна система та компонент системи має точку походження, яка може змінюватися протягом свого існування. Походження – це хронологія походження, розвитку, власності, розташування та змін у системі або компоненті системи та пов’язаних даних. Воно також може включати персонал і процеси, які використовуються для взаємодії або внесення змін до системи, компонента або пов’язаних даних. Організації розглядають розробку процедур (див. SR-1) для

розподілу відповідальності за створення, підтримку та моніторинг походження систем і компонентів системи; передачу документації про походження та відповідальність між організаціями; запобігання та моніторинг неавторизованих змін у записах про походження.
Організації документують, моніторять та підтримують базові лінії походження для систем, компонентів системи та пов'язаних даних обраними методами. Ці дії допомагають відстежувати, оцінювати та документувати будь-які зміни у походженні, включаючи зміни в елементах ланцюга постачання чи конфігурації та допомагають гарантувати неспростовність інформації про походження та записів про зміну походження. Питання про походження розглядають протягом життєвого циклу розробки системи та включають до контрактів та інших домовленостей у разі необхідності.

Пов'язані заходи: CM-8, MA-2, MA-6, RA-9, SA-3, SA-8, SI-4.

Посилення заходів:

(1) ПОХОДЖЕННЯ - ІДЕНТИЧНІСТЬ

Встановити та підтримувати унікальну ідентифікацію наступних елементів ланцюга постачання, процесів і персоналу, пов'язаного з визначеною системою та критичними системними компонентами: [*Призначення: визначені організацією елементи ланцюга постачання, процеси та персонал, пов'язані з визначеними організацією системами та критичними системними компонентами* ].

Рекомендації з реалізації: Знання того, хто і що є в ланцюгах постачання організацій, має вирішальне значення для отримання прозорості його діяльності. Прозорість діяльності ланцюга постачання також важлива для моніторингу та виявлення подій з високим ризиком. Без достатньої прозорості елементів, процесів і персоналу ланцюгів постачання організаціям дуже важко розуміти ризики та керувати ними, а також зменшувати свою сприйнятливість до несприятливих подій. Елементи ланцюга постачання включають організації або інструменти, що використовуються для дослідження, розробки, проектування, виробництва, придбання, доставки, інтеграції, експлуатації, обслуговування та утилізації систем і компонентів системи. Процеси ланцюга постачання включають процеси розробки апаратного і програмного забезпечення та мікропрограм; процедури доставки та обробки; засоби керування конфігурацією, методи та заходи для підтримки походження; програми кадрової та фізичної безпеки; або інші програми, процеси чи процедури, пов'язані з виробництвом і розповсюдженням елементів ланцюга постачання. Персонал ланцюга постачання – це особи, які мають певні ролі та обов'язки, пов'язані з безпечним дослідженням і розробкою, проектуванням, виробництвом, придбанням, доставкою, інтеграцією, експлуатацією та обслуговуванням, а також утилізацією системи або системного компонента. Методи ідентифікації є достатніми для підтримки відстеження у випадку зміни ланцюга постачання (наприклад, якщо купується компанія-постачальник), компрометації або події.

Пов'язані заходи: IA-2, IA-8, PE-16.

(2) ПОХОДЖЕННЯ - УНІКАЛЬНА ІДЕНТИФІКАЦІЯ

Встановити та підтримувати унікальну ідентифікацію наступних систем і критичних компонентів системи для відстеження через ланцюг постачання:

[*Призначення: визначені організацією системи та критичні системні компоненти*].

Рекомендації з реалізації: Відстеження унікальної ідентифікації систем і компонентів системи під час розробки та транспортування забезпечує базову структуру ідентифікації для встановлення та підтримки походження. Наприклад, компоненти системи можуть бути позначені серійними номерами або позначені тегами радіочастотної ідентифікації. Мітки та теги можуть допомогти забезпечити кращу прозорість походження системи або системного компонента. Система або компонент системи може мати більше одного унікального ідентифікатора. Методи ідентифікації є достатніми для підтримки судово-медичного розслідування після порушення ланцюга постачання або події.

Пов'язані заходи: IA-2, IA-8, PE-16, PL-2.

(3) ПОХОДЖЕННЯ - ПЕРЕВІРКА НА СПРАВЖНІСТЬ І ВІДСУТНІСТЬ ВНЕСЕННЯ ЗМІН

Використовуйте такі заходи захисту, щоб підтвердити, що отримана система або компонент системи є справжніми та не зміненими: [*Призначення: заходи захисту, визначені організацією*].

Рекомендації з реалізації: Для багатьох систем і компонентів системи, особливо апаратного забезпечення, існують технічні засоби для визначення справжності елементів та їх незмінності, включаючи оптичні та нанотехнологічні теги, фізично неклоновані функції, аналіз бічних каналів, криптографічні геш-перевірки або цифрові підписи, а також видимі анти-маркування етикеток або наклейок. Заходи захисту також можуть включати моніторинг продуктивності компоненту, який не відповідає специфікаціям, що також може бути показником фальсифікату або підробки. Організації можуть використовувати процеси постачальника та підрядника для підтвердження того, що система чи компонент є справжніми та не зміненими, а також для заміни підозрілої системи чи компонента. Деякі ознаки фальсифікації можуть бути видимими, наприклад невідповідна упаковка, зламані пломби та неправильні етикетки. Якщо існує підозра, що система або компонент системи є зміненими або підробленими, постачальник, підрядник або виробник оригінального обладнання може замінити елемент або надати можливість для проведення судово-медичної експертизи для визначення походження такого компонента. Організації також можуть здійснювати навчання персоналу щодо того, як ідентифікувати підозрілі системи або компоненти під час поставки.

Пов'язані заходи: AT-3, SR-9, SR-10, SR-11.

(4) ПОХОДЖЕННЯ – ПЕРЕВІРКА ЛАНЦЮГА ЦІЛІСНОСТІ

Використовуйте [*Завдання: заходи захисту, визначені організацією*] та проводьте [*Завдання: аналіз, визначений організацією*], щоб забезпечити цілісність системи та компонентів системи шляхом перевірки внутрішнього складу та походження критично важливих або важливих технологій, продуктів і послуг.

Рекомендації з реалізації: Достовірна інформація щодо внутрішнього складу компонентів системи та походження технологій, продуктів і послуг забезпечує

основу для довіри. Перевірка внутрішнього складу та походження технологій, продуктів і послуг називається родоводом. Для мікроелектроніки це - склад матеріалів компонентів. Для програмного забезпечення це - склад відкритого та закритого кодів коду, включаючи версію компонента на даний момент часу. Родоводи підвищують впевненість у тому, що заяви постачальників про внутрішній склад і походження продуктів, послуг і технологій, які вони надають, є дійсними. Перевірка внутрішнього складу та походження може бути досягнута різними доказовими артефактами або записами, які виробники та постачальники створюють під час досліджень і розробок, проектування, виробництва, придбання, постачання, інтеграції, експлуатації та обслуговування, а також утилізації технологій, продуктів і послуг. Доказові артефакти включають: теги ідентифікації програмного забезпечення (SWID), інвентаризацію компонентів програмного забезпечення, заяви виробників про атрибути платформи (наприклад, серійні номери, інвентаризацію апаратних компонентів) і вимірювання (наприклад, геші мікропрограм), які точно пов'язані з апаратним забезпеченням.

Пов'язані заходи: RA-3.

Посилання: [FASC18], [41 CFR 201], [EO 13873], [ISO 27036], [ISO 20243], [SP 800-160-1], [SP 800-161], [IR 7622], [IR 8112], [IR 8272].

## SR-5 СТРАТЕГІЇ ПРИДБАННЯ, ІНСТРУМЕНТИ І МЕТОДИ

Заходи захисту: Використовуйте наступні стратегії придбання, контрактні інструменти та методи закупівель, щоб захистити від ризиків ланцюга постачання, визначити та пом'якшити їх: [*Призначення: визначені організацією стратегії придбання, контрактні інструменти та методи закупівель*].

Рекомендації з реалізації: Процес придбання є важливим засодом захисту ланцюга постачання. Існує багато корисних інструментів і методів, зокрема приховування кінцевого використання системи чи системного компонента, використання сліпих або відфільтрованих покупок, вимога упаковки, яка захищена від несанкціонованого відкриття, або використання надійного чи контрольованого розповсюдження. Результатами оцінки ризику ланцюга постачання можна керувати та інформувати про стратегії, інструменти та методи, які найбільше підходять для конкретної ситуації. Інструменти та методи можуть забезпечувати захист від несанкціонованого виробництва, крадіжки, втручання, підробок, шкідливого програмного забезпечення або бекдорів, а також неналежних методів розробки протягом життєвого циклу розробки системи. Організації також розглядають можливість надання стимулів для постачальників, які впроваджують заходи захисту, сприяють прозорості своїх процесів і методів безпеки та конфіденційності, передбачають формулювання в контрактах, які стосуються заборони зіпсованих або підроблених компонентів, і обмежують покупки в ненадійних постачальників. Організації розглядають можливість проведення тренінгів, навчань та програм підвищення обізнаності персоналу щодо ризиків ланцюга постачання, доступних стратегій пом'якшення та того, коли програми слід використовувати. Методи перевірки та захисту планів розвитку, документації та доказів мають відповідають вимогам організації щодо безпеки та приватності. В контракти також можуть бути включені вимоги щодо захисту документації.

Пов'язані заходи: AT-3, SA-2, SA-3, SA-4, SA-5, SA-8, SA-9, SA-10, SA-15, SR-6, SR-9, SR-10, SR-11.

Посилення заходів:

(1) СТРАТЕГІЇ ПРИДБАННЯ, ІНСТРУМЕНТИ І МЕТОДИ - НАЛЕЖНЕ ПОСТАЧАННЯ

Використовуйте наступні заходи захисту, щоб забезпечити належне постачання [*Призначення: критичні компоненти системи, визначені організацією*]: [*Призначення: засходи захисту, визначені організацією*].

Рекомендації з реалізації: Зловмисники можуть спробувати перешкодити організаційним операціям, перериваючи постачання критично важливих компонентів системи або руйнуючи роботу постачальників. Організації можуть відстежувати середній час відмови систем і компонентів, щоб зменшити втрату тимчасової або постійної функції системи. Засходи захисту для забезпечення належного постачання критично важливих компонентів системи включають використання кількох постачальників по всьому ланцюгу постачання з визначеннням критичних компонентів, накопиченням запасних компонентів для забезпечення роботи в критично важливий період, а також ідентифікацію функціонально ідентичних або схожих компонентів, які можуть бути використані у разі необхідності.

Пов’язані заходи: RA-9.

(2) СТРАТЕГІЇ ПРИДБАННЯ, ІНСТРУМЕНТИ І МЕТОДИ - ОЦІНКА ПЕРЕД ВІДБОРОМ, ПРИЙНЯТТЯ, МОДИФІКАЦІЯ ЧИ ОНОВЛЕННЯ

Оцініть систему, компонент системи або послугу в системі перед вибором, прийняттям, модифікацією або оновленням.

Рекомендації з реалізації: Персонал організації або незалежні зовнішні організації проводять оцінку систем, компонентів, продуктів, інструментів і послуг, щоб виявити докази втручання, ненавмисних і навмисних уразливостей або докази невідповідності контролю ланцюга постачання. До них належать: зловмисний код, шкідливі процеси, несправне програмне забезпечення, бекдори та підробки. Оцінювання може включати: огляд проектних пропозицій; візуальний або фізичний огляд; статичний і динамічний аналізи; візуальний, рентгенівський або магнітно-порошковий контроль; моделювання; тестування методами білої, сірої або чорної скриньки; фаз-тестування; стрес-тестування; і тестування на проникнення (див. SR-6(1)). Результати, отримані під час організаційного чи незалежного оцінювання елементів ланцюга постачання документуються та можуть бути використані для покращення процесів ланцюга постачання та управління ризиками. Результати оцінювання та інша документація можуть надаватися згідно з угодами організації та використовуватися в подальших оцінюваннях.

Пов’язані заходи: CA-8, RA-5, SA-11, SI-7.

Посилання: [FASC18], [41 CFR 201], [EO 13873], [ISO 27036], [ISO 20243], [SP 800-30], [SP 800- 161], [IR 7622], [IR 8272].

## SR-6 ОЦІНКА ПОСТАЧАЛЬНИКІВ

Заходи захисту: Оцініть і перегляньте ризики ланцюга постачання, пов’язані з постачальниками або підрядниками, системою, системним компонентом або системною послугою, яку вони надають [*Призначення: частота, визначена організацією*].

Рекомендації з реалізації: Оцінка та аналіз ризиків постачальника включає процеси управління ризиками безпеки та ланцюга постачання, іноземну власність, контроль або вплив (FOCI), а також здатність постачальника ефективно оцінювати залежних постачальників і підрядників другого та третього рівня. Перевірки можуть проводитися організацією або незалежною третьою стороною і розглядають задокументовані процеси, задокументовані заходи захисту, розвідку з усіх джерел і загальнодоступну інформацію, пов'язану з постачальником або підрядником. Організації можуть використовувати інформацію з відкритих джерел для моніторингу ознак викраденої інформації, поганої розробки та практики контролю якості, витоку інформації або підробок. У деяких випадках може бути доцільним або необхідним поділитися результатами оцінювання та перегляду з іншими організаціями відповідно до будь-яких застосовних правил, політик або міжорганізаційних угод чи контрактів.

Пов'язані заходи: SR-3, SR-5.

Посилення заходів:

(1) ОЦІНКА ПОСТАЧАЛЬНИКІВ - ТЕСТУВАННЯ ТА АНАЛІЗ

Вжити заходів щодо [*Вибір (один або декілька): аналіз організації; незалежний сторонній аналіз; організаційне тестування; незалежне стороннє тестування*] наступних елементів ланцюга постачання, процесів і учасників, пов'язаних із системою, системним компонентом або системною службою: [*Призначення: визначені організацією елементи, процеси та учасники ланцюга постачання*].

Рекомендації з реалізації: Розглядаються відносини між суб'єктами та процедурами в ланцюзі постачання, включаючи розробку та доставку. Елементами ланцюга постачання є організації або інструменти, які використовуються для дослідження та розробки, проектування, виробництва, придбання, постачання, інтеграції, експлуатації, обслуговування та утилізації систем, компонентів системи або послуг для системи. Процеси ланцюга постачання включають програми управління ризиками ланцюга постачання; стратегії та плани реалізації SCRM; програми кадрової та фізичної безпеки; процеси розробки апаратного, програмного та мікропрограмного забезпечення; засоби керування конфігурацією, методи та заходи для підтримки походження; процедури доставки та обробки; і програми, процеси або процедури, пов'язані з виробництвом і розподілом елементів ланцюга постачання. Учасники ланцюга постачання — це особи, які виконують певні ролі та обов'язки в ланцюзі постачання. Результати, отримані та зібрані під час аналізу та тестування елементів, процесів і учасників ланцюга постачання, документуються та використовуються для інформування про заходи та рішення з управління ризиками організації.

Пов'язані заходи: CA-8, SI-4.

Посилання: [FASC18], [41 CFR 201], [EO 13873], [ISO 27036], [ISO 20243], [FIPS 140-3], [FIPS 180-4], [FIPS 186-4], [FIPS 202], [SP 800-30], [SP 800-161], [IR 7622], [IR 8272].

## SR-7 БЕЗПЕКА ОПЕРАЦІЙ ЛАНЦЮГА ПОСТАЧАННЯ

Заходи захисту: Використовуйте такі заходи захисту операційної безпеки (OPSEC), щоб захистити інформацію, пов'язану з ланцюгом постачання для системи, системного

компонента чи системної служби: [*Призначення: визначені організацією заходи захисту операційної безпеки (OPSEC)*].

Рекомендації з реалізації: Ланцюг постачання OPSEC розширює сферу дії OPSEC, включаючи постачальників і потенційних постачальників. OPSEC — це процес, який включає ідентифікацію критичної інформації, аналіз дружніх дій, пов'язаних з операціями та іншими видами діяльності, щоб ідентифікувати дії, які можуть вивчати потенційні супротивники, визначення показників, які потенційні супротивники можуть отримати, або які можна інтерпретувати чи об'єднати для отримання інформації для того, щоб завдавати шкоди організаціям. Необхідно застосовувати запобіжні заходи чи контрзаходи для усунення або зменшення до прийнятного рівня вразливостей і ризиків, які можуть бути використані супротивниками та одночасно розглядати сукупності інформації, які наражають користувачів або конкретні види використання ланцюга постачання. Інформація про ланцюг постачання включає ідентифікаційні дані користувачів; використання для систем, компонентів системи і послуг для системи; ідентифікатори постачальників; вимоги безпеки та приватності; конфігурації системи та компонентів; процеси постачальника; специфікації конструкції; а також результати тестування та оцінки. OPSEC ланцюга постачання може вимагати від організацій приховувати інформацію про місію чи бізнес від постачальників і може включати використання посередників, щоб приховати кінцеве використання або користувачів систем, компонентів системи або послуг для системи.

Пов'язані заходи: SC-38.

Посилення заходів: Немає.

Посилання: [EO 13873], [SP 800-30], [ISO 27036], [SP 800-161], [IR 7622].

## SR-8 ПОВІДОМЛЕННЯ ПРО ПОРУШЕННЯ ЛАНЦЮГА ПОСТАЧАННЯ

Заходи захисту: Затвердити угоди та процедури з суб'єктами, залученими до ланцюга постачання для системи, системного компонента або системної послуги для [*Вибір (одного або кількох): повідомлення про порушення ланцюга постачання; результати оцінювання або аудитів; [Призначення: інформація, визначена організацією*]].

Рекомендації з реалізації: Затвердження угод і процедур полегшує взаємодію між суб'єктами ланцюга постачання. Для ефективного реагування на інциденти, які можуть негативно вплинули на системи чи компоненти організації, важливо завчасно повідомляти про порушення ланцюга постастачання, суб'єктів, залучених до нього. Результати оцінювання або аудитів можуть включати інформацію з відкритих джерел, яка сприяла прийняттю рішення або результату та могла бути використана, щоб допомогти суб'єкту ланцюга постачання вирішити проблему або покращити свої процеси.

Пов'язані заходи: IR-4, IR-6, IR-8.

Посилення заходів: Немає.

Посилання: [FASC18], [41 CFR 201], [EO 13873], [ISO 27036], [SP 800-30], [SP 800-161], [IR 7622].

## SR-9 ЗАХИСТ ВІД ЗЛОМУ ТА ВИЯВЛЕННЯ

Заходи захисту: Впровадити програму захисту від несанкціонованого доступу для

системи, системного компонента або системної служби.

Рекомендації з реалізації: Технології, інструменти та методи захисту від несанкціонованого доступу забезпечують певний рівень захисту для систем, компонентів системи і служб від багатьох загроз, включаючи зворотнє проектування, модифікацію та заміну. Надійна ідентифікація в поєднанні із захистом від несанкціонованого доступу та/або виявлення втручання має важливе значення для захисту систем і компонентів під час розповсюдження та використання.

Пов'язані заходи: PE-3, PM-30, SA-15, SI-4, SI-7, SR-3, SR-4, SR-5, SR-10, SR-11.

Посилення заходів:

(1) ЗАХИСТ ВІД ЗЛОМУ ТА ВИЯВЛЕННЯ - ЕТАПИ ЧИ СИСТЕМИ РОЗВИТКУ ЖИТТЄВОГО ЦИКЛУ

Використовуйте технології, інструменти та методи захисту від втручання протягом усього життєвого циклу розвитку системи.

Рекомендації з реалізації: Життєвий цикл розробки системи включає дослідження, розробку, проектування, виробництво, придбання, доставку, інтеграцію, експлуатацію, технічне обслуговування та утилізацію. Організації використовують комбінацію апаратних і програмних засобів для захисту від втручання та виявлення, а також обфускацію та самоперевірку, щоб зробити зворотню інженерію та модифікацію складними, трудомісткими та дорогими для використання противниками. Налаштування систем і компонентів системи може полегшити виявлення замін і таким чином обмежити шкоду.

Пов'язані заходи: SA-3.

Посилання: [ISO 20243].

## SR-10 ПЕРЕВІРКА СИСТЕМИ І КОМПОНЕНТІВ СИСТЕМИ

Заходи захисту: Перевірте наступні системи або системні компоненти [*Вибір (один або більше): випадковим чином обраних; на [Призначення: частота, визначена організацією*], після [*Призначення: визначені організацією ознаки необхідності перевірки*]] для виявлення втручання: [*Призначення: визначені організацією системи або компоненти системи*].

Рекомендації з реалізації: Перевірка систем або компонентів системи на захист від несанкціонованого доступу та втручання стосується фізичного та логічного втручання і застосовується до систем і компонентів, видалених із зон, контрольованих організацією. Ознаки необхідності перевірки включають зміни в упаковці, специфікаціях, місці розташування фабрики або організації, в якій придбано деталь, а також коли особи повертаються з подорожі до місць високого ризику.

Пов'язані заходи: AT-3, PM-30, SI-4, SI-7, SR-3, SR-4, SR-5, SR-9, SR-11.

Посилання: [ISO 20243].

## SR-11 АВТЕНТИЧНІСТЬ КОМПОНЕНТУ

Заходи захисту:

a. Розробити та впровадити політику та процедури боротьби з підробками, які включають засоби для виявлення та запобігання потраплянню підроблених компонентів у систему;

b. Повідомляти про підроблені системні компоненти [*Вибір (один або кілька): джерело підробленого компонента; [Призначення: зовнішні звітні організації, визначені організацією*]; [*Призначення: персонал або ролі, визначені організацією*]].

Рекомендації з реалізації: Джерелами підроблених компонентів є виробники, розробники, постачальники та підрядники. Політика та процедури боротьби з підробками забезпечують захист від несанкціонованого доступу та забезпечують певний рівень захисту від впровадження шкідливого коду. Пов'язані заходи: PE-3, SA-4, SI-7, SR-9, SR-10.

Посилення заходів:

(1) АВТЕНТИЧНІСТЬ КОМПОНЕНТУ - ТРЕНУВАННЯ ПО БОРОТЬБІ З ПІДРОБКАМИ

Навчити [*Призначення: персонал або ролі, визначені організацією*] виявленню підроблених компонентів системи (включаючи апаратне, програмне та мікропрограмне забезпечення).

Рекомендації з реалізації: Немає.

Пов'язані заходи: AT-3.

(2) АВТЕНТИЧНІСТЬ КОМПОНЕНТУ - КОНТРОЛЬ КОНФІГУРАЦІЇ КОМПОНЕНТІВ, ЯКІ ПОТРЕБУЮТЬ СЕРВІСНОГО ОБСЛУГОВУВАННЯ І РЕМОНТУ

Зберігайте контроль конфігурації для компонентів системи, які очікують обслуговування або ремонту, і компонентів, які очікують повернення в експлуатацію після обслуговування або ремонту: [*Призначення: системні компоненти, визначені організацією*].

Рекомендації з реалізації: Немає.

Пов'язані заходи: CM-3, MA-2, MA-4, SA-10.

(3) АВТЕНТИЧНІСТЬ КОМПОНЕНТУ - СКАНУВАННЯ ДЛЯ ВИЯВЛЕННЯ ПІДРОБОК

Сканування для виявлення підроблених компонентів системи [*Призначення: частота, визначена організацією*].

Рекомендації з реалізації: Тип компонента визначає тип сканування, яке буде виконано (наприклад, сканування вебпрограми, якщо компонент є вебпрограмою).

Пов'язані заходи: RA-5.

Посилання: [ISO 20243].

## SR-12 УТИЛІЗАЦІЯ КОМПОНЕНТУ

Заходи захисту: Утилізуйте [*Призначення: визначені організацією дані, документація, інструменти або системні компоненти*] за допомогою таких прийомів і методів: [*Призначення: визначені організацією прийоми та методи*].

Рекомендації з реалізації: Дані, документація, інструменти або системні компоненти можуть бути утилізовані в будь-який час протягом життєвого циклу системи (не лише на етапі утилізації чи виходу з експлуатації життєвого циклу). Наприклад, утилізація може відбуватися під час досліджень і розробок, проектування, створення прототипів або експлуатації/технічного обслуговування та включати такі методи, як очищення диска, видалення криптографічних ключів, часткове повторне використання компонентів. Можливості для компроментації під час утилізації впливають на фізичні та логічні дані, включаючи системну документацію в паперових або цифрових файлах; товарно-транспортну документацію; карти пам'яті з програмним кодом; або маршрутизатори чи сервери, які включають постійні носії інформації з песональними даними або конфіденційною інформацією. Крім того, належна утилізація компонентів системи допомагає запобігти потраплянню таких компонентів на сірий ринок.

Пов’язані заходи: MP-6.

Посилання: Немає.

## Додаток А
## БАЗОВІ ПРОФІЛІ БЕЗПЕКИ

У таблиці А.1 надані три базових профілі безпеки для інформаційних систем низької, середньої та високої категорії критичності. Ці базові профілі безпеки є початковою відправною точкою для вибору заходів захисту з метою впровадження (реалізації) в інформаційних системах. Базові профілі безпеки є ієрархічними щодо заходів захисту, що включені в ці профілі. Якщо захід захисту вноситься до базового профілю безпеки, то ідентифікатор класу заходів захисту та номер заходу захисту наводиться у відповідному стовпчику. Посилення заходів захисту вказуються номером посилення. Наприклад, запис АС-11(1) у базовому профілі безпеки вказує на те, що одинадцятий захід захисту з класу управління доступом було обрано разом з першим удосконаленням заходу захисту.

Заходи захисту та посилення заходів захисту, які не внесені в жоден базовий профіль безпеки, можуть бути обрані розробником галузевого або цільового профілю на факультативній основі. Вибір може бути здійснений, наприклад, коли результати оцінювання ризику вказують на необхідність впровадження додаткових заходів захисту або посилення заходів захисту, щоб мати можливість ефективно реагувати на виявлені ризики. Заходи захисту персональних даних вказуються у стовпці «Приватність».

Таблиця А.1 — Базові профілі безпеки

| Шифр | Назва заходу захисту | Приватність | Рівні безпеки | | |
|---|---|---|---|---|---|
| | | | Низький | Середній | Високий |
| УПРАВЛІННЯ ДОСТУПОМ (AC) | | | | | |
| AC-1 | Політика та процедури управління доступом | AC-1 | AC-1 | AC-1 | AC-1 |
| AC-2 | Управління обліковими записами | | AC-2 | AC-2 (1) (2) (3) (4) (5) (13) | AC-2 (1) (2) (3) (4) (5) (11) (12)(13) |
| AC-3 | Забезпечення доступу | AC-3 (14) | AC-3 | AC-3 | AC-3 |
| AC-4 | Управління інформаційними потоками | | | AC-4 | AC-4 (4) |
| AC-5 | Розмежування обов'язків | | | AC-5 | AC-5 |
| AC-6 | Мінімізація повноважень | | | AC-6 (1) (2) (5) (7) (9) (10) | AC-6 (1) (2) (3) (5) (7) (9) (10) |
| AC-7 | Невдалі спроби входу в систему | | AC-7 | AC-7 | AC-7 |
| AC-8 | Попередження про використання системи | | AC-8 | AC-8 | AC-8 |
| AC-9 | Сповіщення про попередній вхід (доступ) | | | | |
| AC-10 | Управління паралельною сесією | | | | AC-10 |
| AC-11 | Блокування пристрою | | | AC-11 (1) | AC-11 (1) |
| AC-12 | Припинення сеансу | | | AC-12 | AC-12 |
| AC-13 | Вилучено | | | | |
| AC-14 | Дозволені дії без ідентифікації або автентифікації | | AC-14 | AC-14 | AC-14 |
| AC-15 | Вилучено | | | | |
| AC-16 | Атрибути безпеки та приватності | | | | |
| AC-17 | Віддалений доступ | | AC-17 | AC-17 (1) (2) (3) (4) | AC-17 (1) (2) (3) (4) |
| AC-18 | Бездротовий доступ | | AC-18 | AC-18 (1) (3) | AC-18 (1) (3) (4) (5) |
| AC-19 | Контроль доступу для мобільних пристроїв | | AC-19 | AC-19 (5) | AC-19 (5) |
| AC-20 | Використання зовнішніх систем | | AC-20 | AC-20 (1) (2) | AC-20 (1) (2) |
| AC-21 | Розповсюдження інформації | | | AC-21 | AC-21 |
| AC-22 | Публічно доступний контент | | AC-22 | AC-22 | AC-22 |
| AC-23 | Захист від несанкціонованого інтелектуального аналізу даних | | | | |
| AC-24 | Рішення щодо управління доступом | | | | |

| Шифр | Назва заходу захисту | Приватність | Рівні безпеки | | |
|---|---|---|---|---|---|
| | | | Низький | Середній | Високий |
| AC-25 | Диспетчер доступу | | | | |
| ОБІЗНАНІСТЬ І НАВЧАННЯ (AT) | | | | | |
| AT-1 | Політика та процедури підвищення обізнаності та навчання | AT-1 | AT-1 | AT-1 | AT-1 |
| AT-2 | Навчання з підвищення обізнаності | AT-2 | AT-2 (2) | AT-2 (2) (3) | AT-2 (2) (3) |
| AT-3 | Рольове навчання | AT-3 (5) | AT-3 | AT-3 | AT-3 |
| AT-4 | Навчальні записи | AT-4 | AT-4 | AT-4 | AT-4 |
| AT-5 | Вилучено | | | | |
| AT-6 | Відгуки про проведені навчання | | | | |
| АУДИТ І ПІДЗВІТНІСТЬ (AU) | | | | | |
| AU-1 | Політика та процедури аудиту та підзвітності | AU-1 | AU-1 | AU-1 | AU-1 |
| AU-2 | Події аудиту | AU-2 | AU-2 | AU-2 | AU-2 |
| AU-3 | Зміст записів аудиту | AU-3 (3) | AU-3 | AU-3 (1) | AU-3 (1) |
| AU-4 | Місткість сховища записів аудиту | | AU-4 | AU-4 | AU-4 |
| AU-5 | Реагування на відмови обробки даних аудиту | | AU-5 | AU-5 | AU-5 (1) (2) |
| AU-6 | Огляд, аналіз і звітність аудиту | | AU-6 | AU-6 (1) (3) | AU-6 (1) (3) (5) (6) |
| AU-7 | Скорочення записів аудиту та формування звіту | | | AU-7 (1) | AU-7 (1) |
| AU-8 | Позначка часу | | AU-8 | AU-8 | AU-8 |
| AU-9 | Захист інформації аудиту | | AU-9 | AU-9 (4) | AU-9 (2) (3) (4) |
| AU-10 | Неспростовність | | | | AU-10 |
| AU-11 | Збереження записів аудиту | AU-11 | AU-11 | AU-11 | AU-11 |
| AU-12 | Генерація даних аудиту | | AU-12 | AU-12 | AU-12 (1) (3) |
| AU-13 | Моніторинг розкриття інформації | | | | |
| AU-14 | Аудит сесії | | | | |
| AU-15 | Альтернативна можливість аудиту | | | | |
| AU-16 | Міжорганізаційний аудит | | | | |
| ОЦІНЮВАННЯ, АКРЕДИТАЦІЯ ТА МОНІТОРИНГ (CA) | | | | | |
| CA-1 | Політика та процедури оцінювання, акредитації та моніторингу | CA-1 | CA-1 | CA-1 | CA-1 |
| CA-2 | Оцінювання | CA-2 | CA-2 | CA-2 (1) | CA-2 (1) (2) |
| CA-3 | Взаємодія систем | | CA-3 | CA-3 | CA-3 (6) |

| Шифр | Назва заходу захисту | Приватність | Рівні безпеки | | |
|---|---|---|---|---|---|
| | | | Низький | Середній | Високий |
| CA-4 | Вилучено | | | | |
| CA-5 | План усунення недоліків та контрольні показники | CA-5 | CA-5 | CA-5 | CA-5 |
| CA-6 | Акредитація | CA-6 | CA-6 | CA-6 | CA-6 |
| CA-7 | Безперервний моніторинг | CA-7 (4) | CA-7 (4) | CA-7 (1) (4) | CA-7 (1) (4) |
| CA-8 | Тестування на проникнення | | | | CA-8 (1) |
| CA-9 | Внутрішні з’єднання системи | | CA-9 | CA-9 | CA-9 |
| УПРАВЛІННЯ КОНФІГУРАЦІЄЮ (CM) | | | | | |
| CM-1 | Політика та процедури управління конфігурацією | CM-1 | CM-1 | CM-1 | CM-1 |
| CM-2 | Базова конфігурація | | CM-2 | CM-2 (2) (3) (7) | CM-2 (2) (3) (7) |
| CM-3 | Управління змінами конфігурації | | | CM-3 (2) (4) | CM-3 (1) (2) (4) (6) |
| CM-4 | Аналіз впливу на безпеку та приватність | CM-4 | CM-4 | CM-4 (2) | CM-4 (1) (2) |
| CM-5 | Обмеження доступу до змін | | CM-5 | CM-5 | CM-5 (1) |
| CM-6 | Налаштування конфігурації | | CM-6 | CM-6 | CM-6 (1) (2) |
| CM-7 | Мінімально необхідна функціональність | | CM-7 | CM-7 (1) (2) (5) | CM-7 (1) (2) (5) |
| CM-8 | Інвентаризація компонентів системи | | CM-8 | CM-8 (1) (3) | CM-8 (1) (2) (3) (4) |
| CM-9 | План управління конфігурацією | | | CM-9 | CM-9 |
| CM-10 | Обмеження використання програмного забезпечення | | CM 10 | CM-10 | CM-10 |
| CM-11 | Встановлене користувачем програмне забезпечення | | CM-11 | CM-11 | CM-11 |
| CM-12 | Розташування інформації | | | CM-12 (1) | CM-12 (1) |
| CM-13 | Відображення дій даних | | | | |
| CM-14 | Підписані компоненти | | | | |
| ПЛАНУВАННЯ БЕЗПЕРЕРВНОЇ РОБОТИ (CP) | | | | | |
| CP-1 | Політика та процедури планування безперервної роботи | | CP-1 | CP-1 | CP-1 |
| CP-2 | План забезпечення безперервної роботи та відновлення функціонування | | CP-2 | CP-2 (1) (3) (8) | CP-2 (1) (2) (3) (5) (8) |
| CP-3 | Навчання із забезпечення безперервної роботи | | CP-3 | CP-3 | CP-3 (1) |
| CP-4 | Тестування плану забезпечення безперервної роботи та відновлення функціонування | | CP-4 | CP-4 (1) | CP-4 (1) (2) |
| CP-5 | Вилучено | | | | |

| Шифр | Назва заходу захисту | Приватність | Рівні безпеки | | |
|---|---|---|---|---|---|
| | | | Низький | Середній | Високий |
| CP-6 | Альтернативне місце зберігання | | | CP-6 (1) (3) | CP-6 (1) (2) (3) |
| CP-7 | Альтернативний майданчик роботи | | | CP-7 (1) (2) (3) | CP-7 (1) (2) (3) (4) |
| CP-8 | Комунікаційні послуги | | | CP-8 (1) (2) | CP-8 (1) (2) (3) (4) |
| CP-9 | Резервне копіювання | | CP-9 | CP-9 (1) (8) | CP-9 (1) (2) (3) (5) (8) |
| CP-10 | Відновлення та відтворення системи | | CP-10 | CP-10 (2) | CP-10 (2) (4) |
| CP-11 | Альтернативні протоколи зв’язку | | | | |
| CP-12 | Безпечний режим | | | | |
| CP-13 | Альтернативні механізми безпеки | | | | |
| ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (IA) | | | | | |
| IA-1 | Політика та процедури ідентифікації та автентифікації | | IA-1 | IA-1 | IA-1 |
| IA-2 | Ідентифікація та автентифікація (користувачів організації) | | IA-2 (1) (2) (8) (12) | IA-2 (1) (2) (8) (12) | IA-2 (1) (2) (5) (8)(12) |
| IA-3 | Ідентифікація та автентифікація пристроїв | | | IA-3 | IA-3 |
| IA-4 | Управління ідентифікацією | | A-4 | IA-4 (4) | IA-4 (4) |
| IA-5 | Управління автентифікатором | | IA-5 (1) | IA-5 (1) (2) (6) | IA-5 (1) (2) (6) |
| IA-6 | Зворотний зв’язок автентифікатора | | IA-6 | IA-6 | IA-6 |
| IA-7 | Автентифікація криптографічного модуля | | IA-7 | IA-7 | IA-7 |
| IA-8 | Ідентифікація та автентифікація (не організаційні користувачі) | | IA-8 (1) (2) (4) | IA-8 (1) (2) (4) | IA-8 (1) (2) (4) |
| IA-9 | Послуги ідентифікації та автентифікації | | | | |
| IA-10 | Адаптивна автентифікація | | | | |
| IA-11 | Повторна автентифікація | | IA-11 | IA-11 | IA-11 |
| IA-12 | Перевірка справжності (ідентичності) | | | IA-12 (2) (3) (5) | IA-12 (2) (3) (4) (5) |
| РЕАГУВАННЯ НА ІНЦИДЕНТИ (IR) | | | | | |
| IR-1 | Політика та процедури реагування на інциденти | IR-1 | IR-1 | IR-1 | IR-1 |
| IR-2 | Навчання з реагуванням на інциденти | IR-2 (3) | IR-2 | IR-2 | IR-2 (1) (2) |
| IR-3 | Перевірка реагувань на інциденти | IR-3 | | IR-3 (2) | IR-3 (2) |

| Шифр | Назва заходу захисту | Приватність | Рівні безпеки | | |
|---|---|---|---|---|---|
| | | | Низький | Середній | Високий |
| IR-4 | Обробка інциденту | IR-4 | IR-4 | IR-4 (1) | IR-4 (1) (4) (11) |
| IR-5 | Моніторинг інциденту | IR-5 | IR-5 | IR-5 | IR-5 (1) |
| IR-6 | Звітність про інциденти | IR-6 | IR-6 | IR-6 (1) (3) | IR-6 (1) (3) |
| IR-7 | Підтримка реагування на інциденти | IR-7 | IR-7 | IR-7 (1) | IR-7 (1) |
| IR-8 | План реагування на інцидент | IR-8 (1) | IR-8 | IR-8 | IR-8 |
| IR-9 | Реагування на витік інформації | | | | |
| IR-10 | Інтегрована команда аналізу інформаційної безпеки | | | | |
| ТЕХНІЧНЕ ОБСЛУГОВУВАННЯ (MA) | | | | | |
| MA-1 | Політика та процедури технічного обслуговування | | MA-1 | MA-1 | MA-1 |
| MA-2 | Контрольоване обслуговування | | MA-2 | MA-2 | MA-2 (2) |
| MA-3 | Інструменти для обслуговування | | | MA-3 (1) (2) (3) | MA-3 (1) (2) (3) |
| MA-4 | Віддалене обслуговування | | MA 4 | MA-4 | MA-4 (3) |
| MA-5 | Технічний персонал | | MA-5 | MA-5 | MA-5 (1) |
| MA-6 | Своєчасне обслуговування | | | MA-6 | MA-6 |
| MA-7 | Технічне обслуговування в польових умовах | | | | |
| ЗАХИСТ НОСІЇВ ІНФОРМАЦІЇ (MP) | | | | | |
| MP-1 | Політика та процедури щодо захисту носіїв інформації | MP-1 | MP-1 | MP-1 | MP-1 |
| MP-2 | Доступ до носіїв інформації | | MP-2 | MP-2 | MP-2 |
| MP-3 | Маркування носіїв інформації | | | MP-3 | MP-3 |
| MP-4 | Зберігання носіїв інформації | | | MP-4 | MP-4 |
| MP-5 | Транспортування носіїв інформації | | | MP-5 | MP-5 |
| MP-6 | Знищення інформації на носіях інформації | MP-6 | MP-6 | MP-6 | MP-6 (1) (2) (3) |
| MP-7 | Використання носіїв інформації | | MP-7 | MP-7 | MP-7 |
| MP-8 | Зниження категорії безпеки носіїв інформації | | | | |
| ФІЗИЧНИЙ ЗАХИСТ І ЗАХИСТ РОБОЧОГО СЕРЕДОВИЩА (PE) | | | | | |
| PE-1 | Політика та процедури фізичного захисту та захисту робочого середовища | | PE-1 | PE-1 | PE-1 |
| PE-2 | Авторизація фізичного доступу | | PE-2 | PE-2 | PE-2 |
| PE-3 | Керування фізичним доступом | | PE-3 | PE-3 | PE-3 (1) |
| PE-4 | Контроль доступу до джерел і ліній електроживлення | | | PE-4 | PE-4 |

| Шифр | Назва заходу захисту | Приватність | Рівні безпеки | | |
|---|---|---|---|---|---|
| | | | Низький | Середній | Високий |
| PE-5 | Контроль доступу для пристроїв виведення інформації | | | PE-5 | PE-5 |
| PE-6 | Моніторинг фізичного доступу | | PE-6 | PE-6 (1) | PE-6 (1) (4) |
| PE-7 | Вилучено | | | | |
| PE-8 | Реєстр доступу відвідувачів | | PE-8 | PE-8 | PE-8 (1) |
| PE-9 | Енергетичне обладнання та кабелі | | | PE-9 | PE-9 |
| PE-10 | Аварійне відключення | | | PE-10 | PE-10 |
| PE-11 | Аварійне енергозабезпечення | | | PE-11 | PE-11 (1) |
| PE-12 | Аварійне освітлення | | PE-12 | PE-12 | PE-12 |
| PE-13 | Протипожежний захист | | PE-13 | PE-13 (1) | PE-13 (1) (2) |
| PE-14 | Контроль температури та вологості | | PE-14 | PE-14 | PE-14 |
| PE-15 | Захист від пошкодження водою | | PE-15 | PE-15 | PE-15 (1) |
| PE-16 | Доставлення та видалення | | PE-16 | PE-16 | PE-16 |
| PE-17 | Альтернативне робоче місце | | | PE-17 | PE-17 |
| PE-18 | Розташування компонентів системи | | | | PE-18 |
| PE-19 | Витік інформації | | | | |
| PE-20 | Моніторинг і відстеження активів | | | | |
| PE-21 | Захист від електромагнітного імпульсу | | | | |
| PE-22 | Маркування компонентів | | | | |
| PE-23 | Розташування об’єкта | | | | |
| ПЛАНУВАННЯ БЕЗПЕКИ (PL) | | | | | |
| PL-1 | Політики та процедури планування безпеки | PL-1 | PL-1 | PL-1 | PL-1 |
| PL-2 | Плани захисту інформації та персональних даних | PL-2 | PL-2 | PL-2 | PL-2 |
| PL-3 | Вилучено | | | | |
| PL-4 | Правила поведінки | PL-4 (1) | PL-4 (1) | PL-4 (1) | PL-4 (1) |
| PL-5 | Вилучено | | | | |
| PL-6 | Вилучено | | | | |
| PL-7 | Концепція експлуатації | | | | |
| PL-8 | Архітектура безпеки та приватності | PL-8 | | PL-8 | PL-8 |
| PL-9 | Централізоване управління | PL-9 | | | |
| PL-10 | Вибір базового профілю безпеки | | PL-10 | PL-10 | PL-10 |

| Шифр | Назва заходу захисту | Приват ність | Рівні безпеки | | |
|---|---|---|---|---|---|
| | | | Низький | Середній | Високий |
| PL-11 | Налаштування базового профілю безпеки | | PL-11 | PL-11 | PL-11 |
| МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ (PM) | | | | | |
| PM-1 | Програма (концепція) інформаційної безпеки | | Заходи захисту класу PM визначені таким чином, щоб сприяти дотриманню вимог законів, нормативних документів, директив, правил, політик і стандартів.<br>Заходи захисту PM не залежать від будь-яких конкретних нормативних документів і безпосередньо не пов'язані з базовими профілями безпеки.<br>Заходи класу PM фокусуються на управлінських і організаційних вимогах щодо безпеки та приватності, є незалежними від будь-якої інформаційної системи та важливими для управління програмами безпеки та приватності.<br>Організації можуть задокументувати заходи захисту у своїй програмі (концепції) безпеки та приватності. Концепція разом з планами захисту інформації та персональних даних для окремих інформаційних систем охоплюють сукупність заходів захисту, які впроваджуються організацією.<br>Конкретні заходи захисту не визначаються базовими профілями безпеки. | | |
| PM-2 | Ролі програми інформаційної безпеки | | | | |
| PM-3 | Ресурси забезпечення інформаційної безпеки та приватності | PM-3 | | | |
| PM-4 | План дій та етапи | PM-4 | | | |
| PM-5 | Інвентаризація системи | PM-5 (1) | | | |
| PM-6 | Показники продуктивності | PM-6 | | | |
| PM-7 | Архітектура підприємства | PM-7 | | | |
| PM-8 | План захисту критичної інфраструктури | PM-8 | | | |
| PM-9 | Стратегія управління ризиками | PM-9 | | | |
| PM-10 | Процес акредитації | PM-10 | | | |
| PM-11 | Визначення завдань і процесів | PM-11 | | | |
| PM-12 | Програма інсайдерської загрози | | | | |
| PM-13 | Безпека та приватність працівників | PM-13 | | | |
| PM-14 | Тестування, навчання та моніторинг | PM-14 | | | |
| PM-15 | Контакти з групами та асоціаціями | | | | |
| PM-16 | Програма інформування про загрози | | | | |
| PM-17 | Захист публічної інформації на зовнішніх системах | PM-17 | | | |
| PM-18 | Програма (концепція) забезпечення приватності | PM-18 | | | |
| PM-19 | Ролі програми приватності | PM-19 | | | |
| PM-20 | Система записів | PM-20 (1) | | | |
| PM-21 | Поширення інформації про програму забезпечення приватності | PM-21 | | | |
| PM-22 | Облік розкриття персональних даних | PM-22 | | | |
| PM-23 | Управління якістю персональних даних | | | | |
| PM-24 | Комісія з управління даними | PM-24 | | | |

| Шифр | Назва заходу захисту | Приватність | Рівні безпеки | | |
|---|---|---|---|---|---|
| | | | Низький | Середній | Високий |
| PM-25 | Комісія з питань цілісності даних | PM-25 | | | |
| PM-26 | Мінімізація персональних даних, що використовуються під час тестування, навчання та досліджень | PM-26 | | | |
| PM-27 | Індивідуальний контроль доступу | PM-27 | | | |
| PM-28 | Управління скаргами | PM-28 | | | |
| PM-29 | Інвентаризація персональних даних | | | | |
| PM-30 | Звіт про приватність | | | | |
| PM-31 | План управління ризиком ланцюга постачання | PM-31 | | | |
| PM-32 | Визначення ризиків | | | | |
| КАДРОВА БЕЗПЕКА (PS) | | | | | |
| PS-1 | Політика та процедури кадрової безпеки | | PS-1 | PS-1 | PS-1 |
| PS-2 | Визначення посадового ризику | | PS-2 | PS-2 | PS-2 |
| PS-3 | Перевірка персоналу | | PS-3 | PS-3 | PS-3 |
| PS-4 | Звільнення персоналу | | PS-4 | PS-4 | PS-4 (2) |
| PS-5 | Переведення персоналу | | PS-5 | PS-5 | PS-5 |
| PS-6 | Угоди про доступ | PS-6 | PS-6 | PS-6 | PS-6 |
| PS-7 | Безпека зовнішнього персоналу | | PS-7 | PS-7 | PS-7 |
| PS-8 | Кадрові санкції | | PS-8 | PS-8 | PS-8 |
| PS-9 | Опис позицій | | PS-9 | PS-9 | PS-9 |
| ПОВНОВАЖЕННЯ НА ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ (PT) | | | | | |
| PT-1 | Політика та процедури обробки персональних даних | PT-1 | Заходи захисту класу PT і заходи контролю прозорості не відносять до базових заходів захисту. Заходи захисту приватності обираються відповідно до критерій, визначених у розділі 2.2 | | |
| PT-2 | Повноваження на обробку персональних даних | PT-2 | | | |
| PT-3 | Цілі обробки персональних даних | PT-3 | | | |
| PT-4 | Згода на обробку персональних даних | PT-4 | | | |
| PT-5 | Повідомлення про конфіденційність | PT-5 (2) | | | |
| PT-6 | Система записів повідомлень про конфіденційність | PT-6 (1) (2) | | | |
| PT-7 | Спеціальні категорії персональних даних | PT-7 (1) (2) | | | |
| PT-8 | Вимоги до відповідності | PT-8 | | | |

| Шифр | Назва заходу захисту | Приватність | Рівні безпеки | | |
|---|---|---|---|---|---|
| | | | Низький | Середній | Високий |
| ОЦІНЮВАННЯ РИЗИКУ (RA) | | | | | |
| RA-1 | Політика та процедури оцінювання ризику | RA-1 | RA-1 | RA-1 | RA-1 |
| RA-2 | Категоріювання безпеки | | RA-2 | RA-2 | RA-2 |
| RA-3 | Оцінювання ризику | RA-3 | RA-3 (1) | RA-3 (1) | RA-3 (1) |
| RA-4 | Вилучено | | | | |
| RA-5 | Сканування вразливостей | | RA-5 (2) (11) | RA-5 (2) (5) (11) | RA-5 (2) (4) (5) (11) |
| RA-6 | Заходи протидії технічній розвідці | | — | — | — |
| RA-7 | Реагування на ризик | RA-7 | RA-7 | RA-7 | RA-7 |
| RA-8 | Оцінювання впливу на приватність | RA-8 | | | |
| RA-9 | Аналіз критичності | | | RA-9 | RA 9 |
| RA-10 | Активний пошук загроз | | | | |
| ПРИДБАННЯ СИСТЕМИ ТА ПОСЛУГ (SA) | | | | | |
| SA-1 | Політика й процедури придбання системи та послуг | SA-1 | SA-1 | SA-1 | SA-1 |
| SA-2 | Розподіл ресурсів | SA-2 | SA-2 | SA-2 | SA-2 |
| SA-3 | Життєвий цикл розробки системи | SA-3 | SA-3 | SA-3 | SA-3 |
| SA-4 | Процес закупівель | SA-4 | SA-4 (10) | SA-4 (1) (2) (9) (10) | SA-4 (1) (2) (5) (9)(10) |
| SA-5 | Системна документація | | SA-5 | SA-5 | SA-5 |
| SA-6 | Вилучено | | | | |
| SA-7 | Вилучено | | | | |
| SA-8 | Безпека та приватність принципів інжинірингу (проєктування) | SA-8 (33) | SA-8 | SA-8 | SA-8 |
| SA-9 | Зовнішні послуги для системи | SA-9 | SA-9 | SA-9 (2) | SA-9 (2) |
| SA-10 | Управління конфігурацією розробника | | | SA-10 | SA-10 |
| SA-11 | Тестування та оцінювання розробника | SA-11 | | SA-11 | SA-11 |
| SA-12 | Вилучено | | | SA-12 | SA-12 (2) (10) (16) |
| SA-13 | Вилучено | | | | |
| SA-14 | Вилучено | | | | |
| SA-15 | Процеси, стандарти та інструменти розробки | | | SA-15 (3) | SA-15 (3) |
| SA-16 | Навчання, що надається розробниками | | | | SA-16 |
| SA-17 | Проєкт і архітектура безпеки розробника | | | | SA-17 |

| Шифр | Назва заходу захисту | Приватність | Рівні безпеки | | |
|---|---|---|---|---|---|
| | | | Низький | Середній | Високий |
| SA-18 | Вилучено | | | | |
| SA-19 | Вилучено | | | | |
| SA-20 | Індивідуальна розробка критичних компонентів | | | | |
| SA-21 | Перевірка розробника | | | | SA-21 |
| SA-22 | Компоненти системи, що не підтримуються | | SA-22 | SA-22 | SA-22 |
| СИСТЕМНИЙ І КОМУНІКАЦІЙНИЙ ЗАХИСТ (SC) | | | | | |
| SC-1 | Політика та процедури захисту системи та комунікацій | | SC-1 | SC-1 | SC-1 |
| SC-2 | Розділення додатків | | | SC-2 | SC-2 |
| SC-3 | Ізоляція функцій безпеки | | | | SC-3 |
| SC-4 | Інформація в загальних ресурсах системи | | | SC-4 | SC-4 |
| SC-5 | Захист від атак «Відмова в обслуговуванні» | | SC-5 | SC-5 | SC-5 |
| SC-6 | Доступність ресурсів | | | | |
| SC-7 | Захист периметра | | SC-7 | SC-7 (3)(4)(5)(7) (8) | SC-7 (3)(4)(5)(7) (8) (18) (21) |
| SC-8 | Конфіденційність та цілісність передачі | | | SC-8 (1) | SC-8 (1) |
| SC-9 | Вилучено | | | | |
| SC-10 | Відключення мережі | | | SC-10 | SC-10 |
| SC-11 | Довірений канал зв’язку | | | | |
| SC-12 | Встановлення та управління криптографічними ключами | | SC-12 | SC-12 | SC-12 (1) |
| SC-13 | Криптографічний захист | | SC-13 | SC-13 | SC-13 |
| SC-14 | Вилучено | | | | |
| SC-15 | Спільні обчислювальні пристрої та застосунки | | SC-15 | SC-15 | SC-15 |
| SC-16 | Передача атрибутів безпеки та приватності | | | | |
| SC-17 | Сертифікати інфраструктури відкритих ключів | | | SC-17 | SC-17 |
| SC-18 | Мобільний код | | | SC-18 | SC-18 |
| SC-19 | Вилучено | | | | |
| SC-20 | Безпечний сервіс регулювання імені/адреси (уповноважене джерело) | | SC-20 | SC-20 | SC-20 |
| SC-21 | Безпечний сервіс регулювання імені/адреси (рекурсивний або кешувальний перетворювач) | | SC-21 | SC-21 | SC-21 |
| SC-22 | Архітектура та забезпечення служби імен/адрес | | SC-22 | SC-22 | SC-22 |

| Шифр | Назва заходу захисту | Приват ність | Рівні безпеки | | |
|---|---|---|---|---|---|
| | | | Низький | Середній | Високий |
| SC-23 | Автентифікація сесії | | | SC-23 | SC-23 |
| SC-24 | Уведення у відомий стан | | | | SC-24 |
| SC-25 | Тонкі вузли | | | | |
| SC-26 | Приманка для зловмисників (honeypots) | | | | |
| SC-27 | Незалежні від платформи застосунки | | | | |
| SC-28 | Захист інформації в стані спокою | | | SC-28 (1) | SC-28 (1) |
| SC-29 | Гетерогенність | | | | |
| SC-30 | Маскування та хибний напрям | | | | |
| SC-31 | Аналіз прихованого каналу | | | | |
| SC-32 | Поділ системи на частини | | | | |
| SC-33 | Вилучено | | | | |
| SC-34 | Незмінювані виконавчі програми | | | | |
| SC-35 | Розпізнавання приманок для зловмисників (honeyclient) | | | | |
| SC-36 | Розподілена обробка та зберігання | | | | |
| SC-37 | Позасмугові канали | | | | |
| SC-38 | Безпека операцій | | | | |
| SC-39 | Ізоляція процесу | | SC-39 | SC-39 | SC-39 |
| SC-40 | Захист бездротового з’єднання | | | | |
| SC-41 | Доступ до портів і пристроїв введення/виведення | | | | |
| SC-42 | Можливості датчика та дані | | | | |
| SC-43 | Обмеження використання | | | | |
| SC-44 | Екрановані камери | | | | |
| SC-45 | Синхронізація системи з часом | | | | |
| SC-46 | Забезпечення виконання міждоменної політики | | | | |
| SC-47 | Альтернативний шлях зв’язку | | | | |
| SC-48 | Переміщення датчика | | | | |
| SC-49 | Примусове апаратне розділення та політика забезпечення виконання | | | | |
| SC-50 | Примусове програмне розділення та політика забезпечення виконання | | | | |
| SC-51 | Апаратний захист | | | | |
| ЦІЛІСНІСТЬ СИСТЕМИ ТА ІНФОРМАЦІЇ (SI) | | | | | |

| Шифр | Назва заходу захисту | Приватність | Рівні безпеки | | |
|---|---|---|---|---|---|
| | | | Низький | Середній | Високий |
| SI-1 | Політика та процедури цілісності інформації | SI-1 | SI-1 | SI-1 | SI-1 |
| SI-2 | Виправлення дефектів | | SI-2 | SI-2 (2) | SI-2 (2) |
| SI-3 | Захист від шкідливого коду | | SI-3 | SI-3 | SI-3 |
| SI-4 | Моніторинг системи | | SI-4 | SI-4 (2) (4) (5) | SI-4 (2) (4) (5) (10)(12)(14) (20) (22) |
| SI-5 | Попередження, рекомендації та директиви з безпеки | | SI-5 | SI-5 | SI-5 (1) |
| SI-6 | Перевірка функцій безпеки та приватності | | | | SI-6 |
| SI-7 | Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації | | | SI-7 (1) (7) | SI-7 (1) (2) (5) (7) (15) |
| SI-8 | Захист від спаму | | | SI-8 (2) | SI-8 (2) |
| SI-9 | Вилучено | | | | |
| SI-10 | Перевірка вводу інформації | | | SI-10 | SI-10 |
| SI-11 | Обробка помилок | | | SI-11 | SI-11 |
| SI-12 | Управління та збереження інформації | SI-12 (1) (2) (3) | SI-12 | SI-12 | SI-12 |
| SI-13 | Передбачуване запобігання збоям | | | | |
| SI-14 | Нестійкість | | | | |
| SI-15 | Фільтрація вихідних даних | | | | |
| SI-16 | Захист пам’яті | | | SI-16 | SI-16 |
| SI-17 | Відмовостійкі процедури | | | | |
| SI-18 | Видалення інформації | SI-18 (4) | | | |
| SI-19 | Операції забезпечення якості даних | SI-19 | | | |
| SI-20 | Деідентифікація | | | | |
| SI-21 | Оновлення інформації | | | | |
| SI-22 | Різновиди інформації | | | | |
| SI-23 | Фрагментація інформації | | | | |
| УПРАВЛІННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ (SR) | | | | | |
| SR-1 | Політика та процедури управління ризиками ланцюга постачання | | SR-1 | SR-1 | SR-1 |
| SR-2 | План управління ризиками ланцюга постачання | | SR-2 (1) | SR-2 (1) | SR-2 (1) |
| SR-3 | Контроль ланцюга постачання і процесів | | SR-3 | SR-3 | SR-3 |

| Шифр | Назва заходу захисту | Приватність | Рівні безпеки | | |
|---|---|---|---|---|---|
| | | | Низький | Середній | Високий |
| SR-4 | Походження | | | | |
| SR-5 | Стратегії придбання, інструменти і методи | | SR-5 | SR-5 | SR-5 |
| SR-6 | Оцінка постачальників | | | SR-6 | SR-6 |
| SR-7 | Безпека операцій ланцюга постачання | | | | |
| SR-8 | Повідомлення про порушення ланцюга постачання | | SR-8 | SR-8 | SR-8 |
| SR-9 | Захист від злому та виявлення | | | | SR-9 (1) |
| SR-10 | Перевірка системи і компонентів системи | | SR-10 | SR-10 | SR-10 |
| SR-11 | Автентичність компоненту | | SR-11 (1) (2) | SR-11 (1) (2) | SR-11 (1) (2) |
| SR-12 | Утилізація компоненту | | SR-12 | SR-12 | SR-12 |

## Додаток Б
## Характеристика заходів захисту в контексті впровадження

У таблиці Б.1 наведена характеристика заходів захисту інформації та персональних даних. Таблиця надає характеристику класів заходів захисту. У таблиці використовуються такі позначення:

«Х» — заходи захисту, які внесені до базового профілю безпеки;

«В» — заходи захисту, що вилучені з каталогу;

«П» — заходи захисту, що пов’язані із захистом персональних даних;

«Т» — заходи захисту, що можуть бути реалізовані технічними засобами в інформаційній системі;

«О» — заходи захисту, що впроваджуються людиною за допомогою нетехнічних засобів (організаційні заходи захисту);

«О/Т» — заходи захисту, що можуть бути реалізовані як технічними, так і організаційними засобами або їх комбінацією;

«Г» — заходи захисту, що можуть використовуватися для забезпечення гарантій безпеки.

Таблиця Б.1 — Характеристика заходів захисту

| Шифр | Назва заходу захисту<br>Назва удосконаленого заходу захисту | Вилучено | Приватність | Впровадження | Гарантії | Профіль безпеки | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Низький | Середній | Високий |
| УПРАВЛІННЯ ДОСТУПОМ (AC) | | | | | | | | |
| **AC-1** | **Політика та процедури управління доступом** | | П | О | Г | Х | Х | Х |
| **AC-2** | **Управління обліковими записами** | | | О | | Х | Х | Х |
| AC-2(1) | Автоматизоване управління системними обліковими записами | | | О | | | Х | Х |
| AC-2(2) | Видалення тимчасових та екстрених облікових записів | | | Т | | | Х | Х |
| AC-2(3) | Деактивація облікових записів | | | Т | | | Х | Х |
| AC-2(4) | Дії при автоматизованому аудиті | | | Т | | | Х | Х |
| AC-2(5) | Вихід із системи за неактивністю | | | О/Т | | | Х | Х |
| AC-2(6) | Динамічне управління привілеями | | | Т | | | | |
| AC-2(7) | Схеми, засновані на ролях | | | О | | | | |
| AC-2(8) | Динамічне управління обліковими записами | | | Т | | | | |
| AC-2(9) | Обмеження на використання спільних і групових облікових записів | | | О | | | | |
| AC-2(10) | Обмежений доступ до привілейованих функцій | В | Включено в AC-2к | | | | | |
| AC-2(11) | Умови використання | | | Т | | | | Х |
| AC-2(12) | Моніторинг нетипового використання облікових записів | | | О/Т | | | | Х |
| AC-2(13) | Деактивація облікових записів осіб з високим рівнем ризику | | | О | | | Х | Х |

| Шифр | Назва заходу захисту<br>Назва удосконаленого заходу захисту | Вилучено | Приватність | Впровадження | Гарантії | Профіль безпеки | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Низький | Середній | Високий |
| **AC-3** | **Забезпечення доступу** | | | T | | X | X | X |
| AC-3(1) | Обмежений доступ до привілейованих функцій | B | Включено в AC-6. | | | | | |
| AC-3(2) | Подвійна авторизація | | | T | | | | |
| AC-3(3) | Мандатне управління доступом | | | T | | | | |
| AC-3(4) | Дискреційне управління доступом | | | T | | | | |
| AC-3(5) | Інформація щодо безпеки | | | T | | | | |
| AC-3(6) | Захист інформації користувача та системи | B | Включено в MP-4, SC-28. | | | | | |
| AC-3(7) | Управління доступом на основі ролей | | | O/T | | | | |
| AC-3(8) | Анулювання прав доступу | | | O/T | | | | |
| AC-3(9) | Керована передача (публікація) інформації | | | O/T | | | | |
| AC-3(10) | Перегляд аудитом механізмів контролю доступу | | | O | | | | |
| AC-3(11) | Обмеження доступу до спеціальної інформації | | | T | | | | |
| AC-3(12) | Встановлення та забезпечення доступу до застосунків | | | T | | | | |
| AC-3(13) | Управління доступом на основі атрибутів | | | T | | | | |
| AC-3(14) | Індивідуальний доступ | | | T | | | | |
| AC-3(15) | Дискреційний та обов’язковий контроль доступу | | | T | | | | |
| **AC-4** | **Управління інформаційними потоками** | | | | | | X | X |
| AC-4(1) | Атрибути безпеки об’єкту | | | T | | | | |
| AC-4(2) | Домени обробки даних | | | T | | | | |
| AC-4(3) | Динамічне управління інформаційним потоком | | | T | | | | |
| AC-4(4) | Управління потоком зашифрованої інформації | | | T | | | | X |
| AC-4(5) | Вбудовування типів даних | | | T | | | | |
| AC-4(6) | Метадані | | | T | | | | |
| AC-4(7) | Механізми одностороннього потоку | | | T | | | | |
| AC-4(8) | Фільтри політики безпеки | | | T | | | | |
| AC-4(9) | Перевірки, що проводить персонал | | | O/T | | | | |
| AC-4(10) | Активація та деактивація фільтрів політики безпеки | | | T | | | | |
| AC-4(11) | Конфігурація фільтрів політики безпеки | | | T | | | | |
| AC-4(12) | Ідентифікатори типу даних | | | T | | | | |

| Шифр | Назва заходу захисту<br>Назва удосконаленого заходу захисту | Вилучено | Приватність | Впровадження | Гарантії | Профіль безпеки | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Низький | Середній | Високий |
| AC-4(13) | Декомпозиція на відповідні політиці субкомпоненти | | | T | | | | |
| AC-4(14) | Обмеження фільтра політики безпеки | | | T | | | | |
| AC-4(15) | Виявлення несанкціонованої інформації | | | T | | | | |
| AC-4(16) | Передача інформації про взаємопов'язані системи | B | Включено в AC-4. | | | | | |
| AC-4(17) | Автентифікація домену | | | T | | | | |
| AC-4(18) | Прив'язка атрибуту безпеки | B | Включено в AC-16. | | | | | |
| AC-4(19) | Перевірка метаданих | | | T | | | | |
| AC-4(20) | Затверджені рішення | | | O | | | | |
| AC-4(21) | Фізичне та логічне відділення інформаційних потоків | | | T | | | | |
| AC-4(22) | Єдиний доступ | | | T | | | | |
| AC-4(23) | Модифікована інформація, яка не підлягає оприлюдненню | | | O/T | | | | |
| AC-4(24) | Внутрішній нормалізований формат | | | T | | | | |
| AC-4(25) | Очищення даних | | | T | | | | |
| AC-4(26) | Дії з фільтрації аудиту | | | O/T | | | | |
| AC-4(27) | Надлишкові/незалежні фільтруючі механізми | | | T | | | | |
| AC-4(28) | Лінійні фільтрувальні канали | | | T | | | | |
| AC-4(29) | Фільтр механізмів оркестровки | | | O/T | | | | |
| AC-4(30) | Механізми фільтрації з використанням кількох процесів | | | T | | | | |
| AC-4(31) | Запобігання невдалим спробам передачі вмісту | | | T | | | | |
| AC-4(32) | Вимоги до процесу передачі інформації | | | T | | | | |
| **AC-5** | **Розмежування обов'язків** | | | O | | | X | X |
| **AC-6** | **Мінімізація повноважень** | | | O | | | X | X |
| AC-6(1) | Авторизований доступ до функцій безпеки | | | O | | | X | X |
| AC-6(2) | Непривілейований доступ до незахищених функцій | | | O | | | X | X |
| AC-6(3) | Мережевий доступ до привілейованих команд | | | O | | | | X |
| AC-6(4) | Роздільні домени обробки | | | O/T | | | | |
| AC-6(5) | Привілейовані облікові записи | | | O | | | X | X |
| AC-6(6) | Привілейований доступ користувачами, що не належать до організації | | | O | | | | |

| Шифр | Назва заходу захисту<br>Назва удосконаленого заходу захисту | Вилучено | Приватність | Впровадження | Гарантії | Профіль безпеки | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Низький | Середній | Високий |
| AC-6(7) | Перегляд повноважень користувача | | | О | | | X | X |
| AC-6(8) | Рівні привілеїв для виконання коду | | | Т | | | | |
| AC-6(9) | Аудит використання привілейованих функцій | | | Т | | | X | X |
| AC-6(10) | Заборона непривілейованим користувачам виконувати привілейовані функції | | | Т | | | X | X |
| **AC-7** | **Невдалі спроби входу в систему** | | | Т | | X | X | X |
| AC-7(1) | Автоматичне блокування облікового запису | В | Включено в AC-7. | | | | | |
| AC-7(2) | Очищення або стирання мобільного пристрою | | | Т | | | | |
| AC-7(3) | Обмеження на спроби біометричного входу | | | О | | | | |
| AC-7(4) | Використання альтернативного фактора | | | О/Т | | | | |
| **AC-8** | **Попередження про використання системи** | | | О/Т | | X | X | X |
| **AC-9** | **Сповіщення про попередній вхід (доступ)** | | | Т | | | | |
| AC-9(1) | Невдалі спроби входу до системи | | | Т | | | | |
| AC-9(2) | Успішні та невдалі спроби входу до системи | | | Т | | | | |
| AC-9(3) | Повідомлення про зміни в обліковому записі | | | Т | | | | |
| AC-9(4) | Додаткова інформація про вхід | | | Т | | | | |
| **AC-10** | **Управління паралельною сесією** | | | Т | | | | X |
| **AC-11** | **Блокування пристрою** | | | Т | | | X | X |
| AC-11(1) | Приховані дисплеї | | | Т | | | X | X |
| **AC-12** | **Припинення сеансу** | | | Т | | | X | X |
| AC-12(1) | Ініційоване користувачем блокування | | | О/Т | | | | |
| AC-12(2) | Повідомлення про припинення сеансу | | | Т | | | | |
| AC-12(3) | Застережне повідомлення про те, що час сесії добігає кінця | | | Т | | | | |
| **AC-13** | **Нагляд і огляд — управління доступом** | В | Включено в AC-2, AU-6. | | | | | |
| **AC-14** | **Дозволені дії без ідентифікації або автентифікації** | | | О | | X | X | X |
| AC-14(1) | Необхідне використання | В | Включено в AC-14. | | | | | |
| **AC-15** | **Автоматизоване маркування** | В | Включено в MP-3. | | | | | |
| **AC-16** | **Атрибути безпеки та приватності** | | | О | | | | |
| AC-16(1) | Динамічне пов’язання атрибутів | | | Т | | | | |

| Шифр | Назва заходу захисту<br>Назва удосконаленого заходу захисту | Вилучено | Приватність | Впровадження | Гарантії | Профіль безпеки | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Низький | Середній | Високий |
| AC-16(2) | Зміна значень атрибутів авторизованими особами | | | T | | | | |
| AC-16(3) | Підтримка системою пов’язання атрибутів | | | T | | | | |
| AC-16(4) | Пов’язання атрибутів авторизованими особами | | | T | | | | |
| AC-16(5) | Відображення атрибутів на пристроях виведення | | | T | | | | |
| AC-16(6) | Підтримка пов’язання атрибутів організацією | | | O | | | | |
| AC-16(7) | Послідовна інтерпретація атрибутів | | | O | | | | |
| AC-16(8) | Техніки та технології пов’язання атрибутів | | | T | | | | |
| AC-16(9) | Перепризначення атрибутів | | | O | | | | |
| AC-16(10) | Конфігурація атрибутів уповноваженими особами | | | O | | | | |
| **AC-17** | **Віддалений доступ** | | | O | | X | X | X |
| AC-17(1) | Автоматизований моніторинг і управління | | | O/T | | | X | X |
| AC-17(2) | Захист конфіденційності та цілісності за допомогою шифрування | | | T | | | X | X |
| AC-17(3) | Керовані точки контролю доступу | | | T | | | X | X |
| AC-17(4) | Привілейовані команди та доступ | | | O | | | X | X |
| AC-17(5) | Моніторинг для неавторизованих підключень | B | Включено в SI-4. | | | | | |
| AC-17(6) | Захист інформації | | | O | | | | |
| AC-17(7) | Додатковий захист для доступу до функцій безпеки | B | Включено в AC-3(10). | | | | | |
| AC-17(8) | Деактивація незахищених протоколів мережі | B | Включено в CM-7. | | | | | |
| AC-17(9) | Відключення або деактивація доступу | | | O | | | | |
| **AC-18** | **Бездротовий доступ** | | | O | | X | X | X |
| AC-18(1) | Автентифікація та шифрування | | | T | | | X | X |
| AC-18(2) | Моніторинг неавторизованих підключень | B | Включено в SI-4. | | | | | |
| AC-18(3) | Відключення бездротової мережі | | | O/T | | | X | X |
| AC-18(4) | Обмеження налаштування користувачами | | | O | | | | X |
| AC-18(5) | Антени та рівень потужності передачі | | | O | | | | X |
| **AC-19** | **Контроль доступу для мобільних пристроїв** | | | O | | X | X | X |

| Шифр | Назва заходу захисту<br>Назва удосконаленого заходу захисту | Вилучено | Приватність | Впровадження | Гарантії | Профіль безпеки | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Низький | Середній | Високий |
| AC-19(1) | Використання записуваних та переносних запам'ятовувальних пристроїв | В | Включено в MP-7. | | | | | |
| AC-19(2) | Використання персональних переносних запам'ятовувальних пристроїв | В | Включено в MP-7. | | | | | |
| AC-19(3) | Використання переносних запам'ятовувальних пристроїв з неідентифікованим власником | В | Включено в MP-7. | | | | | |
| AC-19(4) | Обмеження для засекреченої інформації | | | О | | | | |
| AC-19(5) | Повне шифрування пристроїв і сховищ інформації | | | О | | | Х | Х |
| **AC-20** | **Використання зовнішніх систем** | | | О | | Х | Х | Х |
| AC-20(1) | Обмеження на авторизоване використання | | | О | | | Х | Х |
| AC-20(2) | Переносні пристрої зберігання даних | | | О | | | Х | Х |
| AC-20(3) | Системи та компоненти, що не перебувають у власності організації | | | О | | | | |
| AC-20(4) | Пристрої для зберігання даних, які можуть мати доступ до мережі | | | О | | | | |
| **AC-21** | **Розповсюдження інформації** | | | О | | | Х | Х |
| AC-21(1) | Автоматична підтримка ухвалення рішень | | | Т | | | | |
| AC-21(2) | Пошук і перевірка інформації | | | Т | | | | |
| **AC-22** | **Публічно доступний контент** | | | О | | Х | Х | Х |
| **AC-23** | **Захист від несанкціонованого інтелектуального аналізу даних** | | | О | | | | |
| **AC-24** | **Рішення щодо управління доступом** | | | О | | | | |
| AC-24(1) | Інформація про передачу авторизованого доступу | | | Т | | | | |
| AC-24(2) | Відсутність ідентифікації користувача або процесу, що діє від імені користувача | | | Т | | | | |
| **AC-25** | **Диспетчер доступу** | | | Т | Г | | | |
| ОБІЗНАНІСТЬ І НАВЧАННЯ (AT) | | | | | | | | |
| **AT-1** | **Політика та процедури підвищення обізнаності та навчання** | | П | О | Г | Х | Х | Х |
| **AT-2** | **Навчання з підвищення обізнаності** | | П | О | Г | Х | Х | Х |
| AT-2(1) | Практичні заняття | | П | О | Г | | | |
| AT-2(2) | Внутрішні загрози | | | О | Г | Х | Х | Х |

| Шифр | Назва заходу захисту<br>Назва удосконаленого заходу захисту | Вилучено | Приватність | Впровадження | Гарантії | Профіль безпеки | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Низький | Середній | Високий |
| AT-2(3) | Соціальна інженерія та соціальний інтелектуальний аналіз даних | | | О | Г | | Х | Х |
| AT-2(4) | Підозрілі повідомлення та аномальна поведінка системи | | | О | Г | | | |
| AT-2(5) | Вдосконалена стійка загроза | | | О | Г | | | |
| AT-2(6) | Середовище кіберзагроз | | | О | Г | | | |
| **AT-3** | **Рольове навчання** | | П | О | Г | Х | Х | Х |
| AT-3(1) | Заходи безпеки навколишнього середовища | | | О | Г | | | |
| AT-3(2) | Фізичні заходи безпеки | | | О | Г | | | |
| AT-3(3) | Практичні заняття | | | О | Г | | | |
| AT-3(4) | Підозрілі зв’язки та аномальна поведінка системи | В | Включено в AT-2(4). | | | | | |
| AT-3(5) | Обробка персональної ідентифікаційної інформації | | П | О | Г | | | |
| **AT-4** | **Навчальні записи** | | П | О | Г | Х | Х | Х |
| **AT-5** | **Контакти з групами безпеки та асоціаціями** | В | Включено в PM-15. | | | | | |
| **AT-6** | **Відгуки про проведені навчання** | | | О | Г | | | |
| АУДИТ І ПІДЗВІТНІСТЬ (AU) | | | | | | | | |
| **AU-1** | **Політика та процедури аудиту та підзвітності** | | П | О | Г | Х | Х | Х |
| **AU-2** | **Події аудиту** | | П | О | | Х | Х | Х |
| AU-2(1) | Узагальнення записів про аудит з декількох джерел | В | Включено в AU-12. | | | | | |
| AU-2(2) | Вибір події аудиту за компонентами | В | Включено в AU-12. | | | | | |
| AU-2(3) | Перегляд і оновлення | В | Включено в AU-2. | | | | | |
| AU-2(4) | Привілейовані функції | В | Включено в AC-6(9). | | | | | |
| **AU-3** | **Зміст записів аудиту** | | | Т | | Х | Х | Х |
| AU-3(1) | Додаткова інформація про аудит | | | Т | | | Х | Х |
| AU-3(2) | Централізоване управління плановим змістом записів аудиту | В | Включено в PL-9. | | | | | |
| AU-3(3) | Обмеження елементів персональних даних | | П | О | | | | |
| **AU-4** | **Місткість сховища записів аудиту** | | | О/Т | | Х | Х | Х |
| AU-4(1) | Передача до альтернативного сховища | | | О/Т | | | | |
| **AU-5** | **Реагування на відмови обробки даних аудиту** | | | Т | | Х | Х | Х |
| AU-5(1) | Місткість сховища записів аудиту | | | Т | | | | Х |
| AU-5(2) | Тривожне сповіщення в реальному часі | | | Т | | | | Х |

| Шифр | Назва заходу захисту<br>Назва удосконаленого заходу захисту | Вилучено | Приватність | Впровадження | Гарантії | Профіль безпеки | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Низький | Середній | Високий |
| AU-5(3) | Налаштування порогового обсягу трафіку | | | Т | | | | |
| AU-5(4) | Вимкнення в разі відмови | | | Т | | | | |
| AU-5(5) | Можливість альтернативного журналювання аудиту | | | О | | | | |
| **AU-6** | **Огляд, аналіз і звітність аудиту** | | | О | Г | Х | Х | Х |
| AU-6(1) | Автоматизована інтеграція процесів | | | О | Г | | Х | Х |
| AU-6(2) | Автоматизовані сповіщення про порушення безпеку | В | Включено в SI-4. | | | | | |
| AU-6(3) | Зіставляння сховищ аудиту | | | О | Г | | Х | Х |
| AU-6(4) | Централізований перегляд і аналіз | | | Т | Г | | | |
| AU-6(5) | Інтегрований аналіз записів аудиту | | | О | Г | | | Х |
| AU-6(6) | Кореляція з фізичним моніторингом | | | О | Г | | | Х |
| AU-6(7) | Дозволені дії | | | О | Г | | | |
| AU-6(8) | Аналіз повного тексту привілейованих команд | | | О | Г | | | |
| AU-6(9) | Кореляція з інформацією з нетехнічних джерел | | | О | Г | | | |
| AU-6(10) | Регулювання рівня аудиту | В | Включено в AU-6. | | | | | |
| **AU-7** | **Скорочення записів аудиту та формування звіту** | | | Т | Г | | Х | Х |
| AU-7(1) | Автоматична обробка | | | Т | Г | | Х | Х |
| AU-7(2) | Автоматичне сортування та пошук | В | Включено в AU-7(1). | | | | | |
| **AU-8** | **Позначка часу** | | | Т | | Х | Х | Х |
| AU-8(1) | Синхронізація з авторитетним джерелом часу | В | Включено в SC-45(1). | | | | | |
| AU-8(2) | Вторинне авторитетне джерело часу | В | Включено в SC-45(2). | | | | | |
| **AU-9** | **Захист інформації аудиту** | | | Т | | Х | Х | Х |
| AU-9(1) | Апаратні носії інформації одноразового запису | | | Т | | | | |
| AU-9(2) | Зберігання на окремих фізичних системах або компонентах | | | Т | | | | Х |
| AU-9(3) | Криптографічний захист | | | Т | | | | Х |
| AU-9(4) | Доступ, який надається через членство в підмножині привілейованих користувачів | | | О | | | Х | Х |
| AU-9(5) | Подвійна авторизація | | | О/Т | | | | |
| AU-9(6) | Доступ тільки для читання | | | О/Т | | | | |
| AU-9(7) | Зберігання на компоненті іншої операційної системи | | | О | | | | |
| **AU-10** | **Неспростовність** | | | Т | Г | | | Х |
| AU-10(1) | Асоціація ідентичності | | | Т | Г | | | |

| Шифр | Назва заходу захисту<br>Назва удосконаленого заходу захисту | Вилучено | Приватність | Впровадження | Гарантії | Профіль безпеки | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Низький | Середній | Високий |
| AU-10(2) | Ратифікація прив'язки інформації про ідентичність виробника | | | Т | Г | | | |
| AU-10(3) | Ланцюжок збереження доказів | | | О/Т | Г | | | |
| AU-10(4) | Валідація зв'язку ідентичності переглядача інформації | | | Т | Г | | | |
| AU-10(5) | Цифрові підписи | В | Включено в SI-7. | | | | | |
| **AU-11** | **Збереження записів аудиту** | | П | О | | Х | Х | Х |
| AU-11(1) | Довгострокова можливість отримання | | | О | Г | | | |
| **AU-12** | **Генерація даних аудиту** | | | Т | | Х | Х | Х |
| AU-12(1) | Загальносистемний і синхронізований за часом журналу аудиту | | | Т | | | | Х |
| AU-12(2) | Стандартизовані формати | | | Т | | | | |
| AU-12(3) | Зміни, що вносять авторизовані особи | | | Т | | | | Х |
| AU-12(4) | Аудит запитів персональної ідентифікаційної інформації | | | Т | | | | |
| **AU-13** | **Моніторинг розкриття інформації** | | | О | Г | | | |
| AU-13(1) | Використання автоматичних засобів | | | О/Т | Г | | | |
| AU-13(2) | Огляд сайтів, що підлягають моніторингу | | | О | Г | | | |
| **AU-14** | **Аудит сесії** | | | О/Т | Г | | | |
| AU-14(1) | Система запуску | | | Т | Г | | | |
| AU-14(2) | Захоплення та запис інформації | В | Включено в AU-14. | | | | | |
| AU-14(3) | Дистанційне спостереження та прослуховування | | | Т | Г | | | |
| **AU-15** | **Альтернативна можливість аудиту** | В | Включено в AU-(5). | | | | | |
| **AU-16** | **Міжорганізаційний аудит** | | | О | | | | |
| AU-16(1) | Збереження ідентичності | | | О | | | | |
| AU-16(2) | Обмін інформацією аудиту | | | О | | | | |
| AU-16(3) | Розмежування | | | О | | | | |
| ОЦІНЮВАННЯ, АКРЕДИТАЦІЯ ТА МОНІТОРИНГ (CA) | | | | | | | | |
| **CA-1** | **Політика та процедури оцінювання, акредитації та моніторингу** | | П | О | Г | Х | Х | Х |
| **CA-2** | **Оцінювання** | | П | О | Г | Х | Х | Х |
| CA-2(1) | Незалежні експерти | | | О | Г | | Х | Х |
| CA-2(2) | Спеціалізовані оцінювання | | | О | Г | | | Х |
| CA-2(3) | Зовнішні організації | | | О | Г | | | |

| Шифр | Назва заходу захисту<br>Назва удосконаленого заходу захисту | Вилучено | Приватність | Впровадження | Гарантії | Профіль безпеки | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Низький | Середній | Високий |
| **CA-3** | **Взаємодія систем** | | | О | Г | Х | Х | Х |
| CA-3(1) | Незахищені з’єднання системи | В | Включено в SC-7(25). | | | | | |
| CA-3(2) | Захищені з’єднання системи | В | Включено в SC-7(26). | | | | | |
| CA-3(3) | Несекретні з’єднання системи безпеки, що не є національними | В | Включено в SC-7(27). | | | | | |
| CA-3(4) | Підключення до загальнодоступних мереж | В | Включено в SC-7(28). | | | | | |
| CA-3(5) | Обмеження зв’язку із зовнішніми системами | В | Включено в SC-7(29). | | | | | |
| CA-3(6) | Вторинні та третинні зв’язки | | | О/Т | | | | Х |
| CA-3(7) | Транзитивний обмін інформацією | | | О/Т | | | | |
| **CA-4** | **Сертифікація безпеки** | В | Включено в CA-2. | | | | | |
| **CA-5** | **План усунення недоліків та контрольні показники** | | П | О | Г | Х | Х | Х |
| CA-5(1) | Автоматизація підтримки задля точності та вживаності | | | О | Г | | | |
| **CA-6** | **Акредитація** | | П | О | Г | Х | Х | Х |
| CA-6(1) | Спільна акредитація — одна й та ж організація | | | О | Г | | | |
| CA-6(2) | Спільна акредитація — різні організації | | | О | Г | | | |
| **CA-7** | **Безперервний моніторинг** | | П | О | Г | Х | Х | Х |
| CA-7(1) | Незалежне оцінювання | | | О | Г | | Х | Х |
| CA-7(2) | Види оцінювань | В | Включено в CA-2. | | | | | |
| CA-7(3) | Аналіз тенденції | | | О | Г | | | |
| CA-7(4) | Моніторинг ризику | | П | О/Т | Г | Х | Х | Х |
| CA-7(5) | Узгоджений аналіз | | | О | Г | | | |
| CA-7(6) | Автоматична підтримка моніторингу | | | О/Т | Г | | | |
| **CA-8** | **Тестування на проникнення** | | | О | Г | | | Х |
| CA-8(1) | Незалежна команда або агент на проникнення | | | О | Г | | | Х |
| CA-8(2) | Червона команда | | | О | Г | | | |
| CA-8(3) | Можливості перевірки на проникнення | | | О | Г | | | |
| **CA-9** | **Внутрішні з’єднання системи** | | | О | Г | Х | Х | Х |
| CA-9(1) | Відповідність перевірки | | | О/Т | Г | | | |
| УПРАВЛІННЯ КОНФІГУРАЦІЄЮ (CM) | | | | | | | | |
| **CM-1** | **Політика та процедури управління конфігурацією** | | П | О | Г | Х | Х | Х |
| **CM-2** | **Базова конфігурація** | | | О | Г | Х | Х | Х |

| Шифр | Назва заходу захисту<br>Назва удосконаленого заходу захисту | Вилучено | Приватність | Впровадження | Гарантії | Профіль безпеки | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Низький | Середній | Високий |
| CM-2(1) | Перегляд і оновлення | B | Включено в CM-2. | | | | | |
| CM-2(2) | Автоматизація підтримки задля точності та вживаності | | | O | Г | | X | X |
| CM-2(3) | Зберігання попередніх версій конфігурацій | | | O | Г | | X | X |
| CM-2(4) | Неавторизоване програмне забезпечення | B | Включено в CM-7. | | | | | |
| CM-2(5) | Авторизоване програмне забезпечення | B | Включено в CM-7. | | | | | |
| CM-2(6) | Розробка та середовище тестування | | | O | Г | | | |
| CM-2(7) | Конфігурація систем і компонентів для сфер з високим ризиком | | | O | Г | | X | X |
| **CM-3** | **Управління змінами конфігурації** | | | O | Г | | X | X |
| CM-3(1) | Автоматизоване документування, повідомлення та заборона внесення змін | | | O | Г | | | X |
| CM-3(2) | Тестування, валідація та документування змін | | | O | Г | | X | X |
| CM-3(3) | Автоматизована реалізація змін | | | O | | | | |
| CM-3(4) | Представник безпеки | | | O | | | X | X |
| CM-3(5) | Автоматичне реагування безпеки | | | T | | | | |
| CM-3(6) | Управління засобами криптографічного захисту | | | O | | | | X |
| CM-3(7) | Перегляд змін у системі | | | O | | | | |
| CM-3(8) | Запобігання чи обмеження змін конфігурації | | | T | | | | |
| **CM-4** | **Аналіз впливу на безпеку та приватність** | | П | O | Г | X | X | X |
| CM-4(1) | Відокремлені випробувальні середовища | | | O | Г | | | X |
| CM-4(2) | Верифікація функцій безпеки та приватності | | | O | Г | | X | X |
| **CM-5** | **Обмеження доступу до змін** | | | O | | X | X | X |
| CM-5(1) | Аудит і здійснення автоматичного доступу | | | T | | | | x |
| CM-5(2) | Перегляд змін у системі | B | | Включено в CM-3(7). | | | | |
| CM-5(3) | Підписані компоненти | B | | Включено в CM-14. | | | | |
| CM-5(4) | Подвійна авторизація | | | O/T | | | | |
| CM-5(5) | Обмеження повноважень для виробництва та експлуатації | | | O | | | | |
| CM-5(6) | Обмеження повноважень для бібліотек | | | O | | | | |
| CM-5(7) | Автоматичне впровадження заходів захисту | B | Включено в SI-7. | | | | | |

| Шифр | Назва заходу захисту<br>Назва удосконаленого заходу захисту | Вилучено | Приватність | Впровадження | Гарантії | Профіль безпеки | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Низький | Середній | Високий |
| **CM-6** | **Налаштування конфігурації** | | | О/Т | | Х | Х | Х |
| CM-6(1) | Автоматизоване управління, застосування та верифікація | | | О | | | | Х |
| CM-6(2) | Реагування на несанкціоновані зміни | | | О | | | | Х |
| CM-6(3) | Виявлення неавторизованих змін | В | Включено в SI-7. | | | | | |
| CM-6(4) | Демонстрація відповідності | В | Включено в CM-4. | | | | | |
| **CM-7** | **Мінімізація функціональності** | | | О | | Х | Х | Х |
| CM-7(1) | Періодичний перегляд | | | О | | | Х | Х |
| CM-7(2) | Заборона виконання програми | | | Т | | | Х | Х |
| CM-7(3) | Відповідність реєстрації | | | О | | | | |
| CM-7(4) | Неавторизоване програмне забезпечення — чорний список | | | О/Т | | | | |
| CM-7(5) | Авторизоване програмне забезпечення — білий список | | | О/Т | | | Х | Х |
| CM-7(6) | Замкнуті середовища з обмеженими правами | | | О | | | | |
| CM-7(7) | Виконуваний код в захищеному середовищі | | | О/Т | | | | |
| CM-7(8) | Бінарний або машинний виконуваний код | | | О/Т | | | | |
| CM-7(9) | Заборона використання неавторизованого обладнання | | | О/Т | | | | |
| **CM-8** | **Інвентаризація компонентів системи** | | | О | Г | Х | Х | Х |
| CM-8(1) | Оновлення під час встановлення та видалення | | | О | Г | | Х | Х |
| CM-8(2) | Автоматизована підтримка | | | О | Г | | | Х |
| CM-8(3) | Автоматизоване виявлення неавторизованих компонентів | | | О | Г | | Х | Х |
| CM-8(4) | Інформація про підзвітність | | | О | Г | | | Х |
| CM-8(5) | Виключення дублювання компонентів обліку | В | Включено в CM-8. | | | | | |
| CM-8(6) | Оцінювані налаштування та затверджені відхилення | | | О | Г | | | |
| CM-8(7) | Централізоване сховище | | | О | Г | | | |
| CM-8(8) | Автоматизоване відстеження місця перебування | | | О | Г | | | |
| CM-8(9) | Призначення компонентів системам | | | О | Г | | | |
| **CM-9** | **План управління конфігурацією** | | | О | | | Х | Х |
| CM-9(1) | Встановлення відповідальності | | | О | | | | |
| **CM-10** | **Обмеження використання програмного забезпечення** | | | О | | Х | Х | Х |

| Шифр | Назва заходу захисту<br>Назва удосконаленого заходу захисту | Вилучено | Приватність | Впровадження | Гарантії | Профіль безпеки | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Низький | Середній | Високий |
| CM-10(1) | Програмне забезпечення з відкритим вихідним кодом | | | O | | | | |
| **CM-11** | **Встановлене користувачем програмне забезпечення** | | | O | | X | X | X |
| CM-11(1) | Попередження про несанкціоновану інсталяцію | B | Включено в CM-8(3). | | | | | |
| CM-11(2) | Встановлення програмного забезпечення з привілейованим статусом | | | T | | | | |
| CM-11(3) | Автоматичне виконання та моніторинг | | | T | | | | |
| **CM-12** | **Розташування інформації** | | | O | Г | | X | X |
| CM-12(1) | Автоматизовані інструменти підтримки розташування інформації | | | O | Г | | X | X |
| **CM-13** | **Відображення дій даних** | | | O | | | | |
| **CM-14** | **Підписані компоненти** | | | O/T | | | | |
| ПЛАНУВАННЯ БЕЗПЕРЕРВНОЇ РОБОТИ (CP) | | | | | | | | |
| **CP-1** | **Політика та процедури планування безперервної роботи** | | | O | Г | X | X | X |
| **CP-2** | **План забезпечення безперервної роботи та відновлення функціонування** | | | O | | X | X | X |
| CP-2(1) | Координація з пов’язаними планами | | | O | | | X | X |
| CP-2(2) | Планування ресурсів | | | O | | | | X |
| CP-2(3) | Відновлення критичних функцій | | | O | | | X | X |
| CP-2(4) | Відновлення всіх функцій | B | Включено в CP-2(3). | | | | | |
| CP-2(5) | Безперервність виконання критичних функцій | | | O | | | | X |
| CP-2(6) | Місця альтернативної обробки та зберігання | | | O | | | | |
| CP-2(7) | Координація з провайдерами зовнішніх послуг | | | O | | | | |
| CP-2(8) | Визначення критичних активів | | | O | | | X | X |
| **CP-3** | **Навчання із забезпечення безперервної роботи** | | | O | Г | X | X | X |
| CP-3(1) | Зімітовані події | | | O | Г | | | X |
| CP-3(2) | Автоматизовані навчальні середовища | | | O | Г | | | |
| **CP-4** | **Тестування плану забезпечення безперервної роботи та відновлення функціонування** | | | O | Г | X | X | X |
| CP-4(1) | Координація з пов’язаним планами | | | O | Г | | X | X |
| CP-4(2) | Альтернативна платформа тестування | | | O | Г | | | X |

| Шифр | Назва заходу захисту<br>Назва удосконаленого заходу захисту | Вилучено | Приватність | Впровадження | Гарантії | Профіль безпеки | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Низький | Середній | Високий |
| CP-4(3) | Автоматичне тестування | | | O | Г | | | |
| CP-4(4) | Повне відновлення | | | O | Г | | | |
| CP-4(5) | Самовиклик | | | O/T | Г | | | |
| **CP-5** | **Оновлення плану забезпечення безперервної роботи та відновлення функціонування** | В | Включено в CP-2. | | | | | |
| **CP-6** | **Альтернативне місце зберігання** | | | O | | | X | X |
| CP-6(1) | Відділення від первинного сховища | | | O | | | X | X |
| CP-6(2) | Час відновлення та встановлення цілей відновлення | | | O | | | | X |
| CP-6(3) | Доступність | | | O | | | X | X |
| **CP-7** | **Альтернативний майданчик роботи** | | | O | | | X | X |
| CP-7(1) | Відділення від основного майданчика | | | O | | | X | X |
| CP-7(2) | Доступність | | | O | | | X | X |
| CP-7(3) | Пріоритет обслуговування | | | O | | | X | X |
| CP-7(4) | Підготовка для використання | | | O | | | | X |
| CP-7(5) | Еквівалентні заходи безпеки інформації | В | Включено в CP-7. | | | | | |
| CP-7(6) | Нездатність повернутися на основний майданчик | | | O | | | | |
| **CP-8** | **Комунікаційні послуги** | | | O | | | X | X |
| CP-8(1) | Пріоритет постачання послуг | | | O | | | X | X |
| CP-8(2) | Єдині точки відмови | | | O | | | X | X |
| CP-8(3) | Відділення основних та альтернативних провайдерів | | | O | | | | X |
| CP-8(4) | План забезпечення безперервної роботи постачальника комунікаційних послуг | | | O | | | | X |
| CP-8(5) | Тестування альтернативних комунікаційних послуг | | | O | | | | |
| **CP-9** | **Резервне копіювання** | | | O | | X | X | X |
| CP-9(1) | Випробування на надійність і цілісність | | | O | | | X | X |
| CP-9(2) | Тестування відновлення з використанням зразків | | | O | | | | X |
| CP-9(3) | Відокремлене сховище критичної інформації | | | O | | | | X |
| CP-9(4) | Захист від неавторизованих модифікацій | | Включено в CP-9 | | | | | |
| CP-9(5) | Передача на альтернативне сховище зберігання | | | O | | | | X |

| Шифр | Назва заходу захисту<br>Назва удосконаленого заходу захисту | Вилучено | Приватність | Впровадження | Гарантії | Профіль безпеки | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Низький | Середній | Високий |
| CP-9(6) | Надлишкова вторинна система | | | O | | | | |
| CP-9(7) | Подвійна авторизація | | | O | | | | |
| CP-9(8) | Криптографічний захист | | | O | | | X | X |
| **CP-10** | **Відновлення та відтворення системи** | | | O | | X | X | X |
| CP-10(1) | Тестування плану забезпечення безперервної роботи та відновлення функціонування | B | Включено в CP-4 | | | | | |
| CP-10(2) | Відновлення транзакцій | | | O | | | X | X |
| CP-10(3) | Компенсаційні заходи безпеки | B | Включено в PL-11. | | | | | |
| CP-10(4) | Відновлення в межах часового періоду | | | O | | | | X |
| CP-10(5) | Здатність відмовостійкості | B | Включено в SI-13. | | | | | |
| CP-10(6) | Захист компоненту | | | O | | | | |
| **CP-11** | **Альтернативні протоколи зв'язку** | | | O | | | | |
| **CP-12** | **Безпечний режим** | | | T | Г | | | |
| **CP-13** | **Альтернативні механізми безпеки** | | | O/T | | | | |
| ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ (IA) | | | | | | | | |
| **IA-1** | **Політика та процедури ідентифікації та автентифікації** | | | O | Г | X | X | X |
| **IA-2** | **Ідентифікація та автентифікація (користувачів організації)** | | | O/T | | X | X | X |
| IA-2(1) | Багатофакторна автентифікація привілейованих облікових записів | | | T | | X | X | X |
| IA-2(2) | Багатофакторна автентифікація непривілейованих облікових записів | | | T | | X | X | X |
| IA-2(3) | Локальний доступ до привілейованих облікових записів | B | Включено в IA-2(1)(2). | | | | | |
| IA-2(4) | Локальний доступ до непривілейованих облікових записів | B | Включено в IA-2(1)(2). | | | | | |
| IA-2(5) | Індивідуальна автентифікація з груповою автентифікацією | | | O/T | | | | X |
| IA-2(6) | Мережевий доступ до привілейованих облікових записів — окремий пристрій | | | T | | | | |
| IA-2(7) | Мережевий доступ до непривілейованих облікових записів — окремий пристрій | B | Включено в IA-2(6). | | | | | |
| IA-2(8) | Доступ до облікових записів — стійкість до відтворення | | | T | | X | X | X |
| IA-2(9) | Доступ до непривілейованих облікових записів — стійкість до відтворення | B | Включено в IA-2(8). | | | | | |
| IA-2(10) | Єдина точка входу | | | T | | | | |

| Шифр | Назва заходу захисту<br>Назва удосконаленого заходу захисту | Вилучено | Приватність | Впровадження | Гарантії | Профіль безпеки | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Низький | Середній | Високий |
| IA-2(11) | Віддалений доступ — окремий пристрій | В | Включено в IA-2(6). | | | | | |
| IA-2(12) | Прийняття повноважень для верифікації особистої інформації (PIV credentials) | | | Т | | Х | Х | Х |
| IA-2(13) | Автентифікація по зовнішньому каналу | | | Т | | | | |
| **IA-3** | **Ідентифікація та автентифікація пристроїв** | | | Т | | | Х | Х |
| IA-3(1) | Криптографічна двобічна автентифікація | | | Т | | | | |
| IA-3(2) | Криптографічна двобічна мережа автентифікації | В | Включено в IA-3(1). | | | | | |
| IA-3(3) | Динамічний розподіл адреси | | | О | | | | |
| IA-3(4) | Атестація пристрою | | | О | | | | |
| **IA-4** | **Управління ідентифікацією** | | | О | | Х | Х | Х |
| IA-4(1) | Заборона використання ідентифікаторів облікових записів таких самих, як і публічні ідентифікатори | | | О | | | | |
| IA-4(2) | Авторизація супервайзера | В | Включено в IA-12(1). | | | | | |
| IA-4(3) | Множинні форми сертифікації | | Включено в IA-12(2). | | | | | |
| IA-4(4) | Ідентифікація статусу користувача | | | О | | | Х | Х |
| IA-4(5) | Динамічне управління | | | Т | | | | |
| IA-4(6) | Крос-організаційне управління | | | О | | | | |
| IA-4(7) | Особиста реєстрація | | Включено в IA-12(4). | | | | | |
| IA-4(8) | Попарні псевдонімні ідентифікатори | | | О | | | | |
| IA-4(9) | Обслуговування та захист атрибутів | | | О/Т | | | | |
| **IA-5** | **Управління автентифікатором** | | | О/Т | | Х | Х | Х |
| IA-5(1) | Автентифікація на основі пароля | | | О/Т | | Х | Х | Х |
| IA-5(2) | Автентифікація на основі відкритого ключа | | | Т | | | Х | Х |
| IA-5(3) | Особиста або довірча автентифікація зовнішньої сторони | В | Включено в IA-12(4). | | | | | |
| IA-5(4) | Автоматизована підтримка для визначення міцності пароля | В | Включено в IA-5(1). | | | | | |
| IA-5(5) | Зміна автентифікаторів до доставлення | | | О | | | | |
| IA-5(6) | Захист автентифікаторів | | | О | | | Х | Х |
| IA-5(7) | Відсутність вбудованих незашифрованих статичних автентифікаторів | | | О | | | | |
| IA-5(8) | Багатосистемні облікові записи | | | О | | | | |

| Шифр | Назва заходу захисту<br>Назва удосконаленого заходу захисту | Вилучено | Приватність | Впровадження | Гарантії | Профіль безпеки | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Низький | Середній | Високий |
| IA-5(9) | Управління об’єднанням автентифікаторів | | | O | | | | |
| IA-5(10) | Динамічне зв’язування мандатів | | | T | | | | |
| IA-5(11) | Автентифікація на основі апаратних токенів | B | Включено в IA-2(1)(2). | | | | | |
| IA-5(12) | Ефективність біометричної автентифікації | | | T | | | | |
| IA-5(13) | Закінчення терміну кешування автентифікаторів | | | T | | | | |
| IA-5(14) | Управління змістом довірчих сховищ інфраструктури відкритих ключів | | | O | | | | |
| IA-5(15) | Продукти та послуги, затверджені Управлінням загальними послугами | | | O | | | | |
| IA-5(16) | Передача особистої або довірчої автентифікації зовнішньої сторони | | | O | | | | |
| IA-5(17) | Автоматизовані засоби виявлення атак з використанням біометричних автентифікаторів | | | T | | | | |
| **IA-6** | **Зворотній зв’язок автентифікатора** | | | T | | X | X | X |
| **IA-7** | **Автентифікація криптографічного модуля** | | | T | | X | X | X |
| **IA-8** | **Ідентифікація та автентифікація (користувачі, що не належать до організації)** | | | T | | X | X | X |
| IA-8(1) | Визнання посвідчень ідентифікаційних даних від інших установ | | | T | | X | X | X |
| IA-8(2) | Визнання зовнішніх посвідчень ідентифікаційних даних | | | T | | X | X | X |
| IA-8(3) | Використання затверджених продуктів | | Включено в IA-8(2). | | | | | |
| IA-8(4) | Використання профілів виданих уповноваженим органом | | | T | | X | X | X |
| IA-8(5) | Визнання посвідчень особи, що видаються недержавними органами | | | T | | | | |
| IA-8(6) | Роз’єднання | | | O | | | | |
| **IA-9** | **Послуги ідентифікації та автентифікації** | | | O/T | | | | |
| IA-9(1) | Обмін інформацією | B | Включено в IA-9. | | | | | |
| IA-9(2) | Передача рішень | B | Включено в IA-9. | | | | | |
| **IA-10** | **Адаптивна автентифікація** | | | O | | | | |
| **IA-11** | **Повторна автентифікація** | | | O/T | | X | X | X |
| **IA-12** | **Перевірка справжності (ідентичності)** | | | O | | | X | X |

| Шифр | Назва заходу захисту<br>Назва удосконаленого заходу захисту | Вилучено | Приватність | Впровадження | Гарантії | Профіль безпеки | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Низький | Середній | Високий |
| IA-12(1) | Авторизація супервайзера | | | O | | | | |
| IA-12(2) | Посвідчення особи | | | O | | | X | X |
| IA-12(3) | Перевірка та верифікація доказів ідентичності | | | O | | | X | X |
| IA-12(4) | Очна перевірка та верифікація | | | O | | | | X |
| IA-12(5) | Підтвердження адреси | | | O | | | X | X |
| IA-12(6) | Прийняття ідентифікацій, схвалених третьою стороною | | | O | | | | |
| | РЕАГУВАННЯ НА ІНЦИДЕНТИ (IR) | | | | | | | |
| **IR-1** | **Політика та процедури реагування на інциденти** | | П | O | Г | X | X | X |
| **IR-2** | **Навчання з реагування на інциденти** | | П | O | Г | X | X | X |
| IR-2(1) | Модельована подія | | | O | Г | | | X |
| IR-2(2) | Автоматизовані навчальні середовища | | | O | Г | | | X |
| IR-2(3) | Злам | | П | O | Г | | | |
| **IR-3** | **Перевірка реагувань на інциденти** | | П | O | Г | | X | X |
| IR-3(1) | Автоматичне тестування | | | O | Г | | | |
| IR-3(2) | Координація з пов’язаними планами | | | O | Г | | X | X |
| IR-3(3) | Постійне поліпшення | | | O | Г | | | |
| **IR-4** | **Обробка інциденту** | | П | O | | X | X | X |
| IR-4(1) | Автоматизовані процеси обробки інцидентів | | | O | | | X | X |
| IR-4(2) | Динамічна реконфігурація | | | O | | | | |
| IR-4(3) | Безперервність операцій | | | O | | | | |
| IR-4(4) | Інформаційна кореляція | | | O | | | | X |
| IR-4(5) | Автоматичне вимкнення системи | | | O/T | | | | |
| IR-4(6) | Внутрішні загрози — особливі можливості | | | O | | | | |
| IR-4(7) | Внутрішні загрози — внутрішньоорганізаційна координація | | | O | | | | |
| IR-4(8) | Координація із зовнішніми організаціями | | | O | | | | |
| IR-4(9) | Здатність динамічного реагування | | | O | | | | |
| IR-4(10) | Координація ланцюга постачання | | | O | | | | |
| IR-4(11) | Інтегрована група реагування на інциденти | | | O | | | | X |
| IR-4(12) | Зловмисний код та криміналістичний аналіз | | | O | | | | |
| IR-4(13) | Аналіз поведінки | | | O | | | | |

| Шифр | Назва заходу захисту<br>Назва удосконаленого заходу захисту | Вилучено | Приватність | Впровадження | Гарантії | Профіль безпеки | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Низький | Середній | Високий |
| IR-4(14) | Центр безпеки | | | О/Т | | | | |
| IR-4(15) | Зв’язки з громадкістю та відновлення репутації | | | О | | | | |
| **IR-5** | **Моніторинг інциденту** | | П | О | Г | Х | Х | Х |
| IR-5(1) | Автоматизоване відстеження, збір даних і аналіз | | | О | Г | | | Х |
| **IR-6** | **Звітність про інциденти** | | П | О | | Х | Х | Х |
| IR-6(1) | Автоматичне звітування | | | О | | | Х | Х |
| IR-6(2) | Вразливість, пов’язана з інцидентами | | | О | | | | |
| IR-6(3) | Координація ланцюжка постачання | | | О | | | Х | Х |
| **IR-7** | **Підтримка реагування на інциденти** | | П | О | | Х | Х | Х |
| IR-7(1) | Автоматизація підтримки для доступності інформації та підтримки | | | О | | | Х | Х |
| IR-7(2) | Координація із зовнішніми постачальниками | | | О | | | | |
| **IR-8** | **План реагування на інциденти** | | П | О | | Х | Х | Х |
| IR-8(1) | Обробка персональних даних | | П | О | | | | |
| **IR-9** | **Реагування на витік інформації** | | | О | | | | |
| IR-9(1) | Відповідальний персонал | В | Включено в IR-9. | | | | | |
| IR-9(2) | Тренування | | | О | | | | |
| IR-9(3) | Робота після витоку | | | О | | | | |
| IR-9(4) | Викриття неавторизованого персоналу | | | О | | | | |
| **IR-10** | **Інтегрована команда аналізу інформаційної безпеки** | В | Включено в IR-4(11). | | | | | |
| ТЕХНІЧНЕ ОБСЛУГОВУВАННЯ (MA) | | | | | | | | |
| **MA-1** | **Політика та процедури технічного обслуговування** | | | О | Г | Х | Х | Х |
| **MA-2** | **Контрольоване обслуговування** | | | О | | Х | Х | Х |
| MA-2(1) | Зміст запису | В | Включено в MA-2. | | | | | |
| MA-2(2) | Автоматизована технічна діяльність | | | О | | | | Х |
| **MA-3** | **Інструменти для обслуговування** | | | О | | | Х | Х |
| MA-3(1) | Перевірка інструментів | | | О | | | Х | Х |
| MA-3(2) | Перевірка носіїв інформації | | | О | | | Х | Х |
| MA-3(3) | Запобігання несанкціонованому переміщенню | | | О | | | Х | Х |
| MA-3(4) | Обмеження використання інструмента | | | О/Т | | | | |
| MA-3(5) | Привілейоване виконання | | | О/Т | | | | |

| Шифр | Назва заходу захисту<br>Назва удосконаленого заходу захисту | Вилучено | Приватність | Впровадження | Гарантії | Профіль безпеки | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Низький | Середній | Високий |
| MA-3(6) | Оновлення програмного забезпечення | | | O/T | | | | |
| **MA-4** | **Віддалене обслуговування** | | | O | | X | X | X |
| MA-4(1) | Аудит і огляд | | | O | | | | |
| MA-4(2) | Документування віддаленого обслуговування | B | Включено в MA-1, MA-4. | | | | | |
| MA-4(3) | Порівняльна безпека та очищення | | | O | | | | X |
| MA-4(4) | Автентифікація та розподіл сесії обслуговування | | | O | | | | |
| MA-4(5) | Схвалення та повідомлення | | | O | | | | |
| MA-4(6) | Криптографічний захист | | | O/T | | | | |
| MA-4(7) | Перевірка віддаленого роз'єднання | | | T | | | | |
| **MA-5** | **Технічний персонал** | | | O | | X | X | X |
| MA-5(1) | Особи без належного доступу | | | O | | | | X |
| MA-5(2) | Оформлення рівнів допуску для систем, що обробляють інформацію з обмеженим доступом | | | O | | | | |
| MA-5(3) | Вимоги до громадянства | | | O | | | | |
| MA-5(4) | Іноземні громадяни | | | O | | | | |
| MA-5(5) | Несистемне обслуговування | | | O | | | | |
| **MA-6** | **Своєчасне обслуговування** | | | O | | | X | X |
| MA-6(1) | Профілактичне обслуговування | | | O | | | | |
| MA-6(2) | Планове технічне обслуговування | | | O | | | | |
| MA-6(3) | Автоматизована підтримка планового технічного обслуговування | | | O | | | | |
| **MA-7** | **Технічне обслуговування в польових умовах** | | | O | | | | |
| ЗАХИСТ НОСІЇВ ІНФОРМАЦІЇ (MP) | | | | | | | | |
| **MP-1** | **Політика та процедури щодо захисту носіїв інформації** | | П | O | Г | X | X | X |
| **MP-2** | **Доступ до носіїв інформації** | | | O | | X | X | X |
| MP-2(1) | Автоматизований обмежений доступ | B | Включено в MP-4(2). | | | | | |
| MP-2(2) | Криптографічний захист | B | Включено в SC-28(1). | | | | | |
| **MP-3** | **Маркування носіїв інформації** | | | O | | | X | X |
| **MP-4** | **Зберігання носіїв інформації** | | | O | | | X | X |
| MP-4(1) | Криптографічний захист | B | Включено в SC-28(1). | | | | | |
| MP-4(2) | Автоматизований обмежений доступ | | | O | | | | |

| Шифр | Назва заходу захисту<br>Назва удосконаленого заходу захисту | Вилучено | Приватність | Впровадження | Гарантії | Профіль безпеки | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Низький | Середній | Високий |
| **MP-5** | **Транспортування носіїв інформації** | | | O | | | x | x |
| MP-5(1) | Захист поза контрольованими зонами | | Включено в MP-5. | | | | | |
| MP-5(2) | Документування дій | B | Включено в MP-5. | | | | | |
| MP-5(3) | Зберігачі | | | O | | | | |
| MP-5(4) | Криптографічний захист | B | Включено в SC-28(1). | | | | | |
| **MP-6** | **Знищення інформації на носіях інформації** | | П | O | | X | X | X |
| MP-6(1) | Переглядання, затвердження, відстеження, документування та перевірка | | | O | | | | X |
| MP-6(2) | Перевірка обладнання | | | O | | | | X |
| MP-6(3) | Неруйнівні методи | | | O | | | | X |
| MP-6(4) | Керована несекретна інформація | | Включено в MP-6. | | | | | |
| MP-6(5) | Секретна інформація | B | Включено в MP-6. | | | | | |
| MP-6(6) | Знищення носіїв інформації | B | Включено в MP-6. | | | | | |
| MP-6(7) | Подвійна авторизація | | | O | | | | |
| MP-6(8) | Віддалене очищення або стирання інформації | | | O | | | | |
| **MP-7** | **Використання носіїв інформації** | | | O | | X | X | X |
| MP-7(1) | Заборона використання без визначеного власника | B | Включено в MP-7. | | | | | |
| MP-7(2) | Заборона використання стійких до очищення носіїв інформації | | | O | | | | |
| **MP-8** | **Зниження категорії безпеки носіїв інформації** | | | O | | | | |
| MP-8(1) | Документування процесу | | | O | | | | |
| MP-8(2) | Перевірка обладнання | | | O | | | | |
| MP-8(3) | Критична інформація | | | O | | | | |
| MP-8(4) | Таємна інформація | | | O | | | | |
| ФІЗИЧНИЙ ЗАХИСТ І ЗАХИСТ РОБОЧОГО СЕРЕДОВИЩА (PE) | | | | | | | | |
| **PE-1** | **Політика та процедури фізичного захисту та захисту робочого середовища** | | | O | Г | X | X | X |
| **PE-2** | **Авторизація фізичного доступу** | | | O | | X | X | X |
| PE-2(1) | Доступ на основі посади або ролі | | | O | | | | |
| PE-2(2) | Дві форми ідентифікації | | | O | | | | |
| PE-2(3) | Обмеження доступу без супроводу | | | O | | | | |
| **PE-3** | **Керування фізичним доступом** | | | O | | X | X | X |
| PE-3(1) | Доступ до системи | | | O | | | | X |

| Шифр | Назва заходу захисту<br>Назва удосконаленого заходу захисту | Вилучено | Приватність | Впровадження | Гарантії | Профіль безпеки | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Низький | Середній | Високий |
| PE-3(2) | Межі об’єкту та системи | | | О | | | | |
| PE-3(3) | Безперервна охорона | | | О | | | | |
| PE-3(4) | Корпуси посиленого захисту | | | О | | | | |
| PE-3(5) | Захист від злому | | | О | | | | |
| PE-3(6) | Тестування на можливість проникнення | В | Включено в CA-8. | | | | | |
| PE-3(7) | Фізичні перешкоди | | | О | | | | |
| PE-3(8) | Контроль доступу у вестибюлі (холі) | | | О | | | | |
| **PE-4** | **Контроль доступу до джерел і ліній електроживлення** | | | О | | | Х | Х |
| **PE-5** | **Контроль доступу для пристроїв виведення інформації** | | | О | | | Х | Х |
| PE-5(1) | Доступ до вихідних даних уповноваженими особами | В | Включено в PE-5. | | | | | |
| PE-5(2) | Доступ до вихідних даних фізичними особами | | | Т | | | | |
| PE-5(3) | Маркування пристроїв виведення інформації | В | Включено в PE-22. | | | | | |
| **PE-6** | **Моніторинг фізичного доступу** | | | О | Г | Х | Х | Х |
| PE-6(1) | Охоронна сигналізація та обладнання для спостереження | | | О | Г | | Х | Х |
| PE-6(2) | Автоматичне розпізнавання вторгнень і відповідна реакція | | | О | Г | | | |
| PE-6(3) | Відеоспостереження | | | О | Г | | | |
| PE-6(4) | Моніторинг фізичного доступу до системи | | | О | Г | | | Х |
| **PE-7** | **Контроль відвідувачів** | В | Включено в PE-2, PE-3. | | | | | |
| **PE-8** | **Реєстр доступу відвідувачів** | | | О | Г | Х | Х | Х |
| PE-8(1) | Автоматизоване ведення та перегляд реєстру відвідувачів | | | О | | | | Х |
| PE-8(2) | Реєстр фізичного доступу | В | Включено в PE-2. | | | | | |
| PE-8(3) | Обмеження інформації, що ідентифікують особу | | П | О | | | | |
| **PE-9** | **Енергетичне обладнання та кабелі** | | | О | | | Х | Х |
| PE-9(1) | Резервні кабелі | | | О | | | | |
| PE-9(2) | Автоматичне керування напругою | | | О | | | | |
| **PE-10** | **Аварійне відключення** | | | О | | | Х | Х |
| PE-10(1) | Випадкова та несанкціонована активація | В | Включено в PE-10. | | | | | |
| **PE-11** | **Аварійне енергозабезпечення** | | | О | | | Х | Х |

| Шифр | Назва заходу захисту<br>Назва удосконаленого заходу захисту | Вилучено | Приватність | Впровадження | Гарантії | Профіль безпеки | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Низький | Середній | Високий |
| PE-11(1) | Довгострокове альтернативне джерело живлення — мінімальні експлуатаційні можливості | | | О | | | | Х |
| PE-11(2) | Довгострокове альтернативне джерело живлення — автономне живлення | | | О | | | | |
| **PE-12** | **Аварійне освітлення** | | | О | | Х | Х | Х |
| PE-12(1) | Основні завдання та функції | | | О | | | | |
| **PE-13** | **Протипожежний захист** | | | О | | Х | Х | Х |
| PE-13(1) | Пристрої та системи виявлення | | | О | | | Х | Х |
| PE-13(2) | Пристрої та системи автоматичного пожежогасіння | | | О | | | | Х |
| PE-13(3) | Автоматичне пожежогасіння | В | Включено в PE-13(2). | | | | | |
| PE-13(4) | Перевірки | | | О | | | | |
| **PE-14** | **Контроль температури та вологості** | | | О | | Х | Х | Х |
| PE-14(1) | Автоматичний контроль | | | О | | | | |
| PE-14(2) | Моніторинг за допомогою сигналізації та сповіщень | | | О | | | | |
| **PE-15** | **Захист від пошкодження водою** | | | О | | Х | Х | Х |
| PE-15(1) | Автоматична підтримка | | | О | | | | Х |
| **PE-16** | **Доставлення та видалення** | | | О | | Х | Х | Х |
| **PE-17** | **Альтернативне робоче місце** | | | О | | | Х | Х |
| **PE-18** | **Розташування компонентів системи** | | | О | | | | Х |
| PE-18(1) | Місце розміщення об’єкта | В | Включено в PE-23. | | | | | |
| **PE-19** | **Витік інформації** | | | О | | | | |
| PE-19(1) | Національні політики та процедури щодо ПЕМВН | | | О | | | | |
| **PE-20** | **Моніторинг та відстеження активів** | | | О | | | | |
| **PE-21** | **Захист від електромагнітного імпульсу** | | | О | | | | |
| **PE-22** | **Маркування компонентів** | | | О | | | | |
| **PE-23** | **Розташування об’єкта** | | | О | | | | |
| ПЛАНУВАННЯ БЕЗПЕКИ (PL) | | | | | | | | |
| **PL-1** | **Політики та процедури планування безпеки** | | П | О | Г | Х | Х | Х |
| **PL-2** | **Плани захисту інформації та персональних даних** | | П | О | Г | Х | Х | Х |
| PL-2(1) | Концепція експлуатації | В | Включено в PL-7. | | | | | |
| PL-2(2) | Функціональна архітектура | В | Включено в PL-8. | | | | | |

| Шифр | Назва заходу захисту<br>Назва удосконаленого заходу захисту | Вилучено | Приватність | Впровадження | Гарантії | Профіль безпеки | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Низький | Середній | Високий |
| PL-2(3) | Планування та координація з іншими організаційними структурами | В | Включено в PL-2. | | | | | |
| **PL-3** | **Оновлення планів захисту інформації та персональних даних** | В | Включено в PL-2. | | | | | |
| **PL-4** | **Правила поведінки** | | П | О | Г | Х | Х | Х |
| PL-4(1) | Обмеження на соціальні медіа та мережу | | П | О | Г | Х | Х | Х |
| **PL-5** | **Оцінювання впливу на приватність** | В | Включено в RA-8. | | | | | |
| **PL-6** | **Планування діяльності, пов'язаної з безпекою** | В | Включено в PL-2. | | | | | |
| **PL-7** | **Концепція експлуатації** | | | О | | | | |
| **PL-8** | **Архітектура безпеки та приватності** | | П | О | Г | | Х | Х |
| PL-8(1) | «Глибока оборона» | | | О | Г | | | |
| PL-8(2) | Різноманітність постачальників | | | О | Г | | | |
| **PL-9** | **Централізоване управління** | | П | О | Г | | | |
| **PL-10** | **Вибір базового профілю безпеки** | | | О | | Х | Х | Х |
| **PL-11** | **Налаштування базового профілю безпеки** | | | О | | х | х | х |
| МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ (PM) | | | | | | | | |
| **PM-1** | **Програма (концепція) інформаційної безпеки** | | | О | | | | |
| **PM-2** | **Ролі програми інформаційної безпеки** | | | О | | | | |
| **PM-3** | **Ресурси забезпечення інформаційної безпеки та приватності** | | П | О | | | | |
| **PM-4** | **План дій і етапи** | | П | О | | | | |
| **PM-5** | **Інвентаризація системи** | | | О | | | | |
| PM-5(1) | Інвентаризація персональних даних | | П | О | | | | |
| **PM-6** | **Показники продуктивності** | | П | О | Г | | | |
| **PM-7** | **Архітектура підприємства** | | П | О | | | | |
| PM-7(1) | Розвантаження | | | О | | | | |
| **PM-8** | **План захисту критичної інфраструктури** | | П | О | | | | |
| **PM-9** | **Стратегія управління ризиками** | | П | О | Г | | | |
| **PM-10** | **Процес авторизації** | | П | О | Г | | | |
| **PM-11** | **Визначення завдань і процесів** | | П | О | | | | |
| **PM-12** | **Програма інсайдерської загрози** | | | О | Г | | | |

| Шифр | Назва заходу захисту<br>Назва удосконаленого заходу захисту | Вилучено | Приватність | Впровадження | Гарантії | Профіль безпеки | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Низький | Середній | Високий |
| **PM-13** | **Безпека та приватність працівників** | | П | О | | | | |
| **PM-14** | **Тестування, навчання та моніторинг** | | П | О | Г | | | |
| **PM-15** | **Контакти з групами та асоціаціями з питань безпеки інформації та приватності** | | | О | | | | |
| **PM-16** | **Програма інформування про загрози** | | | О | Г | | | |
| PM-16(1) | Автоматизовані засоби для обміну інформацією про загрози | | | О | Г | | | |
| **PM-17** | **Захист публічної інформації на зовнішніх системах** | | П | О | Г | | | |
| **PM-18** | **Програма (концепція) забезпечення приватності** | | П | О | | | | |
| **PM-19** | **Керівні ролі програми приватності** | | П | О | | | | |
| **PM-20** | **Система записів програми приватності** | | П | О | | | | |
| PM-20(1) | Політика приватності вебсайтів, додатків і цифрових послуг | | П | О | Г | | | |
| **PM-21** | **Облік розкриття персональних даних** | | П | О | | | | |
| **PM-22** | **Управління якістю персональних даних** | | П | О | | | | |
| **PM-23** | **Орган управління персональними даними** | | | О | Г | | | |
| **PM-24** | **Орган з питань цілісності даних** | | П | О | Г | | | |
| **PM-25** | **Мінімізація кількості персональних даних, що використовуються під час тестування, навчання та досліджень** | | П | О | Г | | | |
| **PM-26** | **Управління скаргами** | | П | О | | | | |
| **PM-27** | **Звітність з питань забезпечення приватності** | | П | О | | | | |
| **PM-28** | **Оцінка ризиків** | | П | О | Г | | | |
| **PM-29** | **Ролі керівників програми управління ризиками** | | П | О | | | | |
| **PM-30** | **План управління ризиком ланцюга постачання** | | П | О | Г | | | |
| PM-30(1) | Постачальники критично важливих товарів або товарів, необхідних для виконання місії | | | О | Г | | | |
| **PM-31** | **План безперервного моніторингу** | | П | О | | | | |
| **PM-32** | **Призначення** | | | О | Г | | | |
| КАДРОВА БЕЗПЕКА (PS) | | | | | | | | |

| Шифр | Назва заходу захисту<br>Назва удосконаленого заходу захисту | Вилучено | Приватність | Впровадження | Гарантії | Профіль безпеки | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Низький | Середній | Високий |
| **PS-1** | **Політика та процедури кадрової безпеки** | | | О | Г | X | X | X |
| **PS-2** | **Визначення посадового ризику** | | | О | | X | X | X |
| **PS-3** | **Перевірка персоналу** | | | О | | X | X | X |
| PS-3(1) | Інформація з обмеженим доступом | | | О | | | | |
| PS-3(2) | Інструктаж | | | О | | | | |
| PS-3(3) | Інформація, що потребує додаткових заходів захисту | | | О | | | | |
| PS-3(4) | Вимоги до громадянства | | | О | | | | |
| **PS-4** | **Звільнення персоналу** | | | О | | X | X | X |
| PS-4(1) | Вимоги після закінчення трудової діяльності | | | О | | | | |
| PS-4(2) | Автоматизоване сповіщення | | | О | | | | X |
| **PS-5** | **Переведення персоналу** | | | О | | X | X | X |
| **PS-6** | **Угоди про доступ** | | П | О | Г | X | X | X |
| PS-6(1) | Інформація, що вимагає спеціального захисту | В | Включено в PS-3. | | | | | |
| PS-6(2) | Інформація з обмеженим доступом, що вимагає спеціального захисту | | | О | Г | | | |
| PS-6(3) | Вимоги після закінчення трудової діяльності | | | О | Г | | | |
| **PS-7** | **Безпека зовнішнього персоналу** | | | О | Г | X | X | X |
| **PS-8** | **Кадрові санкції** | | | О | | X | X | X |
| **PS-9** | **Опис позицій** | | | О | | X | X | X |
| ПОВНОВАЖЕННЯ НА ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ (PT) | | | | | | | | |
| **PT-1** | **Політика та процедури обробки персональних даних** | | П | О | Г | | | |
| **PT-2** | **Повноваження на обробку персональних даних** | | П | О | Г | | | |
| PT-2(1) | Тегування даних | | | Т | Г | | | |
| PT-2(2) | Автоматизація | | | О | Г | | | |
| **PT-3** | **Цілі обробки персональних даних** | | П | О | | | | |
| PT-3(1) | Тегування даних | | | Т | Г | | | |
| PT-3(2) | Автоматизація | | | О | Г | | | |
| **PT-4** | **Згода на обробку персональних даних** | | П | О | | | | |
| PT-4(1) | Індивідуальна згода на обробку персональних даних | | | О | | | | |
| PT-4(2) | Своєчасна згода на обробку персональних даних | | | О | | | | |
| PT-4(3) | Відкликання | | | О | | | | |

| Шифр | Назва заходу захисту<br>Назва удосконаленого заходу захисту | Вилучено | Приватність | Впровадження | Гарантії | Профіль безпеки | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Низький | Середній | Високий |
| **PT-5** | **Повідомлення про конфіденційність** | | П | О | | | | |
| PT-5(1) | Своєчасне повідомлення про конфіденційність | | | О | | | | |
| PT-5(2) | Заяви про конфіденційність | | П | О | | | | |
| **PT-6** | **Система записів повідомлень про конфіденційність** | | П | О | | | | |
| PT-6(1) | Звичайне використання | | П | О | | | | |
| PT-6(2) | Правила звільнення | | П | О | | | | |
| **PT-7** | **Спеціальні категорії персональних даних** | | П | О | | | | |
| PT-7(1) | Номери соціального страхування | | П | О | | | | |
| PT-7(2) | Інформація про першу поправку | | П | О | | | | |
| **PT-8** | **Вимоги до відповідності** | | П | О | | | | |
| ОЦІНКА РИЗИКУ (RA) | | | | | | | | |
| **RA-1** | **Політика та процедури оцінювання ризику** | | П | О | Г | Х | Х | Х |
| **RA-2** | **Категоріювання безпеки** | | | О | | Х | Х | Х |
| RA-2(1) | Категоріювання другого рівню | | | О | | | | |
| **RA-3** | **Оцінювання ризику** | | П | О | Г | Х | Х | Х |
| RA-3(1) | Оцінювання ризику ланцюга постачання | | | О | Г | Х | Х | Х |
| RA-3(2) | Використання інформації з усіх доступних джерел | | | О | Г | | | |
| RA-3(3) | Усвідомлення динамічних загроз | | | О | Г | | | |
| RA-3(4) | Прогностична кібер-аналітика | | | О | Г | | | |
| **RA-4** | **Оновлення оцінювання ризику** | | Включено в RA-3. | | | | | |
| **RA-5** | **Сканування вразливостей** | | | О | Г | Х | Х | Х |
| RA-5(1) | Можливість оновлення інструментів | В | Включено в RA-5. | | | | | |
| RA-5(2) | Оновлення за частотою, перед новим скануванням або при ідентифікації | | | О | Г | Х | Х | Х |
| RA-5(3) | Широта та глибина покриття | | | О | Г | | | |
| RA-5(4) | Виявна інформація | | | О | Г | | | Х |
| RA-5(5) | Привілейований доступ | | | О | Г | | Х | Х |
| RA-5(6) | Автоматизований аналіз тенденцій | | | О | Г | | | |
| RA-5(7) | Автоматизоване виявлення та сповіщення про неавторизовані компоненти | В | Включено в CM-8. | | | | | |
| RA-5(8) | Огляд журналів аудиту за минулі періоди | | | О | Г | | | |

| Шифр | Назва заходу захисту<br>Назва удосконаленого заходу захисту | Вилучено | Приватність | Впровадження | Гарантії | Профіль безпеки | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Низький | Середній | Високий |
| RA-5(9) | Тестування та аналіз проникнення | В | Включено в CA-8. | | | | | |
| RA-5(10) | Зіставлення інформації про сканування | | | О | Г | | | |
| **RA-6** | **Заходи протидії технічній розвідці** | | | О | Г | | | |
| **RA-7** | **Реагування на ризик** | | П | О | Г | Х | Х | Х |
| **RA-8** | **Оцінювання впливу на приватність** | | П | О | Г | | | |
| **RA-9** | **Аналіз критичності** | | | О | | | Х | Х |
| **RA-10** | **Активний пошук загроз** | | | О/Т | Г | | | |
| ПРИДБАННЯ СИСТЕМИ ТА ПОСЛУГ (SA) | | | | | | | | |
| **SA-1** | **Політика та процедури придбання системи та послуг** | | П | О | Г | Х | Х | Х |
| **SA-2** | **Розподіл ресурсів** | | П | О | Г | Х | Х | Х |
| **SA-3** | **Життєвий цикл розробки системи** | | П | О | Г | Х | Х | Х |
| SA-3(1) | Управління середовищем розробки | | | О | Г | | | |
| SA-3(2) | Використання реальних даних | | | О | Г | | | |
| SA-3(3) | Оновлення технологій | | | О | Г | | | |
| **SA-4** | **Процес закупівель** | | П | О | Г | Х | Х | Х |
| SA-4(1) | Функціональні властивості заходів | | | О | Г | | Х | Х |
| SA-4(2) | Розробка та впровадження інформації для заходів | | | О | Г | | Х | Х |
| SA-4(3) | Методи, техніки та практики розробки | | | О | Г | | | |
| SA-4(4) | Віднесення компонентів до систем | | Включено в CM-8(9). | | | | | |
| SA-4(5) | Конфігурації системи, компонента та системної служби | | | О | Г | | | Х |
| SA-4(6) | Використання виробів захисту інформації | | | О | Г | | | |
| SA-4(7) | Затверджені профілі захисту | | | О | Г | | | |
| SA-4(8) | План безперервного моніторингу заходів безпеки | | | О | Г | | | |
| SA-4(9) | Функції, порти, протоколи та послуги, що використовуються | | | О | Г | | Х | Х |
| SA-4(10) | Використання затверджених продуктів підтвердження особистості (PIV) | | | О | Г | Х | Х | Х |
| SA-4(11) | Система записів | | | О | Г | | | |
| SA-4(12) | Право власності на дані | | | О | Г | | | |
| **SA-5** | **Системна документація** | | | О | Г | Х | Х | Х |
| SA-5(1) | Функціональні властивості заходів безпеки | | Включено в SA-4(1). | | | | | |

| Шифр | Назва заходу захисту<br>Назва удосконаленого заходу захисту | Вилучено | Приватність | Впровадження | Гарантії | Профіль безпеки | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Низький | Середній | Високий |
| SA-5(2) | Зовнішні системні інтерфейси, що стосуються безпеки | В | Включено в SA-4(2). | | | | | |
| SA-5(3) | Архітектура (проєкт) високого рівня | В | Включено в SA-4(2). | | | | | |
| SA-5(4) | Архітектура (проєкт) низького рівня | В | Включено в SA-4(2). | | | | | |
| SA-5(5) | Вихідний код | | Включено в SA-4(2). | | | | | |
| **SA-6** | **Обмеження щодо використання програмного забезпечення** | В | Включено в CM-10 and SI-7. | | | | | |
| **SA-7** | **Встановлене користувачем програмне забезпечення** | В | Включено в CM-11 and SI-7. | | | | | |
| **SA-8** | **Безпека та приватність принципів інжинірингу (проєктування)** | | | О | Г | Х | Х | Х |
| SA-8(1) | Чітка абстракція | | | О/Т | Г | | | |
| SA-8(2) | Найменш поширений механізм | | | О/Т | Г | | | |
| SA-8(3) | Модульність і багаторівневість | | | О/Т | Г | | | |
| SA-8(4) | Частково впорядковані залежності | | | О/Т | Г | | | |
| SA-8(5) | Ефективний опосередкований доступ | | | О/Т | Г | | | |
| SA-8(6) | Мінімізований обмін | | | О/Т | Г | | | |
| SA-8(7) | Знижена складність | | | О/Т | Г | | | |
| SA-8(8) | Еволюція безпеки в системі | | | О/Т | Г | | | |
| SA-8(9) | Довірені компоненти в системі | | | О/Т | Г | | | |
| SA-8(10) | Ієрархічна довіра | | | О/Т | Г | | | |
| SA-8(11) | Зворотній поріг модифікації | | | О/Т | Г | | | |
| SA-8(12) | Ієрархічний захист | | | О/Т | Г | | | |
| SA-8(13) | Мінімізовані елементи безпеки | | | О/Т | Г | | | |
| SA-8(14) | Найменші привілеї | | | О/Т | Г | | | |
| SA-8(15) | Предикатний дозволу | | | О/Т | Г | | | |
| SA-8(16) | Самостійна надійність | | | О/Т | Г | | | |
| SA-8(17) | Безпечно розподілена композиція | | | О/Т | Г | | | |
| SA-8(18) | Довірені канали комунікації | | | О/Т | Г | | | |
| SA-8(19) | Постійний захист | | | О/Т | Г | | | |
| SA-8(20) | Безпечне керування метаданими | | | О/Т | Г | | | |
| SA-8(21) | Самоаналіз | | | О/Т | Г | | | |
| SA-8(22) | Звітність та відстежуваність | | | О/Т | Г | | | |
| SA-8(23) | Безпечні налаштування за замовчуванням | | | О/Т | Г | | | |
| SA-8(24) | Збої безпеки та відновлення | | | О/Т | Г | | | |
| SA-8(25) | Економічна безпека | | | О/Т | Г | | | |
| SA-8(26) | Безпека продуктивності | | | О/Т | Г | | | |

| Шифр | Назва заходу захисту<br>Назва удосконаленого заходу захисту | Вилучено | Приватність | Впровадження | Гарантії | Профіль безпеки | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Низький | Середній | Високий |
| SA-8(27) | Людський фактор безпеки | | | О/Т | Г | | | |
| SA-8(28) | Прийнятна безпека | | | О/Т | Г | | | |
| SA-8(29) | Повторювані і документовані процедури | | | О/Т | Г | | | |
| SA-8(30) | Процесуальна строгість | | | О/Т | Г | | | |
| SA-8(31) | Безпечна модифікація системи | | | О/Т | Г | | | |
| SA-8(32) | Достатнє документування | | | О/Т | Г | | | |
| SA-8(33) | Мінімізація | | П | О/Т | Г | | | |
| **SA-9** | **Зовнішні послуги для системи** | | П | О | Г | Х | Х | Х |
| SA-9(1) | Оцінювання ризиків та організаційні погодження | | | О | Г | | | |
| SA-9(2) | Визначення функцій, портів, протоколів і служб | | | О | Г | | Х | Х |
| SA-9(3) | Створення та підтримка довірчих відносин з постачальниками | | | О | Г | | | |
| SA-9(4) | Узгодження інтересів споживачів і постачальників | | | О | Г | | | |
| SA-9(5) | Місце обробки, зберігання та обслуговування | | | О | Г | | | |
| SA-9(6) | Криптографічні ключі, керовані організацією | | | О | Г | | | |
| SA-9(7) | Перевірка цілісності, що контролюється організацією | | | О | Г | | | |
| SA-9(8) | Місце обробки та зберігання | | | О | Г | | | |
| **SA-10** | **Управління конфігурацією розробника** | | | О | Г | | Х | Х |
| SA-10(1) | Перевірка цілісності програмного забезпечення та мікропрограм | | | О | Г | | | |
| SA-10(2) | Альтернативні процеси керування конфігурацією | | | О | Г | | | |
| SA-10(3) | Перевірка цілісності апаратних засобів | | | О | Г | | | |
| SA-10(4) | Довірче генерування | | | О | Г | | | |
| SA-10(5) | Цілісність відображення для керування версіями | | | О | Г | | | |
| SA-10(6) | Довірене постачання | | | О | Г | | | |
| SA-10(7) | Представники з питань безпеки та приватності | | | О | Г | | | |
| **SA-11** | **Тестування та оцінювання розробника** | | П | О | Г | | Х | Х |
| SA-11(1) | Аналіз статичного коду | | | О | Г | | | |
| SA-11(2) | Моделювання загроз і аналіз вразливостей | | | О | Г | | | |

| Шифр | Назва заходу захисту<br>Назва удосконаленого заходу захисту | Вилучено | Приватність | Впровадження | Гарантії | Профіль безпеки | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Низький | Середній | Високий |
| SA-11(3) | Незалежна перевірка планів оцінювання та доказів | | | О | Г | | | |
| SA-11(4) | Ручний аналіз кодів | | | О | Г | | | |
| SA-11(5) | Тестування на проникнення | | | О | Г | | | |
| SA-11(6) | Аналіз поверхні атаки | | | О | Г | | | |
| SA-11(7) | Перевірка обсягу тестування та оцінювання | | | О | Г | | | |
| SA-11(8) | Аналіз динамічного коду | | | О | Г | | | |
| SA-11(9) | Інтерактивне тестування безпеки додатків | | | О | Г | | | |
| **SA-12** | **Керування ризиками ланцюга постачання** | В | Включено до класу SR | | | | | |
| SA-12(1) | Стратегії, інструменти та методи закупівель | В | Включено до SR-5 | | | | | |
| SA-12(2) | Аналіз постачальників | В | Включено до SR-6 | | | | | |
| SA-12(3) | Надійне перевезення та зберігання | В | Включено до SR-3 | | | | | |
| SA-12(4) | Диверсифікація постачальників | В | Включено до SR-3(1) | | | | | |
| SA-12(5) | Обмеження шкоди | В | Включено до SR-3(2) | | | | | |
| SA-12(6) | Мінімізація часу закупівель | В | Включено до SR-5(1) | | | | | |
| SA-12(7) | Оцінювання перед вибором, прийняттям та оновленням | В | Включено до SR-5(2) | | | | | |
| SA-12(8) | Використання всебічної розвідувальної інформації | В | Включено до RA-3(2) | | | | | |
| SA-12(9) | Операційна безпека | В | Включено до SR-7 | | | | | |
| SA-12(10) | Перевірка на справжність і незмінність | В | Включено до SR-4(3) | | | | | |
| SA-12(11) | Тестування та аналіз на проникнення | В | Включено до SR-6(1) | | | | | |
| SA-12(12) | Угоди про повідомлення | В | Включено до SR-8 | | | | | |
| SA-12(13) | Компоненти критичних систем | В | Включено в MA-6 and RA-9. | | | | | |
| SA-12(14) | Ідентичність і простежуваність | В | Включено до SR-4(1) та SR-4(2) | | | | | |
| SA-12(15) | Процеси для усунення недоліків або дефектів | В | Включено до SR-3 | | | | | |
| **SA-13** | **Довірчість** | В | Включено в SA-8. | | | | | |
| **SA-14** | **Аналіз критичності** | В | Включено в RA-9. | | | | | |
| SA-14(1) | Критичні компоненти без життєздатних альтернативних джерел | В | Включено в SA-20 | | | | | |
| **SA-15** | **Процеси, стандарти та інструменти розробки** | | | О | Г | | Х | Х |
| SA-15(1) | Показники якості | | | О | Г | | | |

| Шифр | Назва заходу захисту<br>Назва удосконаленого заходу захисту | Вилучено | Приватність | Впровадження | Гарантії | Профіль безпеки | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Низький | Середній | Високий |
| SA-15(2) | Засоби відстеження безпеки | | | О | Г | | | |
| SA-15(3) | Аналіз критичності | | | О | Г | | X | X |
| SA-15(4) | Моделювання загроз і аналіз вразливостей | В | Включено в SA-11(2). | | | | | |
| SA-15(5) | Зменшення поверхні атаки | | | О | Г | | | |
| SA-15(6) | Постійне вдосконалення | | | О | Г | | | |
| SA-15(7) | Автоматизований аналіз вразливостей | | | О | Г | | | |
| SA-15(8) | Повторне використання інформації про загрози та вразливості | | | О | Г | | | |
| SA-15(9) | Використання реальних даних | В | Включено в SA-3(2). | | | | | |
| SA-15(10) | План реагування на інциденти | | | О | Г | | | |
| SA-15(11) | Резервування системи або компоненту | | | О | Г | | | |
| SA-15(12) | Мінімізація персональної інформації | | | О | Г | | | |
| **SA-16** | **Навчання, що надається розробниками** | | | О | Г | | | X |
| **SA-17** | **Проєкт і архітектура безпеки розробника** | | | О | Г | | | X |
| SA-17(1) | Формальна модель політики | | | О | Г | | | |
| SA-17(2) | Компоненти, що необхідні для забезпечення безпеки | | | О | Г | | | |
| SA-17(3) | Формальна відповідність | | | О | Г | | | |
| SA-17(4) | Неформальна відповідність | | | О | Г | | | |
| SA-17(5) | Концептуальний проєкт | | | О | Г | | | |
| SA-17(6) | Структура для тестування | | | О | Г | | | |
| SA-17(7) | Структура для найменшого привілею | | | О | Г | | | |
| SA-17(8) | Оркестровка | | | О | Г | | | |
| SA-17(9) | Різноманітність проектування | | | О | Г | | | |
| **SA-18** | **Захист і виявлення підробки** | В | Включено в SR-9. | | | | | |
| SA-18(1) | Етапи життєвого циклу розробки системи | В | Включено в SR-9(1). | | | | | |
| SA-18(2) | Перевірка систем або компонентів | В | Включено в SR-10. | | | | | |
| **SA-19** | **Справжність компонента** | В | Включено в SR-11. | | | | | |
| SA-19(1) | Навчання боротьбі з підробкою | В | Включено в SR-11(1). | | | | | |
| SA-19(2) | Управління конфігурацією для обслуговування та ремонту компонентів | В | Включено в SR-11(2). | | | | | |
| SA-19(3) | Утилізація компонентів | В | Включено в SR-12. | | | | | |

| Шифр | Назва заходу захисту<br>Назва удосконаленого заходу захисту | Вилучено | Приватність | Впровадження | Гарантії | Профіль безпеки | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Низький | Середній | Високий |
| SA-19(4) | Сканування на підробку | В | Включено в SR-11(3). | | | | | |
| **SA-20** | **Індивідуальна розробка критичних компонентів** | | | О | Г | | | |
| **SA-21** | **Перевірка розробника** | | | О | Г | | | Х |
| SA-21(1) | Перевірка скринінгу | В | Включено в SA-21. | | | | | |
| **SA-22** | **Компоненти системи, що не підтримуються** | | | О | Г | Х | Х | Х |
| SA-22(1) | Альтернативні джерела для постійної підтримки | В | Включено в SA-22 | | | | | |
| **SA-23** | **Спеціалізація** | | | О | Г | | | |
| СИСТЕМНИЙ І КОМУНІКАЦІЙНИЙ ЗАХИСТ (SC) | | | | | | | | |
| **SC-1** | **Політика та процедури захисту системи та комунікацій** | | | О | Г | Х | Х | Х |
| **SC-2** | **Розділення додатків** | | | Т | Г | | Х | Х |
| SC-2(1) | Інтерфейси для непривілейованих користувачів | | | Т | Г | | | |
| **SC-3** | **Ізоляція функцій безпеки** | | | Т | Г | | | Х |
| SC-3(1) | Розділення апаратного забезпечення | | | Т | Г | | | |
| SC-3(2) | Функції управління доступом і потоком | | | Т | Г | | | |
| SC-3(3) | Мінімізація функціональності | | | О/Т | Г | | | |
| SC-3(4) | З’єднання модулів і зв’язність | | | О/Т | Г | | | |
| SC-3(5) | Багаторівнева структура | | | О/Т | Г | | | |
| **SC-4** | **Інформація в загальних ресурсах системи** | | | Т | | | Х | Х |
| SC-4(1) | Рівні безпеки | В | Включено в SC-4. | | | | | |
| SC-4(2) | Багаторівнева або періодична обробка | | | Т | | | | |
| **SC-5** | **Захист від атак «Відмова в обслуговуванні»** | | | Т | | Х | Х | Х |
| SC-5(1) | Обмеження внутрішніх користувачів | | | Т | | | | |
| SC-5(2) | Продуктивність, пропускна здатність і надмірність | | | Т | | | | |
| SC-5(3) | Виявлення та моніторинг | | | Т | | | | |
| **SC-6** | **Доступність ресурсів** | | | Т | Г | | | |
| **SC-7** | **Захист периметра** | | | Т | | Х | Х | Х |
| SC-7(1) | Фізично відділені підмережі | В | Включено в SC-7. | | | | | |
| SC-7(2) | Публічний доступ | В | Включено в SC-7. | | | | | |
| SC-7(3) | Точки доступу | | | Т | | | Х | Х |
| SC-7(4) | Зовнішні комунікаційні служби | | | О | | | Х | Х |

| Шифр | Назва заходу захисту<br>Назва удосконаленого заходу захисту | Вилучено | Приватність | Впровадження | Гарантії | Профіль безпеки | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Низький | Середній | Високий |
| SC-7(5) | Відмова за замовчуванням — дозвіл за винятком | | | Т | | | Х | Х |
| SC-7(6) | Відповідь на розпізнані помилки | В | Включено в SC-7(18). | | | | | |
| SC-7(7) | Запобігання поділу тунелювання для віддалених пристроїв | | | Т | | | Х | Х |
| SC-7(8) | Маршрутизація трафіку з автентифікованих проксі-серверів | | | Т | | | Х | Х |
| SC-7(9) | Обмеження трафіку вихідних повідомлень | | | Т | | | | |
| SC-7(10) | Запобігання ексфільтрації | | | Т | | | | |
| SC-7(11) | Обмеження трафіку вхідних повідомлень | | | Т | | | | |
| SC-7(12) | Захист на основі хосту | | | Т | | | | |
| SC-7(13) | Ізоляція засобів безпеки, механізмів і компонентів підтримки | | | Т | | | | |
| SC-7(14) | Захист від несанкціонованих фізичних з’єднань | | | Т | | | | |
| SC-7(15) | Маршрутизація доступу до привілейованої мережі | | | Т | | | | |
| SC-7(16) | Запобігання виявленню компонентів і пристроїв | | | Т | | | | |
| SC-7(17) | Автоматичне примусове виконання форматів протоколів | | | Т | | | | |
| SC-7(18) | Збій у безпеці | | | Т | Г | | | Х |
| SC-7(19) | Блокування комунікації від хостів, що налаштовані поза організацією | | | Т | | | | |
| SC-7(20) | Динамічна ізоляція та відокремлення | | | Т | | | | |
| SC-7(21) | Ізоляція компонентів системи | | | О/Т | Г | | | Х |
| SC-7(22) | Окремі підмережі для підключення до різних доменів безпеки | | | Т | Г | | | |
| SC-7(23) | Відключення функції зворотного зв’язку відправника про помилку перевірки протоколу | | | Т | | | | |
| SC-7(24) | Персональні дані | | П | О/Т | | | | |
| SC-7(25) | З’єднання з несекретними національними системами безпеки | | | О | | | | |
| SC-7(26) | З’єднання з секретними національними системами безпеки | | | О | | | | |
| SC-7(27) | З’єднання з секретними не національними системами безпеки | | | О | | | | |
| SC-7(28) | З’єднання з загальнодоступними мережами | | | О | | | | |
| SC-7(29) | Окремі підмережі для ізоляції функцій | | | Т | | | | |

| Шифр | Назва заходу захисту<br>Назва удосконаленого заходу захисту | Вилучено | Приватність | Впровадження | Гарантії | Профіль безпеки | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Низький | Середній | Високий |
| **SC-8** | **Конфіденційність та цілісність передачі** | | | T | | | X | X |
| SC-8(1) | Криптографічний захист | | | T | | | X | X |
| SC-8(2) | Попередня і постобробка | | | T | | | | |
| SC-8(3) | Криптографічний захист повідомлень | | | T | | | | |
| SC-8(4) | Приховування або рандомізація комунікації | | | T | | | | |
| SC-8(5) | Захищена система розподілу | | | T | | | | |
| **SC-9** | **Конфіденційність передачі** | B | Включено в SC-8. | | | | | |
| **SC-10** | **Відключення мережі** | | | T | | | X | X |
| **SC-11** | **Довірений канал зв'язку** | | | T | Г | | | |
| SC-11(1) | Логічна ізоляція | | | T | Г | | | |
| **SC-12** | **Встановлення та управління криптографічними ключами** | | | O/T | | X | X | X |
| SC-12(1) | Доступність | | | O/T | | | | X |
| SC-12(2) | Симетричні ключі | | | O/T | | | | |
| SC-12(3) | Асиметричні ключі | | | O/T | | | | |
| SC-12(4) | Сертифікати PKI | B | Включено в SC-12. | | | | | |
| SC-12(5) | Сертифікати PKI / апаратні токени | B | Включено в SC-12. | | | | | |
| SC-12(6) | Фізичний контроль ключів | | | O/T | | | | |
| **SC-13** | **Криптографічний захист** | | | T | | X | X | X |
| SC-13(1) | Стандартна криптографія | B | Включено в SC-13. | | | | | |
| SC-13(2) | Затверджена уповноваженим органом криптографія | B | Включено в SC-13. | | | | | |
| SC-13(3) | Особи без офіційних повноважень | B | Включено в SC-13. | | | | | |
| SC-13(4) | Цифрові підписи | B | Включено в SC-13. | | | | | |
| **SC-14** | **Захист громадського доступу** | B | Включено в AC-2, AC-3, AC-5, SI-3, SI-4, SI-5, SI-7, SI-10. | | | | | |
| **SC-15** | **Спільні обчислювальні пристрої та застосунки** | | | T | | X | X | X |
| SC-15(1) | Фізичне відключення | | | T | | | | |
| SC-15(2) | Блокування трафіку вхідних і вихідних повідомлень | B | Включено в SC-7. | | | | | |
| SC-15(3) | Відключення та видалення в безпечних робочих зонах | | | O | | | | |
| SC-15(4) | Чітка ідентифікація поточних учасників | | | T | | | | |
| **SC-16** | **Передача атрибутів безпеки та приватності** | | | T | | | | |
| SC-16(1) | Перевірка цілісності | | | T | | | | |

| Шифр | Назва заходу захисту<br>Назва удосконаленого заходу захисту | Вилучено | Приватність | Впровадження | Гарантії | Профіль безпеки | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Низький | Середній | Високий |
| SC-16(2) | Механізм антиспуфінгу | | | T | | | | |
| SC-16(3) | Криптографічна прив’язка | | | T | | | | |
| **SC-17** | **Сертифікати інфраструктури відкритих ключів** | | | O/T | | | X | X |
| **SC-18** | **Мобільний код** | | | O | | | X | X |
| SC-18(1) | Ідентифікація неприйнятного коду та вживання виправних дій | | | T | | | | |
| SC-18(2) | Придбання, розробка та використання | | | O | | | | |
| SC-18(3) | Запобігання завантаженню та виконанню | | | T | | | | |
| SC-18(4) | Запобігання автоматичному виконанню | | | T | | | | |
| SC-18(5) | Дозвіл виконання тільки в обмежених середовищах | | | T | | | | |
| **SC-19** | **Інтернет-протокол голосового зв’язку** | B | Технологічно специфічний; адресується як будь-яка інша технологія або протокол | | | | | |
| **SC-20** | **Безпечний сервіс регулювання імені/адреси (уповноважене джерело)** | | | T | | X | X | X |
| SC-20(1) | Дочірній підпростір | B | Включено в SC-20. | | | | | |
| SC-20(2) | Джерело даних і цілісність | | | T | | | | |
| **SC-21** | **Безпечний сервіс регулювання імені/адреси (рекурсивний або кешувальний перетворювач)** | | | T | | X | X | X |
| SC-21(1) | Джерело даних і цілісність | B | Включено в SC-21. | | | | | |
| **SC-22** | **Архітектура та забезпечення служби імен/адрес** | | | T | | X | X | X |
| **SC-23** | **Автентифікація сесії** | | | T | | | X | X |
| SC-23(1) | Анулювання ідентифікатора сеансу зв’язку при виході із системи | | | T | | | | |
| SC-23(2) | Ініційовані користувачем виходи та повідомлення | B | Включено в AC-12(1). | | | | | |
| SC-23(3) | Унікальні ідентифікатори сеансів з рандомізацією | | | T | | | | |
| SC-23(4) | Унікальні ідентифікатори сеансів з рандомізацією | B | Включено в SC-23(3). | | | | | |
| SC-23(5) | Дозволені уповноважені із сертифікації | | | T | | | | |
| **SC-24** | **Уведення у відомий стан** | | | T | Г | | | X |
| **SC-25** | **Тонкі вузли** | | | T | | | | |
| **SC-26** | **Приманка для зловмисників (decoys)** | | | T | | | | |
| SC-26(1) | Виявлення шкідливого коду | B | Включено в SC-35. | | | | | |

| Шифр | Назва заходу захисту<br>Назва удосконаленого заходу захисту | Вилучено | Приватність | Впровадження | Гарантії | Профіль безпеки | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Низький | Середній | Високий |
| **SC-27** | **Незалежні від платформи застосунки** | | | T | | | | |
| **SC-28** | **Захист інформації в стані спокою** | | | T | | | X | X |
| SC-28(1) | Криптографічний захист | | | T | | | X | X |
| SC-28(2) | Автономне сховище | | | O | | | | |
| SC-28(3) | Криптографічні ключі | | | O/T | | | | |
| **SC-29** | **Гетерогенність** | | | O | Г | | | |
| SC-29(1) | Методи віртуалізації | | | O | Г | | | |
| **SC-30** | **Маскування та хибний напрям** | | | O | Г | | | |
| SC-30(1) | Методи віртуалізації | В | Включено в SC-29(1). | | | | | |
| SC-30(2) | Випадковість | | | O | Г | | | |
| SC-30(3) | Зміна місця обробки та зберігання | | | O | Г | | | |
| SC-30(4) | Неправдива інформація | | | O | Г | | | |
| SC-30(5) | Маскування компонентів системи | | | O | Г | | | |
| **SC-31** | **Аналіз прихованого каналу** | | | O | Г | | | |
| SC-31(1) | Тестування прихованих каналів для експлуатації | | | O | Г | | | |
| SC-31(2) | Максимальна пропускна здатність | | | O | Г | | | |
| SC-31(3) | Вимірювання пропускної здатності в робочих середовищах | | | O | Г | | | |
| **SC-32** | **Поділ системи на частини** | | | O/T | Г | | | |
| SC-32(1) | Відокремлені фізичні домени для привілейованих функцій | | | O/T | Г | | | |
| **SC-33** | **Підготовка цілісності передачі** | | Включено в SC-8. | | | | | |
| **SC-34** | **Незмінювані виконавчі програми** | | | T | Г | | | |
| SC-34(1) | Відсутність сховища, доступного для запису інформації | | | O | Г | | | |
| SC-34(2) | Захист цілісності на носії, придатному тільки для читання | | | O | Г | | | |
| SC-34(3) | Апаратний захист | В | Включено в SC-51 | | | | | |
| **SC-35** | **Розпізнавання приманок для зловмисників (honeyclient)** | | | T | | | | |
| **SC-36** | **Розподілена обробка та зберігання** | | | O | Г | | | |
| SC-36(1) | Методи опитування | | | O | Г | | | |
| SC-36(2) | Синхронізація | | | O | Г | | | |
| **SC-37** | **Позасмугові канали** | | | O | Г | | | |
| SC-37(1) | Забезпечення доставлення та передачі | | | O | Г | | | |
| **SC-38** | **Безпека операцій** | | | O | Г | | | |
| **SC-39** | **Ізоляція процесу** | | | T | Г | X | X | X |

| Шифр | Назва заходу захисту<br>Назва удосконаленого заходу захисту | Вилучено | Приватність | Впровадження | Гарантії | Профіль безпеки | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Низький | Середній | Високий |
| SC-39(1) | Апаратне розділення | | | Т | Г | | | |
| SC-39(2) | Ізоляція потоків | | | Т | Г | | | |
| **SC-40** | **Захист бездротового з'єднання** | | | Т | | | | |
| SC-40(1) | Електромагнітні перешкоди | | | Т | | | | |
| SC-40(2) | Зменшення потенціалу виявлення | | | Т | | | | |
| SC-40(3) | Імітаційний або маніпулятивний обмін повідомленнями | | | Т | | | | |
| SC-40(4) | Визначення параметрів сигналу | | | Т | | | | |
| **SC-41** | **Доступ до портів і пристроїв введення/виведення** | | | О/Т | | | | |
| **SC-42** | **Можливості датчика та дані** | | | Т | | | | |
| SC-42(1) | Звітування перед уповноваженими або посадовими особами | | | О | | | | |
| SC-42(2) | Дозволене використання | | | О | | | | |
| SC-42(3) | Заборона використання пристроїв | В | Включено в SC-42. | | | | | |
| SC-42(4) | Повідомлення про збір | | | О | | | | |
| SC-42(5) | Мінімізація збору | | | О | | | | |
| **SC-43** | **Обмеження використання** | | | О/Т | | | | |
| **SC-44** | **Екрановані камери** | | | Т | | | | |
| **SC-45** | **Синхронізація системи з часом** | | | Т | | | | |
| SC-45(1) | Синхронізація з авторитетним джерелом часу | | | Т | | | | |
| SC-45(2) | Вторинне авторитетне джерело часу | | | Т | | | | |
| **SC-46** | **Забезпечення виконання міждоменної політики** | | | Т | | | | |
| **SC-47** | **Альтернативний шлях зв'язку** | | | О/Т | | | | |
| **SC-48** | **Переміщення датчика** | | | О/Т | | | | |
| SC-48(1) | Динамічне переміщення сенсорів та моніторинг можливостей | | | О/Т | | | | |
| **SC-49** | **Примусове апаратне розділення та політика забезпечення виконання** | | | О/Т | Г | | | |
| **SC-50** | **Примусове програмне розділення та політика забезпечення виконання** | | | О/Т | Г | | | |
| **SC-51** | **Апаратний захист** | | | О/Т | Г | | | |
| ЦІЛІСНІСТЬ СИСТЕМИ ТА ІНФОРМАЦІЇ (SI) | | | | | | | | |
| **SI-1** | **Політика та процедури цілісності інформації** | | П | О | Г | Х | Х | Х |
| **SI-2** | **Виправлення дефектів** | | | О | | Х | Х | Х |
| SI-2(1) | Централізоване управління | В | Включено в PL-9 | | | | | |

| Шифр | Назва заходу захисту<br>Назва удосконаленого заходу захисту | Вилучено | Приватність | Впровадження | Гарантії | Профіль безпеки | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Низький | Середній | Високий |
| SI-2(2) | Автоматизоване виправлення дефектів | | | О | | | Х | Х |
| SI-2(3) | Час для усунення дефектів та орієнтири для коригувальних дій | | | О | | | | |
| SI-2(4) | Автоматичні засоби управління виправленнями | | | О/Т | | | | |
| SI-2(5) | Автоматичне оновлення програмного забезпечення та вбудованого програмного забезпечення | | | О/Т | | | | |
| SI-2(6) | Видалення попередніх версій програмного забезпечення та вбудованого програмного забезпечення | | | О/Т | | | | |
| **SI-3** | **Захист від шкідливого коду** | | | О/Т | | Х | Х | Х |
| SI-3(1) | Централізоване управління | В | Включено в PL-9 | | | | | |
| SI-3(2) | Автоматичні оновлення | В | Включено в SI-3. | | | | | |
| SI-3(3) | Непривілейовані користувачі | В | Включено в AC-6(10). | | | | | |
| SI-3(4) | Оновлення тільки привілейованими користувачами | | | О/Т | | | | |
| SI-3(5) | Портативні пристрої зберігання даних | В | Включено в MP-7. | | | | | |
| SI-3(6) | Тестування та верифікація | | | О | | | | |
| SI-3(7) | Виявлення без підпису | В | Включено в SI-3. | | | | | |
| SI-3(8) | Виявлення неавторизованих команд | | | Т | | | | |
| SI-3(9) | Автентифікація віддалених команд | В | Включено в AC-17(10) | | | | | |
| SI-3(10) | Аналіз шкідливого коду | | | О | | | | |
| **SI-4** | **Моніторинг системи** | | | О/Т | Г | Х | Х | Х |
| SI-4(1) | Загальносистемна система виявлення вторгнень (IDS) | | | О/Т | Г | | | |
| SI-4(2) | Автоматизовані засоби та механізми аналізу в реальному часі | | | Т | Г | | Х | Х |
| SI-4(3) | Автоматизовані інструменти та механізми інтеграції | | | Т | Г | | | |
| SI-4(4) | Трафік вхідних і вихідних комунікацій | | | Т | Г | | Х | Х |
| SI-4(5) | Системні сповіщення | | | Т | Г | | Х | Х |
| SI-4(6) | Заборона для непривілейованих користувачів | В | Включено в AC-6(10). | | | | | |
| SI-4(7) | Автоматичне реагування на підозрілі події | | | Т | Г | | | |
| SI-4(8) | Захист інформації моніторингу | В | Включено в SI-4. | | | | | |
| SI-4(9) | Тестування засобів і механізмів моніторингу | | | О | Г | | | |

| Шифр | Назва заходу захисту<br>Назва удосконаленого заходу захисту | Вилучено | Приватність | Впровадження | Гарантії | Профіль безпеки | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Низький | Середній | Високий |
| SI-4(10) | Видимість зашифрованих комунікацій | | | О | Г | | | Х |
| SI-4(11) | Аналіз аномалій трафіку комунікацій | | | О/Т | Г | | | |
| SI-4(12) | Створені організацією автоматизовані сповіщення | | | О/Т | Г | | | Х |
| SI-4(13) | Аналіз трафіку та шаблонів подій | | | О/Т | Г | | | |
| SI-4(14) | Виявлення бездротового вторгнення | | | Т | Г | | | Х |
| SI-4(15) | Перехід від бездротового зв’язку до провідних мереж | | | Т | Г | | | |
| SI-4(16) | Зіставлення інформації моніторингу | | | О/Т | Г | | | |
| SI-4(17) | Інтегрована ситуаційна обізнаність | | | О | Г | | | |
| SI-4(18) | Аналіз трафіку та прихованої ексфільтрації | | | О/Т | Г | | | |
| SI-4(19) | Особи, які являють більший ризик | | | О | Г | | | |
| SI-4(20) | Привілейовані користувачі | | | Т | Г | | | Х |
| SI-4(21) | Випробувальні строки | | | О | Г | | | |
| SI-4(22) | Несанкціоновані послуги мережі | | | Т | Г | | | Х |
| SI-4(23) | Пристрої на основі хоста | | | О | Г | | | |
| SI-4(24) | Ознаки компрометації | | | Т | Г | | | |
| SI-4(25) | Аналіз мережевого трафіку | | | О | Г | | | |
| **SI-5** | **Попередження, рекомендації та директиви з безпеки** | | | О | Г | Х | Х | Х |
| SI-5(1) | Автоматичні попередження та рекомендації | | | Т | Г | | | Х |
| **SI-6** | **Перевірка функцій безпеки та приватності** | | | Т | Г | | | Х |
| SI-6(1) | Сповіщення про неуспішне проходження тестів з безпеки | В | Включено в SI-6. | | | | | |
| SI-6(2) | Автоматизована підтримка розподіленого тестування | | | Т | | | | |
| SI-6(3) | Повідомлення про результати перевірки | | | О | | | | |
| **SI-7** | **Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації** | | | О/Т | Г | | Х | Х |
| SI-7(1) | Перевірка цілісності | | | Т | Г | | Х | Х |
| SI-7(2) | Автоматичні сповіщення про порушення цілісності | | | Т | Г | | | Х |
| SI-7(3) | Інструменти цілісності з централізованим управлінням | | | О | Г | | | |
| SI-7(4) | Упаковка з індикацією ознак її несанкціонованого розкриття | В | Включено в SA-12. | | | | | |

| Шифр | Назва заходу захисту<br>Назва удосконаленого заходу захисту | Вилучено | Приватність | Впровадження | Гарантії | Профіль безпеки | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Низький | Середній | Високий |
| SI-7(5) | Автоматичні відповіді про порушення цілісності | | | Т | Г | | | Х |
| SI-7(6) | Криптографічний захист | | | Т | Г | | | |
| SI-7(7) | Інтеграція виявлення і реагування | | | О | Г | | Х | Х |
| SI-7(8) | Аудит важливих подій | | | Т | Г | | | |
| SI-7(9) | Перевірка процесу завантаження | | | Т | Г | | | |
| SI-7(10) | Захист завантажувального вбудованого програмного забезпечення | | | Т | Г | | | |
| SI-7(11) | Обмежене середовище з обмеженими привілеями | В | Включено в СМ-7(6) | | | | | |
| SI-7(12) | Перевірка цілісності | | | О/Т | Г | | | |
| SI-7(13) | Виконання коду в захищених середовищах | В | Включено в СМ-7(7) | | | | | |
| SI-7(14) | Двійковий або машинно виконуваний код | В | Включено в СМ-7(8) | | | | | |
| SI-7(15) | Автентифікація коду | | | Т | Г | | | Х |
| SI-7(16) | Термін виконання процесу без нагляду | | | О | Г | | | |
| SI-7(17) | Самозахист програми під час виконання | | | О/Т | Г | | | |
| **SI-8** | **Захист від спаму** | | | О | | | Х | Х |
| SI-8(1) | Централізоване управління | В | Включено в PL-9 | | | | | |
| SI-8(2) | Автоматичні оновлення | | | Т | | | Х | Х |
| SI-8(3) | Безперервне навчання | | | Т | | | | |
| **SI-9** | **Обмеження на введення інформації** | В | Включено в AC-2, AC-3, AC-5, AC-6. | | | | | |
| **SI-10** | **Перевірка вводу інформації** | | | Т | Г | | Х | Х |
| SI-10(1) | Можливість ручного перевизначення | | | О/Т | Г | | | |
| SI-10(2) | Перегляд і усунення помилок | | | О | Г | | | |
| SI-10(3) | Передбачувана поведінка | | | О/Т | Г | | | |
| SI-10(4) | Часові взаємодії | | | Т | Г | | | |
| SI-10(5) | Обмеження вхідних даних довіреними джерелами та затвердженими форматами | | | Т | Г | | | |
| SI-10(6) | Профілактика вводу даних | | | Т | Г | | | |
| **SI-11** | **Обробка помилок** | | | Т | | | Х | Х |
| **SI-12** | **Управління та збереження інформації** | | П | О | | Х | Х | Х |
| SI-12(1) | Обмеження елементів персональних даних | | П | О | | | | |

| Шифр | Назва заходу захисту<br>Назва удосконаленого заходу захисту | Вилучено | Приватність | Впровадження | Гарантії | Профіль безпеки | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Низький | Середній | Високий |
| SI-12(2) | Мінімізація використання персональних даних під час тестування, навчання та дослідження | | П | О | | | | |
| SI-12(3) | Видалення інформації | | П | О | | | | |
| **SI-13** | **Передбачуване запобігання збоям** | | | О | Г | | | |
| SI-13(1) | Відповідальність за передачу функцій компонентів | | | О | Г | | | |
| SI-13(2) | Термін виконання процесу без нагляду | В | Включено в SI-7(16). | | | | | |
| SI-13(3) | Ручна передача функцій компонентів | | | О | Г | | | |
| SI-13(4) | Встановлення резервних компонентів і оповіщення | | | О/Т | Г | | | |
| SI-13(5) | Можливість аварійного перемикання | | | О | Г | | | |
| **SI-14** | **Нестійкість** | | | О | Г | | | |
| SI-14(1) | Оновлення з надійних джерел | | | О | Г | | | |
| **SI-15** | **Фільтрація вихідних даних** | | | Т | Г | | | |
| **SI-16** | **Захист пам’яті** | | | Т | Г | | Х | Х |
| **SI-17** | **Відмовостійкі процедури** | | | Т | Г | | | |
| **SI-18** | **Видалення інформації** | | П | О/Т | | | | |
| SI-18(1) | Автоматична підтримка | | | О/Т | | | | |
| SI-18(2) | Тегування даних | | | О/Т | | | | |
| SI-18(3) | Збирання | | | О/Т | | | | |
| SI-18(4) | Індивідуальні запити | | | О/Т | | | | |
| SI-18(5) | Повідомлення про виправлення чи видалення | | | О/Т | | | | |
| **SI-19** | **Операції забезпечення якості даних** | | П | О/Т | | | | |
| SI-19(1) | Оновлення та корекція персональних даних | | П | О/Т | | | | |
| SI-19(2) | Мітки (теги) даних | | П | О/Т | | | | |
| SI-19(3) | Збір персональних даних | | П | О/Т | | | | |
| SI-19(4) | Видалення, маскування, шифрування, гешування або заміна прямих ідентифікаторів | | | Т | | | | |
| SI-19(5) | Контроль розкриття статистичних даних | | | О/Т | | | | |
| SI-19(6) | Диференційна конфіденційність | | | О/Т | | | | |
| SI-19(7) | Перевірене програмне забезпечення | | | О | | | | |
| SI-19(8) | Мотивований порушник | | | О/Т | | | | |

| Шифр | Назва заходу захисту<br>Назва удосконаленого заходу захисту | Вилучено | Приватність | Впровадження | Гарантії | Профіль безпеки | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Низький | Середній | Високий |
| **SI-20** | **Деідентифікація** | | П | О/Т | | | | |
| **SI-21** | **Оновлення інформації** | | | О/Т | Г | | | |
| **SI-22** | **Різновиди інформації** | | | О/Т | Г | | | |
| **SI-23** | **Фрагментація інформації** | | | О/Т | Г | | | |
| УПРАВЛІННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ (SR) | | | | | | | | |
| **SR-1** | **Політика та процедури управління ризиками ланцюга постачання** | | | О | Г | Х | Х | Х |
| **SR-2** | **План управління ризиками ланцюга постачання** | | | О | Г | Х | Х | Х |
| SR-2(1) | Створення команди управління ризиками ланцюга постачання | | | О | Г | Х | Х | Х |
| **SR-3** | **Контроль ланцюга постачання і процесів** | | | О/Т | Г | Х | Х | Х |
| SR-3(1) | Різні бази постачання | | | О | Г | | | |
| SR-3(2) | Обмеження шкоди | | | О | Г | | | |
| SR-3(3) | Перенесення заходів захисту управління ризиками ланцюга постачання до субпідрядників | | | О | Г | | | |
| **SR-4** | **Походження** | | | О | Г | | | |
| SR-4(1) | Ідентичність | | | О | Г | | | |
| SR-4(2) | Унікальна ідентифікація | | | О | Г | | | |
| SR-4(3) | Перевірка на справжність і відсутність внесення змін | | | О | Г | | | |
| SR-4(4) | Перевірка ланцюга цілісності | | | О | Г | | | |
| **SR-5** | **Стратегії придбання, інструменти і методи** | | | О | Г | Х | Х | Х |
| SR-5(1) | Належне постачання | | | О | Г | | | |
| SR-5(2) | Оцінка перед відбором, прийняття, модифікація чи оновлення | | | О | Г | | | |
| **SR-6** | **Оцінка постачальників** | | | О | Г | | Х | Х |
| SR-6(1) | Тестування та аналіз | | | О | Г | | | |
| **SR-7** | **Безпека операцій ланцюга постачання** | | | О | Г | | | |
| **SR-8** | **Повідомлення про порушення ланцюга постачання** | | | О | Г | Х | Х | Х |
| **SR-9** | **Захист від злому та виявлення** | | | О | Г | | | Х |
| SR-9(1) | Етапи чи системи розвитку життєвого циклу | | | О | Г | | | Х |
| **SR-10** | **Перевірка системи і компонентів системи** | | | О | Г | Х | Х | Х |
| **SR-11** | **Автентичність компоненту** | | | О | Г | Х | Х | Х |

| Шифр | Назва заходу захисту<br>Назва удосконаленого заходу захисту | Вилучено | Приватність | Впровадження | Гарантії | Профіль безпеки | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | Низький | Середній | Високий |
| SR-11(1) | Тренування по боротьбі з підробками | | | О | Г | Х | Х | Х |
| SR-11(2) | Контроль конфігурації компонентів, які потребують сервісного обслуговування і ремонту | | | О | Г | Х | Х | Х |
| SR-11(3) | Сканування для виявлення підробок | | | О | Г | | | |
| **SR-12** | **Утилізація компоненту** | | | О | Г | Х | Х | Х |

## Додаток В
## ВІДОБРАЖЕННЯ МІЖНАРОДНИХ СТАНДАРТІВ ТА КАТАЛОГУ ЗАХОДІВ ЗАХИСТУ

Таблиці відображень у цьому додатку надають організаціям загальну інформацію щодо відповідності заходів безпеки цього нормативного документа вимогам міжнародного стандарту ISO/IEC 27001 «Інформаційні технології — Технології безпеки — Системи управління інформаційною безпекою» та міжнародного стандарту ISO/IEC 15408 «Інформаційні технології — Техніка безпеки — Критерії оцінювання IT безпеки».

Таблиці відповідності розроблені з метою зіставлення вимог стандартів з вимогами цього нормативного документа. Зіставлення здійснювалося на якісному рівні, тобто припускається, що реалізація (впровадження) заходів захисту, зіставлених у таблицях, приводять до досягнення еквівалентних результатів захисту. Але це не означає, що розробники профілів захисту повинні припускати повну еквівалентність заходів захисту, базуючись на цих таблицях.

Організації можуть використовувати контрольні відображення, які наведено в Таблицях В.1 та В.2, при організації взаємодії із зовнішніми організаціями, включно з, наприклад, визначенням вимог безпеки та приватності в договорах і угодах. Організації відповідають за аналіз заходів захисту, що впроваджені відповідно до вимог ISO/IEC 27001; їх узгодженість з вимогами цього НД ТЗІ і усунення будь-яких прогалин у сфері застосування заходів захисту. Крім того, через процес вибору заходів захисту, захід захисту, який не застосовується в рамках стандартів ISO/IEC 27001 та ISO/IEC 15408, може бути вибраний, впроваджений і оцінений для забезпечення захисту інформації, відповідно до ризиків. Зрештою, рішення про використання вимог ISO/IEC 27001 та ISO/IEC 15408 залишається за уповноваженою посадовою особою організації.

Примітка: зірочка (*) вказує на те, що захід захисту Каталогу заходів захисту не повною мірою відповідає вимогам ISO/IEC 27001.

Таблиця В.1 — Відображення заходів захисту Каталогу, який наведений в цьому НД ТЗІ на вимоги ISO/IEC27001

| Шифр | **Каталог заходів захисту** | **Вимоги ISO/IEC 27001** |
|---|---|---|
| AC-1 | Політика та процедури управління доступом | 5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.9.1.1, A.12.1.1, A.18.1.1, A.18.2.2 |
| AC-2 | Управління обліковими записами | A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6 |
| AC-3 | Забезпечення доступу | A.6.2.2, A.9.1.2, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.1, A.14.1.2, A.14.1.3, A.18.1.3 |
| AC-4 | Управління інформаційними потоками | A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 |
| AC-5 | Розмежування обов’язків | A.6.1.2 |
| AC-6 | Мінімізація повноважень | A.9.1.2, A.9.2.3, A.9.4.4, A.9.4.5 |
| AC-7 | Невдалі спроби входу в систему | A.9.4.2 |
| AC-8 | Попередження про використання системи | A.9.4.2 |
| AC-9 | Сповіщення про попередній вхід (доступ) | A.9.4.2 |
| AC-10 | Управління паралельною сесією | H/A |

| Шифр | **Каталог заходів захисту** | **Вимоги ISO/IEC 27001** |
|---|---|---|
| AC-11 | Блокування пристрою | A.11.2.8, A.11.2.9 |
| AC-12 | Припинення сеансу | H/A |
| AC-13 | Вилучено | --- |
| AC-14 | Дозволені дії без ідентифікації або автентифікації | H/A |
| AC-15 | Вилучено | --- |
| AC-16 | Атрибути безпеки та приватності | H/A |
| AC-17 | Віддалений доступ | A.6.2.1, A.6.2.2, A.13.1.1, A.13.2.1, A.14.1.2 |
| AC-18 | Бездротовий доступ | A.6.2.1, A.13.1.1, A.13.2.1 |
| AC-19 | Контроль доступу для мобільних пристроїв | A.6.2.1, A.11.1.5, A.11.2.6, A.13.2.1 |
| AC-20 | Використання зовнішніх систем | A.11.2.6, A.13.1.1, A.13.2.1 |
| AC-21 | Розповсюдження інформації | H/A |
| AC-22 | Публічно доступний контент | H/A |
| AC-23 | Захист від несанкціонованого інтелектуального аналізу даних | H/A |
| AC-24 | Рішення щодо управління доступом | A.9.4.1* |
| AC-25 | Диспетчер доступу | H/A |
| AT-1 | Політика та процедури підвищення обізнаності та навчання | 5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2 |
| AT-2 | Навчання з підвищення обізнаності | 7.3, A.7.2.2, A.12.2.1 |
| AT-3 | Рольове навчання | A.7.2.2 |
| AT-4 | Навчальні записи | H/A |
| AT-5 | Вилучено | --- |
| AT-6 | ВІдгуки про проведені навчання | H/A |
| AU-1 | Політика та процедури аудиту та підзвітності | 5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2 |
| AU-2 | Події аудиту | H/A |
| AU-3 | Зміст записів аудиту | A.12.4.1* |
| AU-4 | Місткість сховища записів аудиту | A.12.1.3 |
| AU-5 | Реагування на відмови обробки даних аудиту | H/A |
| AU-6 | Огляд, аналіз і звітність аудиту | A.12.4.1, A.16.1.2, A.16.1.4 |
| AU-7 | Скорочення записів аудиту та формування звіту | H/A |
| AU-8 | Позначка часу | A.12.4.4 |
| AU-9 | Захист інформації аудиту | A.12.4.2, A.12.4.3, A.18.1.3 |
| AU-10 | Неспростовність | H/A |
| AU-11 | Збереження записів аудиту | A.12.4.1, A.16.1.7 |
| AU-12 | Генерація даних аудиту | A.12.4.1, A.12.4.3 |

| Шифр | **Каталог заходів захисту** | **Вимоги ISO/IEC 27001** |
|---|---|---|
| AU-13 | Моніторинг розкриття інформації | Н/А |
| AU-14 | Аудит сесії | A.12.4.1* |
| AU-15 | Вилучено | --- |
| AU-16 | Міжорганізаційний аудит | Н/А |
| CA-1 | Політика та процедури оцінювання, акредитації та моніторингу | 5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2 |
| CA-2 | Оцінювання | A.14.2.8, A.18.2.2, A.18.2.3 |
| CA-3 | Взаємодія систем | A.13.1.2, A.13.2.1, A.13.2.2 |
| CA-4 | Вилучено | --- |
| CA-5 | План усунення недоліків та контрольні показники | 8.3, 9.2, 10.1* |
| CA-6 | Акредитація | 9.3* |
| CA-7 | Безперервний моніторинг | 9.1, 9.2, A.18.2.2, A.18.2.3* |
| CA-8 | Тестування на проникнення | Н/А |
| CA-9 | Внутрішні з’єднання системи | Н/А |
| CM-1 | Політика та процедури управління конфігурацією | 5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2 |
| CM-2 | Базова конфігурація | Н/А |
| CM-3 | Управління змінами конфігурації | 8.1, A.12.1.2, A.14.2.2, A.14.2.3, A.14.2.4 |
| CM-4 | Аналіз впливу на безпеку та приватність | A.14.2.3 |
| CM-5 | Обмеження доступу до змін | A.9.2.3, A.9.4.5, A.12.1.2, A.12.1.4, A.12.5.1 |
| CM-6 | Налаштування конфігурації | Н/А |
| CM-7 | Мінімально необхідна функціональність | A.12.5.1* |
| CM-8 | Інвентаризація компонентів системи | A.8.1.1, A.8.1.2 |
| CM-9 | План управління конфігурацією | A.6.1.1* |
| CM-10 | Обмеження використання програмного забезпечення | A.18.1.2 |
| CM-11 | Встановлене користувачем програмне забезпечення | A.12.5.1, A.12.6.2 |
| CM-12 | Розташування інформації | Н/А |
| CM-13 | Відображення дій даних | Н/А |
| CM-14 | Підписані компоненти | Н/А |
| CP-1 | Політика та процедури планування безперервної роботи | 5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2 |
| CP-2 | План забезпечення безперервної роботи та відновлення функціонування | 7.5.1, 7.5.2, 7.5.3, A.6.1.1, A.17.1.1, A.17.2.1 |
| CP-3 | Навчання із забезпечення безперервної роботи | A.7.2.2* |

| Шифр | **Каталог заходів захисту** | **Вимоги ISO/IEC 27001** |
|---|---|---|
| CP-4 | Тестування плану забезпечення безперервної роботи та відновлення функціонування | A.17.1.3 |
| CP-5 | Вилучено | --- |
| CP-6 | Альтернативне місце зберігання | A.11.1.4, A.17.1.2, A.17.2.1 |
| CP-7 | Альтернативний майданчик роботи | A.11.1.4, A.17.1.2, A.17.2.1 |
| CP-8 | Комунікаційні послуги | A.11.2.2, A.17.1.2 |
| CP-9 | Резервне копіювання | A.12.3.1, A.17.1.2, A.18.1.3 |
| CP-10 | Відновлення та відтворення системи | A.17.1.2 |
| CP-11 | Альтернативні протоколи зв’язку | A.17.1.2* |
| CP-12 | Безпечний режим | H/A |
| CP-13 | Альтернативні механізми безпеки | A.17.1.2* |
| IA-1 | Політика та процедури ідентифікації та автентифікації | 5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2 |
| IA-2 | Ідентифікація та автентифікація (користувачів організації) | A.9.2.1 |
| IA-3 | Ідентифікація та автентифікація пристроїв | H/A |
| IA-4 | Управління ідентифікацією | A.9.2.1 |
| IA-5 | Управління автентифікатором | A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.3 |
| IA-6 | Зворотний зв’язок автентифікатора | A.9.4.2 |
| IA-7 | Автентифікація криптографічного модуля | A.18.1.5 |
| IA-8 | Ідентифікація та автентифікація (неорганізаційні користувачі) | A.9.2.1 |
| IA-9 | Послуги ідентифікації та автентифікації | H/A |
| IA-10 | Адаптивна автентифікація | H/A |
| IA-11 | Повторна автентифікація | H/A |
| IA-12 | Перевірка справжності (ідентичності) | H/A |
| IR-1 | Політика та процедури реагування на інциденти | 5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1 A.18.1.1, A.18.2.2 |
| IR-2 | Навчання з реагування на інциденти | A.7.2.2* |
| IR-3 | Перевірка реагувань на інциденти | H/A |
| IR-4 | Обробка інциденту | A.16.1.4, A.16.1.5, A.16.1.6 |
| IR-5 | Моніторинг інциденту | H/A |
| IR-6 | Звітність про інциденти | A.6.1.3, A.16.1.2 |
| IR-7 | Підтримка реагування на інциденти | H/A |
| IR-8 | План реагування на інцидент | 7.5.1, 7.5.2, 7.5.3, A.16.1.1 |
| IR-9 | Реагування на витік інформації | H/A |
| IR-10 | Вилучено | --- |

| Шифр | **Каталог заходів захисту** | **Вимоги ISO/IEC 27001** |
|---|---|---|
| MA-1 | Політика та процедури технічного обслуговування | 5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2 |
| MA-2 | Контрольоване обслуговування | A.11.2.4*, A.11.2.5* |
| MA-3 | Інструменти для обслуговування | Н/А |
| MA-4 | Віддалене обслуговування | Н/А |
| MA-5 | Технічний персонал | Н/А |
| MA-6 | Своєчасне обслуговування | A.11.2.4 |
| MA-7 | Технічне обслуговування в польових умовах | Н/А |
| MP-1 | Політика та процедури щодо захисту носіїв інформації | 5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2 |
| MP-2 | Доступ до носіїв інформації | A.8.2.3, A.8.3.1, A.11.2.9 |
| MP-3 | Маркування носіїв інформації | A.8.2.2 |
| MP-4 | Зберігання носіїв інформації | A.8.2.3, A.8.3.1, A.11.2.9 |
| MP-5 | Транспортування носіїв інформації | A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.5, A.11.2.6 |
| MP-6 | Знищення інформації на носіях інформації | A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 |
| MP-7 | Використання носіїв інформації | A.8.2.3, A.8.3.1 |
| MP-8 | Зниження категорії безпеки носіїв інформації | Н/А |
| PE-1 | Політика та процедури фізичного захисту та захисту робочого середовища | 5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2 |
| PE-2 | Авторизація фізичного доступу | A.11.1.2* |
| PE-3 | Керування фізичним доступом | A.11.1.1, A.11.1.2, A.11.1.3 |
| PE-4 | Контроль доступу до джерел і ліній електроживлення | A.11.1.2, A.11.2.3 |
| PE-5 | Контроль доступу для пристроїв виведення інформації | A.11.1.2, A.11.2.3 |
| PE-6 | Моніторинг фізичного доступу | Н/А |
| PE-7 | Вилучено | ---- |
| PE-8 | Реєстр доступу відвідувачів | Н/А |
| PE-9 | Енергетичне обладнання та кабелі | A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 |
| PE-10 | Аварійне відключення | A.11.2.2* |
| PE-11 | Аварійне енергозабезпечення | A.11.2.2 |
| PE-12 | Аварійне освітлення | A.11.2.2* |
| PE-13 | Протипожежний захист | A.11.1.4, A.11.2.1 |
| PE-14 | Контроль температури та вологості | A.11.1.4, A.11.2.1, A.11.2.2 |
| PE-15 | Захист від пошкодження водою | A.11.1.4, A.11.2.1, A.11.2.2 |
| PE-16 | Доставлення та видалення | A.8.2.3, A.11.1.6, A.11.2.5 |
| PE-17 | Альтернативне робоче місце | A.6.2.2, A.11.2.6, A.13.2.1 |

| Шифр | Каталог заходів захисту | Вимоги ISO/IEC 27001 |
|---|---|---|
| PE-18 | Розташування компонентів системи | A.8.2.3, A.11.1.4, A.11.2.1 |
| PE-19 | Витік інформації | A.11.1.4, A.11.2.1 |
| PE-20 | Моніторинг і відстеження активів | A.8.2.3* |
| PE-21 | Захист від електромагнітного імпульсу | H/A |
| PE-22 | Маркування компонентів | A.8.2.2 |
| PE-23 | Розташування об’єкта | A.11.1.4, A.11.2.1 |
| PL-1 | Політики та процедури планування безпеки | 5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2 |
| PL-2 | Плани захисту інформації та персональних даних | 7.5.1, 7.5.2, 7.5.3, 10.1, A.14.1.1 |
| PL-3 | Вилучено | --- |
| PL-4 | Правила поведінки | A.7.1.2, A.7.2.1, A.8.1.3 |
| PL-5 | Вилучено | --- |
| PL-6 | Вилучено | --- |
| PL-7 | Концепція експлуатації | 8.1, A.14.1.1 |
| PL-8 | Архітектура безпеки та приватності | A.14.1.1* |
| PL-9 | Централізоване управління | H/A |
| PL-10 | Вибір базового профілю безпеки | H/A |
| PL-11 | Налаштування базового профілю безпеки | H/A |
| PM-1 | Програма (концепція) інформаційної безпеки | 4.1, 4.2, 4.3, 4.4, 5.2, 5.3, 6.1.1, 6.2, 7.4, 7.5.1, 7.5.2, 7.5.3, 8.1, 9.3, 10.2, A.5.1.1, A.5.1.2, A.6.1.1, A.18.1.1, A.18.2.2 |
| PM-2 | Ролі програми інформаційної безпеки | 5.1, 5.3, A.6.1.1 |
| PM-3 | Ресурси забезпечення інформаційної безпеки та приватності | 5.1, 6.2, 7.1 |
| PM-4 | План дій та етапи | 6.1.1, 6.2, 7.4, 7.5.1, 7.5.2, 7.5.3, 8.3, 9.2, 9.3, 10.1 |
| PM-5 | Інвентаризація системи | H/A |
| PM-6 | Показники продуктивності | 5.3, 6.1.1, 6.2, 9.1 |
| PM-7 | Архітектура підприємства | H/A |
| PM-8 | План захисту критичної інфраструктури | H/A |
| PM-9 | Стратегія управління ризиками | 4.3, 4.4, 6.1.1, 6.1.2, 6.2, 7.5.1, 7.5.2, 7.5.3, 9.3, 10.2 |
| PM-10 | Процес акредитації | 9.3, A.6.1.1* |
| PM-11 | Визначення завдань і процесів | 4.1 |
| PM-12 | Програма інсайдерської загрози | H/A |
| PM-13 | Безпека та приватність працівників | 7.2, A.7.2.2* |
| PM-14 | Тестування, навчання та моніторинг | 6.2* |
| PM-15 | Контакти з групами й асоціаціями | 7.4, A.6.1.4 |
| PM-16 | Програма інформування про загрози | H/A |

| Шифр | **Каталог заходів захисту** | **Вимоги ISO/IEC 27001** |
|---|---|---|
| PM-17 | Захист публічної інформації на зовнішніх системах | Н/А |
| PM-18 | Програма (концепція) забезпечення приватності | Н/А |
| PM-19 | Ролі програми приватності | Н/А |
| PM-20 | Поширення інформації про програму забезпечення приватності | Н/А |
| PM-21 | Облік розкриття персональних даних | Н/А |
| PM-22 | Управління якістю персональних даних | Н/А |
| PM-23 | Комісія з управління даними | Н/А |
| PM-24 | Комісія з питань цілісності даних | Н/А |
| PM-25 | Мінімізація персональних даних, що використовуються під час тестування, навчання та досліджень | Н/А |
| PM-26 | Система управління скаргами | Н/А |
| PM-27 | Звітність з питань забезпечення приватності | Н/А |
| PM-28 | Оцінка ризиків | 4.3, 6.1.2, 6.2, 7.4, 7.5.1, 7.5.2, 7.5.3 |
| PM-29 | Ролі керівників програми управління ризиками | 5.1, 5.3, 9.2, A.6.1.1 |
| PM-30 | План управління ризиком ланцюга постачання | 4.4, 6.2, 7.5.1, 7.5.2, 7.5.3, 10.2* |
| PM-31 | План безперервного моніторингу | 4.4, 6.2, 7.5.1, 7.5.2, 7.5.3, 9.1, 10.1, 10.2 |
| PM-32 | Призначення | Н/А |
| PS-1 | Політика та процедури кадрової безпеки | 5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2 |
| PS-2 | Визначення посадового ризику | Н/А |
| PS-3 | Перевірка персоналу | A.7.1.1 |
| PS-4 | Звільнення персоналу | A.7.3.1, A.8.1.4 |
| PS-5 | Переведення персоналу | A.7.3.1, A.8.1.4 |
| PS-6 | Угоди про доступ | A.7.1.2, A.7.2.1, A.13.2.4 |
| PS-7 | Безпека зовнішнього персоналу | A.6.1.1, A.7.2.1* |
| PS-8 | Кадрові санкції | 7.3, A.7.2.3 |
| PS-9 | Опис позицій | A.6.1.1 |
| PT-1 | Політика та процедури обробки персональних даних | Н/А |
| PT-2 | Повноваження на обробку персональних даних | Н/А |
| PT-3 | Цілі обробки персональних даних | Н/А |
| PT-4 | Згода на обробку персональних даних | Н/А |
| PT-5 | Повідомлення про конфіденційність | Н/А |
| PT-6 | Система записів повідомлень про конфіденційність | Н/А |

| Шифр | **Каталог заходів захисту** | **Вимоги ISO/IEC 27001** |
|---|---|---|
| PT-7 | Спеціальні категорії персональних даних | Н/А |
| PT-8 | Вимоги до відповідності | Н/А |
| RA-1 | Політика та процедури оцінювання ризику | 5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2 |
| RA-2 | Категоріювання безпеки | A.8.2.1 |
| RA-3 | Оцінювання ризику | 6.1.2, 8.2, A.12.6.1* |
| RA-4 | Вилучено | --- |
| RA-5 | Сканування вразливостей | A.12.6.1* |
| RA-6 | Заходи протидії технічній розвідці | Н/А |
| RA-7 | Реагування на ризик | 6.1.3, 8.3, 10.1 |
| RA-8 | Оцінка впливу на приватність | Н/А |
| RA-9 | Аналіз критичності | A.15.2.2* |
| RA-10 | Активний пошук загроз | Н/А |
| SA-1 | Політика та процедури придбання системи та послуг | 5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, 8.1, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2 |
| SA-2 | Розподіл ресурсів | Н/А |
| SA-3 | Життєвий цикл розробки системи | A.6.1.1, A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.6 |
| SA-4 | Процес закупівель | 8.1, A.14.1.1, A.14.2.7, A.14.2.9, A.15.1.2 |
| SA-5 | Системна документація | 7.5.1, 7.5.2, 7.5.3, A.12.1.1* |
| SA-6 | Вилучено | --- |
| SA-7 | Вилучено | --- |
| SA-8 | Безпека та приватність принципів інжинірингу (проєктування) | A.14.2.5 |
| SA-9 | Зовнішні послуги для системи | A.6.1.1, A.6.1.5, A.7.2.1, A.13.1.2, A.13.2.2, A.15.2.1, A.15.2.2 |
| SA-10 | Управління конфігурацією розробника | A.12.1.2, A.14.2.2, A.14.2.4, A.14.2.7 |
| SA-11 | Тестування та оцінювання розробника | A.14.2.7, A.14.2.8 |
| SA-12 | Вилучено | --- |
| SA-13 | Вилучено | --- |
| SA-14 | Вилучено | --- |
| SA-15 | Процеси, стандарти й інструменти розробки | A.6.1.5, A.14.2.1 |
| SA-16 | Навчання, що надається розробниками | Н/А |
| SA-17 | Проєкт і архітектура безпеки розробника | A.14.2.1, A.14.2.5 |
| SA-18 | Вилучено | --- |
| SA-19 | Вилучено | --- |
| SA-20 | Індивідуальна розробка критичних компонентів | Н/А |
| SA-21 | Перевірка розробника | A.7.1.1 |

| Шифр | **Каталог заходів захисту** | **Вимоги ISO/IEC 27001** |
|---|---|---|
| SA-22 | Компоненти системи, що не підтримуються | Н/А |
| SA-23 | Спеціалізація | Н/А |
| SC-1 | Політика та процедури захисту системи та комунікацій | 5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.18.1.1, A.18.2.2 |
| SC-2 | Розділення додатків | Н/А |
| SC-3 | Ізоляція функцій безпеки | Н/А |
| SC-4 | Інформація в загальних ресурсах системи | Н/А |
| SC-5 | Захист від атак «Відмова в обслуговуванні» | Н/А |
| SC-6 | Доступність ресурсів | Н/А |
| SC-7 | Захист периметра | A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.3 |
| SC-8 | Конфіденційність та цілісність передачі | A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 |
| SC-9 | Вилучено | --- |
| SC-10 | Відключення мережі | A.13.1.1 |
| SC-11 | Довірений канал зв’язку | Н/А |
| SC-12 | Встановлення та управління криптографічними ключами | A.10.1.2 |
| SC-13 | Криптографічний захист | A.10.1.1, A.14.1.2, A.14.1.3, A.18.1.5 |
| SC-14 | Вилучено | --- |
| SC-15 | Спільні обчислювальні пристрої та застосунки | A.13.2.1* |
| SC-16 | Передача атрибутів безпеки та приватності | Н/А |
| SC-17 | Сертифікати інфраструктури відкритих ключів | A.10.1.2 |
| SC-18 | Мобільний код | Н/А |
| SC-19 | Інтернет-протокол голосового зв’язку | Н/А |
| SC-20 | Безпечний сервіс регулювання імені/адреси (уповноважене джерело) | Н/А |
| SC-21 | Безпечний сервіс регулювання імені/адреси (рекурсивний або кешувальний перетворювач) | Н/А |
| SC-22 | Архітектура та забезпечення служби імен/адрес | Н/А |
| SC-23 | Автентифікація сесії | Н/А |
| SC-24 | Уведення у відомий стан | Н/А |
| SC-25 | Тонкі вузли | Н/А |
| SC-26 | Приманка для зловмисників (honeypots) | Н/А |
| SC-27 | Незалежні від платформи застосунки | Н/А |
| SC-28 | Захист інформації в стані спокою | A.8.2.3* |
| SC-29 | Гетерогенність | Н/А |
| SC-30 | Маскування та хибний напрям | Н/А |

| Шифр | **Каталог заходів захисту** | **Вимоги ISO/IEC 27001** |
|---|---|---|
| SC-31 | Аналіз прихованого каналу | Н/А |
| SC-32 | Поділ системи на частини | Н/А |
| SC-33 | Вилучено | --- |
| SC-34 | Незмінювані виконавчі програми | Н/А |
| SC-35 | Розпізнавання приманок для зловмисників (honeyclient) | Н/А |
| SC-36 | Розподілена обробка та зберігання | Н/А |
| SC-37 | Позасмугові канали | Н/А |
| SC-38 | Безпека операцій | А.12.х |
| SC-39 | Ізоляція процесу | Н/А |
| SC-40 | Захист бездротового з'єднання | Н/А |
| SC-41 | Доступ до портів і пристроїв введення/виведення | Н/А |
| SC-42 | Можливості датчика та дані | А.11.1.5* |
| SC-43 | Обмеження використання | Н/А |
| SC-44 | Екрановані камери | Н/А |
| SC-45 | Синхронізація системи з часом | Н/А |
| SC-46 | Забезпечення виконання між доменної політики | Н/А |
| SC-47 | Альтернативний шлях зв'язку | Н/А |
| SC-48 | Переміщення датчика | Н/А |
| SC-49 | Примусове апаратне розділення та політика забезпечення виконання | Н/А |
| SC-50 | Примусове програмне розділення та політика забезпечення виконання | Н/А |
| SC-51 | Апаратний захист | Н/А |
| SI-1 | Політика та процедури цілісності інформації | 5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, А.5.1.1, А.5.1.2, А.6.1.1, А.12.1.1, А.18.1.1, А.18.2.2 |
| SI-2 | Виправлення дефектів | А.12.6.1, А.14.2.2, А.14.2.3, А.16.1.3 |
| SI-3 | Захист від шкідливого коду | А.12.2.1 |
| SI-4 | Моніторинг системи | Н/А |
| SI-5 | Попередження, рекомендації та директиви з безпеки | А.6.1.4* |
| SI-6 | Перевірка функцій безпеки та приватності | Н/А |
| SI-7 | Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації | Н/А |
| SI-8 | Захист від спаму | Н/А |
| SI-9 | Вилучено | --- |
| SI-10 | Перевірка вводу інформації | Н/А |
| SI-11 | Обробка помилок | Н/А |

| Шифр | **Каталог заходів захисту** | **Вимоги ISO/IEC 27001** |
|---|---|---|
| SI-12 | Управління та збереження інформації | Н/А |
| SI-13 | Передбачуване запобігання збоям | Н/А |
| SI-14 | Нестійкість | Н/А |
| SI-15 | Фільтрація вихідних даних | Н/А |
| SI-16 | Захист пам’яті | Н/А |
| SI-17 | Відмовостійкі процедури | Н/А |
| SI-18 | Операції забезпечення якості даних | Н/А |
| SI-19 | Деідентифікація | Н/А |
| SI-20 | Псування | Н/А |
| SI-21 | Оновлення інформації | Н/А |
| SI-22 | Різновиди інформації | Н/А |
| SI-23 | Фрагментація інформації | Н/А |
| SR-1 | Політика та процедури управління ризиками ланцюга постачання | 5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.12.1.1, A.15.1.1, A.18.1.1, A.18.2.2 |
| SR-2 | План управління ризиками ланцюга постачання | A.14.2.7* |
| SR-3 | Контроль ланцюга постачання і процесів | A.15.1.2, A.15.1.3* |
| SR-4 | Походження | A.14.2.7* |
| SR-5 | Стратегії придбання, інструменти і методи | A.15.1.3 |
| SR-6 | Оцінка постачальників | A.15.2.1 |
| SR-7 | Безпека операцій ланцюга постачання | A.15.2.2* |
| SR-8 | Повідомлення про порушення ланцюга постачання | Н/А |
| SR-9 | Захист від злому і виявлення | Н/А |
| SR-10 | Перевірка системи і компонентів системи | Н/А |
| SR-11 | Автентичність компоненту | Н/А |
| SR-12 | Утилізація компоненту | Н/А |

Таблиця В.2 — Відображення вимог ISO/IEC 27001 на заходи захисту Каталогу заходів захисту

| Заходи ISO/IEC 27001 | Каталог заходів захисту |
|---|---|
| **Вимоги ISO/IEC 27001** | |
| **4. Контекст організації** | |
| 4.1 Розуміння організації та її контексту | PM-1, PM-11 |
| 4.2 Розуміння потреб і очікувань зацікавлених сторін | PM-1 |
| 4.3 Визначення сфери застосування системи управління інформаційною безпекою | PM-1, PM-9, PM-28 |
| 4.4 Система управління інформаційною безпекою | PM-1, PM-9, PM-30, PM-31 |
| **5. Лідерство** | |
| 5.1 Лідерство та відданість справі | PM-2, PM-3, PM-29 |
| 5.2 Політика | Всі XX-1 заходи |
| 5.3 Організаційні ролі, обов'язки та повноваження | Всі XX-1 заходи, PM-2, PM-6, PM-29 |
| **6. Планування** | |
| **6.1 Дії щодо ризиків і можливостей** | |
| 6.1.1 Загальні положення | PM-1, PM-4, PM-6, PM-9 |
| 6.1.2 Оцінка ризиків інформаційної безпеки | PM-9, PM-28, RA-3 |
| 6.1.3 Обробка ризиків інформаційної безпеки | RA-7 |
| 6.2 Цілі та планування інформаційної безпеки | PM-1, PM-3, PM-4, PM-6, PM-9, PM-14, PM-28, PM-30, PM-31 |
| **7. Підтримка** | |
| 7.1 Ресурси | PM-3 |
| 7.2 Компетентність | PM-13 |
| 7.3 Обізнаність | AT-2, PS-8 |
| 7.4 Спілкування | PM-1, PM-15, PM-28, PM-31 |
| **7.5 Документована інформація** | |
| 7.5.1 Загальні положення | Всі XX-1 заходи, CP-2, IR-8, PL-2, PM-4, PM-9, PM-28, PM-30, PM-31, SA-5 |
| 7.5.2 Створення та оновлення | Всі XX-1 заходи, CP-2, IR-8, PL-2, PM-4, PM-9, PM-28, PM-30, PM-31, SA-5 |
| 7.5.3 Контроль документованої інформації | Всі XX-1 заходи, CP-2, IR-8, PL-2, PM-4, PM-9, PM-28, PM-30, PM-31, SA-5 |
| **8. Операція** | |
| 8.1 Планування та контроль роботи | CM-3, PL-7, PM-1, SA-1, SA-4 |
| 8.2 Оцінка ризиків інформаційної безпеки | RA-3 |
| 8.3 Обробка ризиків інформаційної безпеки | CA-5, PM-4, RA-7 |
| **9. Оцінка роботи** | |
| 9.1 Моніторинг, вимірювання, аналіз та оцінка | CA-1, CA-7, PM-6, PM-31 |
| 9.2 Внутрішній аудит | CA-1, CA-2, CA-5, CA-7, PM-4 |
| 9.3 Аналіз керівництва | CA-6, PM-1, PM-4, PM-9, PM-10, PM-29 |
| **10. Удосконалення** | |
| 10.1 Невідповідність і коригувальні дії | CA-5, PL-2, PM-4, PM-31, RA-7 |
| 10.2 Постійне вдосконалення | PM-1, PM-9, PM-30, PM-31 |

| Засоби керування ISO/IEC 27001 | |
|---|---|
| **A.5 Політика інформаційної безпеки** | |
| **A.5.1 Настанови в частині інформаційної безпеки** | |
| A.5.1.1 Політики інформаційної безпеки | Всі XX-1 заходи |
| A.5.1.2 Перегляд політик інформаційної безпеки | Всі XX-1 заходи |
| **A.6 Організація діяльності з інформаційної безпеки** | |
| **A.6.1 Внутрішня організація діяльності щодо забезпечення інформаційної безпеки** | |
| A.6.1.1 Ролі та обов'язки щодо забезпечення інформаційної безпеки | Всі XX-1 заходи, CM-9, CP-2, PS-7, SA-3, SA-9, PM-2, PM-10 |
| A.6.1.2 Розподіл обов'язків | AC-5 |
| A.6.1.3 Контакт з владою | IR-6 |
| A.6.1.4 Взаємодія із зацікавленими професійними групами | SI-5, PM-15 |
| A.6.1.5 Інформаційна безпека в управлінні проєктами | SA-3, SA-9, SA-15 |
| **A.6.2 Мобільні пристрої та дистанційна робота** | |
| A.6.2.1 Політика, що стосується мобільних пристроїв | AC-17, AC-18, AC-19 |
| A.6.2.2 Дистанційна робота | AC-3, AC-17, PE-17 |
| **A.7 Безпека, пов'язана з персоналом** | |
| **A.7.1 При прийманні на роботу** | |
| A.7.1.1 Перевірка | PS-3, SA-21 |
| A.7.1.2 Правила та умови роботи | PL-4, PS-6 |
| **A.7.2 Під час роботи** | |
| A.7.2.1 Обов'язки керівництва організації | PL-4, PS-6, PS-7, SA-9 |
| A.7.2.2 Поінформованість, навчання і практична підготовка (тренінги) в області інформаційної безпеки | AT-2, AT-3, CP-3, IR-2, PM-13 |
| A.7.2.3 Дисциплінарний процес | PS-8 |
| **A.7.3 Звільнення і зміна місця роботи** | |
| A.7.3.1 Припинення трудових відносин або зміна трудових обов'язків | PS-4, PS-5 |
| **A.8 Менеджмент активів** | |
| **A.8.1 Відповідальність за активи** | |
| A.8.1.1 Інвентаризація активів | CM-8 |
| A.8.1.2 Володіння активами | CM-8 |
| A.8.1.3 Допустиме використання активів | PL-4 |
| A.8.1.4 Повернення активів | PS-4, PS-5 |
| **A.8.2 Категоріювання інформації** | |
| A.8.2.1 Категоріювання інформації | RA-2 |

| | |
|---|---|
| A.8.2.2 Маркування інформації | MP-3, PE-22 |
| A.8.2.3 Звернення з активами | MP-2, MP-4, MP-5, MP-6, MP-7, PE-16, PE-18, PE-20, SC-8, SC-28 |
| **A.8.3 Поводження з носіями інформації** | |
| A.8.3.1 Управління змінними носіями інформації | MP-2, MP-4, MP-5, MP-6, MP-7 |
| A.8.3.2 Утилізація носіїв інформації | MP-6 |
| A.8.3.3 Переміщення фізичних носіїв | MP-5 |
| **A.9 Управління доступом** | |
| **A.9.1 Вимоги бізнесу з управління доступом** | |
| A.9.1.1 Політика управління доступом | AC-1 |
| A.9.1.2 Доступ до мереж і мережевих сервісів | AC-3, AC-6 |
| **A.9.2 Управління доступом користувачів** | |
| A.9.2.1 Реєстрація та скасування реєстрації користувачів | AC-2, IA-2, IA-4, IA-5, IA-8 |
| A.9.2.2 Надання користувачеві права доступу | AC-2 |
| A.9.2.3 Управління привілейованими правами доступу | AC-2, AC-3, AC-6, CM-5 |
| A.9.2.4 Процес управління секретною автентифікаційною інформацією користувачів | IA-5 |
| A.9.2.5 Перегляд прав доступу користувачів | AC-2 |
| A.9.2.6 Анулювання або коригування прав доступу | AC-2 |
| **A.9.3 Відповідальність користувачів** | |
| A.9.3.1 Використання секретної автентифікаційної інформації | IA-5 |
| **A.9.4 Управління доступом до систем і застосунків** | |
| A.9.4.1 Обмеження доступу до інформації | AC-3, AC-24 |
| A.9.4.2 Безпечні процедури входу в систему | AC-7, AC-8, AC-9, IA-6 |
| A.9.4.3 Система управління паролями | IA-5 |
| A.9.4.4 Використання привілейованих службових програм | AC-3, AC-6 |
| A.9.4.5 Управління доступом до початкового тексту програми | AC-3, AC-6, CM-5 |
| **A.10 Криптографія** | |
| **A.10.1 Криптографічний захист інформації** | |
| A.10.1.1 Політика використання криптографічних заходів і засобів захисту інформації | SC-13 |
| A.10.1.2 Управління ключами | SC-12, SC-17 |
| **A.11 Фізична безпека та захист від впливу навколишнього середовища** | |
| **A.11.1 Зони безпеки** | |
| A.11.1.1 Фізичний периметр безпеки | PE-3* |

| | |
|---|---|
| A.11.1.2 Заходи та засоби контролю й управління фізичним доступом | PE-2, PE-3, PE-4, PE-5 |
| A.11.1.3 Безпека будівель, приміщень і обладнання | PE-3, PE-5 |
| A.11.1.4 Захист від зовнішніх загроз і загроз з боку навколишнього середовища | CP-6, CP-7, PE-9, PE-13, PE-14, PE-15, PE-18, PE-19, PE-23 |
| A.11.1.5 Робота в зонах безпеки | AC-19(4), SC-42* |
| A.11.1.6 Зони навантаження і розвантаження | PE-16 |
| **A.11.2. Обладнання** | |
| A.11.2.1 Розміщення і захист обладнання | PE-9, PE-13, PE-14, PE-15, PE-18, PE-19, PE-23 |
| A.11.2.2 Допоміжні послуги | CP-8, PE-9, PE-10, PE-11, PE-12, PE-14, PE-15 |
| A.11.2.3 Безпека кабельної мережі | PE-4, PE-9 |
| A.11.2.4 Технічне обслуговування обладнання | MA-2, MA-6 |
| A.11.2.5 Переміщення активів | MA-2, MP-5, PE-16 |
| A.11.2.6 Безпека обладнання та активів поза приміщеннями організації | AC-19, AC-20, MP-5, PE-17 |
| A.11.2.7 Безпечна утилізація або повторне використання обладнання | MP-6 |
| A.11.2.8 Обладнання, залишене користувачем без нагляду | AC-11 |
| A.11.2.9 Політика «чистого стола» та «чистого екрана» | AC-11, MP-2, MP-4 |
| **A.12 Безпека при експлуатації** | |
| **A.12.1 Експлуатаційні процедури та обов'язки** | |
| A.12.1.1 Документально оформлені експлуатаційні процедури | Всі XX-1 заходи, SA-5 |
| A.12.1.2 Процес управління змінами | CM-3, CM-5, SA-10 |
| A.12.1.3 Управління продуктивністю | AU-4, CP-2(2), SC-5(2) |
| A.12.1.4 Поділ середовищ розробки, тестування та експлуатації | CM-4(1)*, CM-5* |
| **A.12.2 Захист від шкідливих програм** | |
| A.12.2.1 Заходи й засоби інформаційної безпеки щодо шкідливих програм | AT-2, SI-3 |
| **A.12.3 Резервне копіювання** | |
| A.12.3.1 Резервне копіювання інформації | CP-9 |
| **A.12.4 Реєстрація та моніторинг** | |
| A.12.4.1 Реєстрація подій | AU-3, AU-6, AU-11, AU-12, AU-14 |
| A.12.4.2 Захист інформації реєстраційних журналів | AU-9 |
| A.12.4.3 Реєстраційні журнали дій адміністратора та оператора | AU-9, AU-12 |
| A.12.4.4 Синхронізація годин | AU-8 |

| | |
|---|---|
| **A.12.5 Контроль програмного забезпечення, що перебуває в експлуатації** | |
| A.12.5.1 Установка програмного забезпечення в експлуатованих системах | CM-5, CM-7(4), CM-7(5), CM-11 |
| **A.12.6 Менеджмент технічних уразливостей** | |
| A.12.6.1 Процес управління технічними вразливостями | RA-3, RA-5, SI-2, SI-5 |
| A.12.6.2 Обмеження на установку програмного забезпечення | CM-11 |
| **A.12.7 Особливості аудиту інформаційних систем** | |
| A.12.7.1 Заходи й засоби інформаційної безпеки щодо аудиту інформаційних систем | AU-5* |
| **A.13 Безпека системи зв'язку** | |
| **A.13.1 Менеджмент безпеки мереж** | |
| A.13.1.1 Заходи й засоби інформаційної безпеки для мереж | AC-3, AC-17, AC-18, AC-20, SC-7, SC-8, SC-10 |
| A.13.1.2 Безпека мережевих сервісів | CA-3, SA-9 |
| A.13.1.3 Поділ у мережах | AC-4, SC-7 |
| **A.13.2 Передача інформації** | |
| A.13.2.1 Політики та процедури передачі інформації | AC-4, AC-17, AC-18, AC-19, AC-20, CA-3, PE-17, SC-7, SC-8, SC-15 |
| A.13.2.2 Угоди про передачу інформації | AC-21, CA-3, PA-4, PS-6, SA-9 |
| A.13.2.3 Електронний обмін повідомленнями | SC-8 |
| A.13.2.4 Угоди про конфіденційність або нерозголошення | PS-6 |
| **A.14 Придбання, розробка та підтримка систем** | |
| **A.14.1 Вимоги до безпеки інформаційних систем** | |
| A.14.1.1 Аналіз і специфікація вимог інформаційної безпеки | PL-2, PL-7, PL-8, SA-3, SA-4 |
| A.14.1.2 Забезпечення безпеки прикладних сервісів, що надаються з використанням мереж загального користування | AC-3, AC-4, AC-17, SC-8, SC-13 |
| A.14.1.3 Захист транзакцій прикладних сервісів | AC-3, AC-4, SC-7, SC-8, SC-13 |
| **A.14.2 Безпека в процесах розробки та підтримки** | |
| A.14.2.1 Політика безпечної розробки | SA-3, SA-15, SA-17 |
| A.14.2.2 Процедури управління змінами системи | CM-3, SA-10, SI-2 |
| A.14.2.3 Технічна експертиза застосунків (прикладних програм) після змін операційної платформи | CM-3, CM-4, SI-2 |
| A.14.2.4 Обмеження на зміни пакетів програм | CM-3, SA-10 |
| A.14.2.5 Принципи безпечного проєктування систем | SA-8 |
| A.14.2.6 Безпечне середовище розробки | SA-3* |

| | |
|---|---|
| A.14.2.7 Розробка з використанням аутсорсингу | SA-4, SA-10, SA-11, SA-15, SR-2, SR-4 |
| A.14.2.8 Тестування безпеки систем | CA-2, SA-11 |
| A.14.2.9 Приймально-здавальні випробування системи | SA-4, SR-5(2) |
| **A.14.3 Тестові дані** | |
| A.14.3.1 Захист тестових даних | SA-15(9)* |
| **A.15 Взаємовідносини з постачальниками** | |
| **A.15.1 Інформаційна безпека у взаєминах з постачальниками** | |
| A.15.1.1 Політика інформаційної безпеки у взаєминах з постачальниками | SR-1 |
| A.15.1.2 Розгляд питань безпеки в угодах з постачальниками | SA-4, SR-3 |
| A.15.1.3 Ланцюжок постачань інформаційно-комунікаційної технології | SR-3, SR-5 |
| **A.15.2 Управління послугами, наданими постачальником** | |
| A.15.2.1 Моніторинг і аналіз послуг постачальника | SA-9, SR-6 |
| A.15.2.2 Управління змінами послуг постачальника | RA-9, SA-9, SR-7 |
| **A.16 Менеджмент інцидентів інформаційної безпеки** | |
| **A.16.1 Менеджмент інцидентів інформаційної безпеки поліпшень** | |
| A.16.1.1 Обов’язки та процедури | IR-8 |
| A.16.1.2 Повідомлення про події інформаційної безпеки | AU-6, IR-6 |
| A.16.1.3 Повідомлення про недоліки інформаційної безпеки | SI-2 |
| A.16.1.4 Оцінювання й ухвалення рішень щодо подій інформаційної безпеки | AU-6, IR-4 |
| A.16.1.5 Реагування на інциденти інформаційної безпеки | IR-4 |
| A.16.1.6 Аналіз інцидентів інформаційної безпеки | IR-4 |
| A.16.1.7 Збір свідчень | AU-4, AU-9, AU-10(3), AU-11* |
| **A.17 Аспекти інформаційної безпеки в рамках менеджменту безперервності бізнесу** | |
| **A.17.1 Безперервність інформаційної безпеки** | |
| A.17.1.1 Планування безперервності інформаційної безпеки | CP-2 |
| A.17.1.2 Реалізація безперервності інформаційної безпеки | CP-6, CP-7, CP-8, CP-9, CP-10, CP-11, CP-13 |
| A.17.1.3 Перевірка, аналіз і оцінювання безперервності інформаційної безпеки | CP-4 |

| | |
|---|---|
| **A.17.2 Резервування обладнання** | |
| A.17.2.1 Доступність засобів обробки інформації | CP-2, CP-6, CP-7 |
| **A.18 Відповідність** | |
| **A.18.1 Відповідність правовим і договірним вимогам** | |
| A.18.1.1 Ідентифікація законодавчих і договірних вимог | Всі XX-1 заходи |
| A.18.1.2 Права на інтелектуальну власність | CM-10 |
| A.18.1.3 Захист записів | AC-3, AC-23, AU-9, AU-10, CP-9, SC-8, SC-8(1), SC-13, SC-28, SC-28(1) |
| A.18.1.4 Приватність і захист персональних даних | Appendix J Privacy controls |
| A.18.1.5 Регулювання криптографічних заходів і засобів захисту інформації | IA-7, SC-12, SC-13, SC-17 |
| **A.18.2 Перевірки інформаційної безпеки** | |
| A.18.2.1 Незалежна перевірка інформаційної безпеки | CA-2(1), SA-11(3) |
| A.18.2.2 Відповідність політикам і стандартам безпеки | Всі XX-1 заходи, CA-2 |
| A.18.2.3 Аналіз технічної відповідності | CA-2 |

Таблиця В3 — Відображення вимог ISO/IEC 15408 на заходи захисту НД ТЗІ Порядок вибору заходів захисту інформації та персональних даних для інформаційних систем (Каталог заходів захисту)

| **Вимоги ISO/IEC 15408** | | **Каталог заходів захисту** | |
|---|---|---|---|
| **Функціональні вимоги безпеки** | | | |
| FAU_ARP.1 | Автоматична реакція аудиту безпеки. Сигналізація безпеки | AU-5 | Реагування на відмови обробки даних аудиту |
| | | AU-5(1) | Реагування на відмови обробки даних аудиту — Місткість сховища записів аудиту |
| | | AU-5(2) | Реагування на відмови обробки даних аудиту — Тривожне сповіщення в реальному часі |
| | | AU-5(3) | Реагування на відмови обробки даних аудиту — Налаштування порогового обсягу трафіку |
| | | AU-5(4) | Реагування на відмови обробки даних аудиту — Вимкнення в разі відмови |
| | | PE-6(2) | Моніторинг фізичного доступу — Автоматичні розпізнавання вторгнень і відповідна реакція |
| | | SI-3 | Захист від шкідливого коду |
| | | SI-3(8) | Захист від шкідливого коду — Виявлення неавторизованих команд |
| | | SI-4(5) | Моніторинг системи — Системні сповіщення |
| | | SI-4(7) | Моніторинг системи — Автоматичне реагування на підозрілі події |
| | | SI-4(22) | Моніторинг системи — Несанкціоновані послуги мережі |
| | | SI-7(2) | Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації — Автоматичні сповіщення про порушення цілісності |
| | | SI-7(5) | Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації — Автоматичні відповіді про порушення цілісності |
| | | SI-7(8) | Цілісність програмного забезпечення, вбудованого програмного забезпечення та |

| Вимоги ISO/IEC 15408 | | Каталог заходів захисту | |
|---|---|---|---|
| | | | інформації — Аудит важливих подій |
| FAU_GEN.1 | Генерація даних аудиту безпеки.<br>Генерація даних аудиту | AU-2 | Події аудиту |
| | | AU-3 | Зміст записів аудиту |
| | | AU-3(1) | Зміст записів аудиту — Додаткова інформація про аудит |
| | | AU-12 | Генерація даних аудиту |
| FAU_GEN.2 | Генерація даних аудиту безпеки.<br>Асоціація ідентифікації користувачів | AU-3 | Зміст записів аудиту |
| FAU_SAA.1 | Аналіз аудиту безпеки.<br>Аналіз потенційних порушень. | SI-4 | Моніторинг системи |
| FAU_SAA.2 | Аналіз аудиту безпеки.<br>Виявлення аномалій на основі профілю | AC-2(12) | Управління обліковими записами — Моніторинг нетипового використання облікових записів |
| | | SI-4 | Моніторинг системи |
| FAU_SAA.3 | Аналіз аудиту безпеки.<br>Проста атака евристики | SI-3 | Захист від шкідливого коду |
| | | SI-4 | Моніторинг системи |
| FAU_SAA.4 | Аналіз аудиту безпеки.<br>Комплексна атака евристики | SI-3 | Захист від шкідливого коду |
| | | SI-4 | Моніторинг системи |
| FAU_SAR.1 | Аудит безпеки.<br>Огляд аудиту | AU-7 | Скорочення записів аудиту та формування звіту |
| FAU_SAR.2 | Аудит безпеки.<br>Обмежений огляд аудиту | AU-9(6) | Захист інформації аудиту — Доступ тільки для читання |
| FAU_SAR.3 | Аудит безпеки.<br>Вибірковий огляд аудиту | AU-7 | Скорочення записів аудиту та формування звіту |
| | | AU-7(1) | Скорочення записів аудиту та формування звіту — Автоматична обробка |
| | | AU-7(2) | Скорочення записів аудиту та формування звіту — Автоматичне сортування та пошук |
| FAU_SEL.1 | Вибір подій аудиту безпеки<br>Вибірковий аудит | AU-12 | Генерація даних аудиту |
| FAU_STG.1 | Сховище подій аудиту безпеки<br>Захищене сховище даних аудиту | AU-9 | Захист інформації аудиту |
| FAU_STG.2 | Сховище подій аудиту безпеки | AU-9 | Захист інформації аудиту |

| Вимоги ISO/IEC 15408 | | Каталог заходів захисту | |
|---|---|---|---|
| | Гарантії доступності даних аудиту | | |
| FAU_STG.3 | Сховище подій аудиту безпеки<br>Дія в разі можливої втрати даних аудиту | AU-5 | Реагування на відмови обробки даних аудиту |
| | | AU-5(1) | Реагування на відмови обробки даних аудиту — Місткість сховища записів аудиту |
| | | AU-5(2) | Реагування на відмови обробки даних аудиту — Тривожне сповіщення в реальному часі |
| | | AU-5(4) | Реагування на відмови обробки даних аудиту — Вимкнення в разі відмови |
| FAU_STG.4 | Сховище подій аудиту безпеки<br>Запобігання втрати даних аудиту | AU-4 | Місткість сховища записів аудиту |
| | | AU-5 | Реагування на відмови обробки даних аудиту |
| | | AU-5(2) | Реагування на відмови обробки даних аудиту — Тривожне сповіщення в реальному часі |
| | | AU-5(4) | Реагування на відмови обробки даних аудиту — Вимкнення в разі відмови |
| FCO_NRO.1 | Безвідмовність походження<br>Вибірковий доказ походження | AU-10 | Неспростовність |
| | | AU-10(1) | Неспростовність — Асоціація ідентичності |
| | | AU-10(2) | Неспростовність — Ратифікація прив’язки інформації про ідентичність виробника |
| FCO_NRO.2 | Безвідмовність походження<br>Примусовий доказ походження | AU-10 | Неспростовність |
| | | AU-10(1) | Неспростовність — Асоціація ідентичності |
| | | AU-10(2) | Неспростовність — Ратифікація прив’язки інформації про ідентичність виробника |
| FCO_NRR.1 | Безвідмовність отримувача<br>Вибіркове підтвердження отримання | AU-10 | Неспростовність |
| | | AU-10(1) | Неспростовність — Асоціація ідентичності |
| | | AU-10(2) | Неспростовність — Ратифікація прив’язки інформації про ідентичність виробника |
| FCO_NRR.2 | Безвідмовність отримувача<br>Примусове підтвердження отримання | AU-10 | Неспростовність |
| | | AU-10(1) | Неспростовність — Асоціація ідентичності |
| | | AU-10(2) | Неспростовність — Ратифікація прив’язки інформації про ідентичність виробника |
| FCS_CKM.1 | Управління криптографічними ключами | SC-12 | Встановлення та управління криптографічними ключами |

| Вимоги ISO/IEC 15408 | | Каталог заходів захисту | |
|---|---|---|---|
| | Генерація криптографічного ключа | | |
| FCS_CKM.2 | Управління криптографічними ключами Розподіл криптографічних ключів | SC-12 | Встановлення та управління криптографічними ключами |
| FCS_CKM.3 | Управління криптографічними ключами Криптографічний ключ доступу | SC-12 | Встановлення та управління криптографічними ключами |
| FCS_CKM.4 | Управління криптографічними ключами Знищення криптографічного ключа | SC-12 | Встановлення та управління криптографічними ключами |
| FCS_COP.1 | Криптографічна операція | SC-13 | Криптографічний захист |
| FDP_ACC.1 | Політика контролю доступу Контроль доступу до підмножини | AC-3 | Забезпечення доступу |
| | | AC-3(3) | Забезпечення доступу — Мандатне управління доступом |
| | | AC-3(4) | Забезпечення доступу — Дискреційне управління доступом |
| | | AC-3(7) | Забезпечення доступу — Управління доступом на основі ролей |
| FDP_ACC.2 | Політика контролю доступу Повний контроль доступу | AC-3 | Забезпечення доступу |
| | | AC-3(3) | Забезпечення доступу — Мандатне управління доступом |
| | | AC-3(4) | Забезпечення доступу — Дискреційне управління доступом |
| | | AC-3(7) | Забезпечення доступу — Управління доступом на основі ролей |
| FDP_ACF.1 | Безпека функцій контролю доступу Контроль доступу на основі атрибутів | AC-3 | Забезпечення доступу |
| | | AC-3(3) | Забезпечення доступу - Мандатне управління доступом |
| | | AC-3(4) | Забезпечення доступу - Дискреційне управління доступом |
| | | AC-3(7) | Забезпечення доступу — Управління доступом на основі ролей |
| | | AC-16 | Атрибути безпеки та приватності |
| | | SC-16 | Передача атрибутів безпеки та приватності |
| FDP_DAU.1 | Авентифікація даних Автентифікація основних даних | SI-7 | Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації |

| Вимоги ISO/IEC 15408 | | Каталог заходів захисту | |
|---|---|---|---|
| | | SI-7(1) | Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації — Перевірка цілісності |
| | | SI-7(6) | Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації — Криптографічний захист |
| | | SI-7(10) | Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації - Захист завантажувального вбудованого програмного забезпечення |
| FDP_DAU.2 | Автентифікація даних<br>Автентифікація даних з особою гаранта | SI-7 | Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації |
| | | SI-7(1) | Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації — Перевірка цілісності |
| | | SI-7(6) | Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації — Криптографічний захист |
| | | SI-7(10) | Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації - Захист завантажувального вбудованого програмного забезпечення |
| FDP_ETC.1 | Експорт з Об’єкта оцінювання. Експорт даних користувача без атрибутів безпеки | Н\А | |
| FDP_ETC.2 | Експорт з ТОЕ<br>Експорт даних користувачів з атрибутами безпеки | AC-16 | Атрибути безпеки та приватності |
| | | AC-16(5) | Атрибути безпеки та приватності — Відображення атрибутів на пристроях виведення |
| | | SC-16 | Передача атрибутів безпеки та приватності |
| FDP_IFC.1 | | AC-3 | Забезпечення доступу |

| Вимоги ISO/IEC 15408 | | Каталог заходів захисту | |
|---|---|---|---|
| | Політика управління інформаційним потоком<br>Управління потоком інформації про підмножину | AC-3(3) | Забезпечення доступу — Мандатне управління доступом |
| | | AC-4 | Управління інформаційними потоками |
| | | AC-4(1) | Управління інформаційними потоками — Атрибути безпеки об’єкта |
| FDP_IFC.2 | Політика управління інформаційним потоком<br>Повний контроль інформаційного потоку | AC-3 | Забезпечення доступу |
| | | AC-3(3) | Забезпечення доступу — Мандатне управління доступом |
| | | AC-4 | Управління інформаційними потоками |
| FDP_IFF.1 | Функції управління потоком інформації<br>Прості атрибути безпеки | AC-3 | Забезпечення доступу |
| | | AC-3(3) | Забезпечення доступу — Мандатне управління доступом |
| | | AC-4 | Управління інформаційними потоками |
| | | AC-4(1) | Управління інформаційними потоками — Атрибути безпеки об’єкта |
| | | AC-4(2) | Управління інформаційними потоками — Домени обробки даних |
| | | AC-4(7) | Управління інформаційними потоками — Механізми одностороннього потоку |
| | | AC-16 | Атрибути безпеки та приватності |
| | | SC-7 | Захист периметра |
| FDP_IFF.2 | Функції управління потоком інформації<br>Ієрархічні атрибути безпеки | AC-3 | Забезпечення доступу |
| | | AC-3(3) | Забезпечення доступу — Мандатне управління доступом |
| | | AC-4(1) | Управління інформаційними потоками — Атрибути безпеки об’єкта |
| | | AC-16 | Атрибути безпеки та приватності |
| FDP_IFF.3 | Функції управління потоком інформації<br>Обмеження незаконних потоків інформації | SC-31 | Аналіз прихованого каналу |
| | | SC-31(2) | Аналіз прихованого каналу — Максимальна пропускна здатність |
| FDP_IFF.4 | Функції управління потоком інформації<br>Часткове усунення незаконних інформаційних потоків | SC-31 | Аналіз прихованого каналу |
| | | SC-31(2) | Аналіз прихованого каналу — Максимальна пропускна здатність |
| FDP_IFF.5 | Функції управління потоком інформації<br>Немає незаконних потоків інформації | SC-31 | Аналіз прихованого каналу |
| | | SC-31(2) | Аналіз прихованого каналу — Максимальна пропускна здатність |
| FDP_IFF.6 | | SC-31 | Аналіз прихованого каналу |

| Вимоги ISO/IEC 15408 | | Каталог заходів захисту | |
|---|---|---|---|
| | Функції управління потоком інформації Моніторинг незаконного потоку інформації | SI-4(18) | Моніторинг системи - Аналіз трафіку та прихованої ексфільтрації |
| FDP_ITC.1 | Імпорт за межами TOE Імпорт даних користувача без атрибутів безпеки | AC-4(9) | Управління інформаційними потоками — Перевірки, що проводить персонал |
| | | AC-4(12) | Управління інформаційними потоками — Ідентифікатори типу даних |
| FDP_ITC.2 | Імпорт за межами TOE Імпорт даних користувача з атрибутами безпеки | AC-16 | Атрибути безпеки та приватності |
| | | SC-16 | Передача атрибутів безпеки та приватності |
| FDP_ITT.1 | Внутрішня передача TOE Основний захист від внутрішньої передачі | SC-8 | Конфіденційність та цілісність передачі |
| | | SC-8(1) | Конфіденційність та цілісність передачі — Криптографічний захист |
| | | SC-5 | Захист від атак «Відмова в обслуговуванні» |
| FDP_ITT.2 | Внутрішня передача TOE Поділ передачі за ознаками | AC-4(21) | Управління інформаційними потоками — Фізичне та логічне відділення інформаційних потоків |
| | | SC-8 | Конфіденційність та цілісність передачі |
| | | SC-8(1) | Конфіденційність та цілісність передачі - Криптографічний захист |
| | | SC-5 | Захист від атак «Відмова в обслуговуванні» |
| FDP_ITT.3 | Внутрішня передача TOE Моніторинг цілісності | SC-8(1) | Конфіденційність та цілісність передачі - Криптографічний захист |
| | | SI-7 | Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації |
| | | SI-7(1) | Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації — Перевірка цілісності |
| | | SI-7(5) | Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації — Автоматичні відповіді про порушення цілісності |

| Вимоги ISO/IEC 15408 | | Каталог заходів захисту | |
|---|---|---|---|
| FDP_ITT.4 | Внутрішня передача TOE<br>Моніторинг цілісності на основі атрибутів | AC-4(21) | Управління інформаційними потоками — Фізичне та логічне відділення інформаційних потоків |
| | | SC-8(1) | Конфіденційність та цілісність передачі — Криптографічний захист |
| | | SI-7 | Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації |
| | | SI-7(1) | Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації — Перевірка цілісності |
| | | SI-7(5) | Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації — Автоматичні відповіді про порушення цілісності |
| FDP_RIP.1 | Підмножина захисту залишкової інформації<br>Захист залишкової інформації | SC-4 | Інформація в загальних ресурсах системи |
| FDP_RIP.2 | Захист залишкової інформації<br>Повний залишковий захист інформації | SC-4 | Інформація в загальних ресурсах системи |
| FDP_ROL.1 | Відкат<br>Основний відкат | CP-10(2) | Відновлення та відтворення системи — Відновлення транзакцій |
| FDP_ROL.2 | Відкат<br>Розширений відкат | CP-10(2) | Відновлення та відтворення системи — Відновлення транзакцій |
| FDP_SDI.1 | Цілісність даних, що зберігаються<br>Моніторинг цілісності даних, що зберігаються | SI-7 | Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації |
| | | SI-7(1) | Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації — Перевірка цілісності |
| FDP_SDI.2 | Цілісність даних, що зберігаються<br>Моніторинг і дії з цілісності даних | SI-7 | Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації |
| | | SI-7(1) | Цілісність програмного забезпечення, вбудованого |

| Вимоги ISO/IEC 15408 | | Каталог заходів захисту | |
|---|---|---|---|
| | | | програмного забезпечення та інформації — Перевірка цілісності |
| | | SI-7(5) | Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації — Автоматичні відповіді про порушення цілісності |
| FDP_UCT.1 | Захист конфіденційності при передачі даних користувача між TSF<br>Основна конфіденційність обміну даними | SC-8 | Конфіденційність та цілісність передачі |
| | | SC-8(1) | Конфіденційність та цілісність передачі — Криптографічний захист |
| FDP_UIT.1 | Захист цілісності при передачі даних користувача між TSF<br>Цілісність обміну даними | SC-8 | Конфіденційність та цілісність передачі |
| | | SC-8(1) | Конфіденційність та цілісність передачі — Криптографічний захист |
| | | SI-7 | Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації |
| | | SI-7(6) | Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації — Криптографічний захист |
| FDP_UIT.2 | Захист цілісності при передачі даних користувача між TSF<br>Відновлення обміну вихідними даними | Н\А | |
| FDP_UIT.3 | Захист цілісності при передачі даних користувача між TSF<br>Цільове відновлення обміну даними | Н\А | |
| FIA_AFL.1 | Помилка автентифікації<br>Обробка помилок автентифікації | AC-7 | Невдалі спроби входу в систему |
| FIA_ATD.1 | Визначення атрибута користувача<br>Визначення атрибута користувача | AC-2 | Управління обліковими записами |
| | | IA-2 | Ідентифікація та автентифікація (користувачів організації) |
| FIA_SOS.1 | Специфікація таємниць<br>Створення таємниць TSF | IA-5 | Управління автентифікатором |
| | | IA-5(1) | Управління автентифікатором — Автентифікація на основі пароля |

| Вимоги ISO/IEC 15408 | | Каталог заходів захисту | |
|---|---|---|---|
| FIA_SOS.2 | Специфікація таємниць<br>Перевірка темниць | IA-5 | Управління автентифікатором |
| | | IA-5(1) | Управління автентифікатором — Автентифікація на основі пароля |
| FIA_UAU.1 | Автентифікація користувача<br>Час автентифікації | AC-14 | Дозволені дії без ідентифікації або автентифікації |
| | | IA-2 | Ідентифікація та автентифікація (користувачів організації) |
| | | IA-8 | Ідентифікація та автентифікація (неорганізаційні користувачі) |
| FIA_UAU.2 | Автентифікація користувача<br>Автентифікація користувача перед будь-якими діями | AC-14 | Дозволені дії без ідентифікації або автентифікації |
| | | IA-2 | Ідентифікація та автентифікація (користувачів організації) |
| | | IA-8 | Ідентифікація та автентифікація (неорганізаційні користувачі) |
| FIA_UAU.3 | Автентифікація користувача<br>Непідробна автентифікація | IA-2(8) | Ідентифікація та автентифікація (користувачів організації) - Доступ до облікових записів — стійкість до відтворення |
| FIA_UAU.4 | Автентифікація користувача<br>Механізми автентифікації одноразового використання | IA-2(8) | Ідентифікація та автентифікація (користувачів організації) — Доступ до облікових записів — стійкість до відтворення |
| FIA_UAU.5 | Автентифікація користувача<br>Множинні механізми автентифікації | IA-2(1) | Ідентифікація та автентифікація (користувачів організації) — Багатофакторна автентифікація привілейованих облікових записів |
| | | IA-2(2) | Ідентифікація та автентифікація (користувачів організації) — Багатофакторна автентифікація непривілейованих облікових записів |
| FIA_UAU.6 | Автентифікація користувача<br>Повторне підтвердження автентичності | IA-11 | Повторна автентифікація |
| FIA_UAU.7 | Автентифікація користувача<br>Зворотний зв’язок захищеної автентифікації | IA-6 | Зворотний зв’язок автентифікатора |

| Вимоги ISO/IEC 15408 | | Каталог заходів захисту | |
|---|---|---|---|
| FIA_UID.1 | Ідентифікація користувача<br>Час ідентифікації | AC-14 | Дозволені дії без ідентифікації або автентифікації |
| | | IA-2 | Ідентифікація та автентифікація (користувачів організації) |
| | | IA-8 | Ідентифікація та автентифікація (неорганізаційні користувачі) |
| FIA_UID.2 | Ідентифікація користувача<br>Ідентифікація користувача перед будь-якими діями | AC-14 | Дозволені дії без ідентифікації або автентифікації |
| | | IA-2 | Ідентифікація та автентифікація (користувачів організації) |
| | | IA-8 | Ідентифікація та автентифікація (неорганізаційні користувачі) |
| FIA_USB.1 | Прив’язка предмета до користувача<br>Прив’язка предмета до користувача | AC-16(3) | Атрибути безпеки та приватності — Підтримка системою пов’язання атрибутів |
| FMT_MOF.1 | Управління функціями в TSF Управління поведінкою функцій безпеки | AC-3(7) | Забезпечення доступу — Управління доступом на основі ролей |
| | | AC-6 | Мінімізація повноважень |
| | | AC-6(1) | Мінімізація повноважень — Авторизований доступ до функцій безпеки |
| FMT_MSA.1 | Управління атрибутами безпеки<br>Управління атрибутами безпеки | AC-6 | Мінімізація повноважень |
| | | AC-6(1) | Мінімізація повноважень — Авторизований доступ до функцій безпеки |
| | | AC-6(2) | Атрибути безпеки та приватності - Непривілейований доступ до незахищених функцій |
| | | AC-16(4) | Атрибути безпеки та приватності — Пов’язання атрибутів авторизованими особами |
| | | AC-16 (10) | Атрибути безпеки та приватності — Конфігурація атрибутів уповноваженими особами |
| FMT_MSA.2 | Управління атрибутами безпеки<br>Безпечні атрибути безпеки | AC-16 | Атрибути безпеки та приватності |
| | | CM-6 | Налаштування конфігурації |
| | | SI-10 | Перевірка вводу інформації |
| FMT_MSA.3 | Управління атрибутами безпеки | Немає зіставлення | |

| Вимоги ISO/IEC 15408 | | Каталог заходів захисту | |
|---|---|---|---|
| | Ініціалізація статичних атрибутів | | |
| FMT_MSA.4 | Управління атрибутами безпеки<br>Спадкове значення атрибутів безпеки | Немає зіставлення | |
| FMT_MTD.1 | Управління даними TSF<br>Управління даними TSF | AC-3(7) | Забезпечення доступу — Управління доступом на основі ролей |
| | | AC-6 | Мінімізація повноважень |
| | | AC-6(1) | Мінімізація повноважень — Авторизований доступ до функцій безпеки |
| | | AU-6(7) | Мінімізація повноважень — Перегляд повноважень користувача |
| | | AU-9(4) | Захист інформації аудиту — Доступ, який надається через членство в підмножини привілейованих користувачів |
| FMT_MTD.2 | Управління даними TSF<br>Управління межами даних TSF | AC-3(7) | Забезпечення доступу — Управління доступом на основі ролей |
| | | AC-6 | Мінімізація повноважень |
| | | AC-6(1) | Мінімізація повноважень — Авторизований доступ до функцій безпеки |
| FMT_MTD.3 | Управління даними TSF<br>Захищені дані TSF | SI-10 | Перевірка вводу інформації |
| FMT_REV.1 | Скасування<br>скасування | AC-3(7) | Забезпечення доступу — Управління доступом на основі ролей |
| | | AC-3(8) | Забезпечення доступу — Анулювання прав доступу |
| | | AC-6 | Мінімізація повноважень |
| | | AC-6(1) | Мінімізація повноважень — Авторизований доступ до функцій безпеки |
| FMT_SAE.1 | Термін дії атрибутів безпеки<br>Авторизація, обмежена за часом | AC-3(7) | Забезпечення доступу — Управління доступом на основі ролей |
| | | AC-6 | Мінімізація повноважень |
| | | AC-6(1) | Мінімізація повноважень — Авторизований доступ до функцій безпеки |
| FMT_SMF.1 | Специфікація функцій управління<br>Специфікація функцій управління | Н/А | |

| Вимоги ISO/IEC 15408 | | Каталог заходів захисту | |
|---|---|---|---|
| FMT_SMR.1 | Ролі управління безпекою<br>Ролі безпеки | AC-2(7) | Управління обліковими записами — Схеми, засновані на ролях |
| | | AC-3(7) | Забезпечення доступу — Управління доступом на основі ролей |
| | | AC-5 | Розмежування обов’язків |
| | | AC-6 | Мінімізація повноважень |
| FMT_SMR.2 | Ролі управління безпекою<br>Обмеження щодо ролей безпеки | AC-2(7) | Управління обліковими записами — Схеми, засновані на ролях |
| | | AC-3(7) | Забезпечення доступу — Управління доступом на основі ролей |
| | | AC-5 | Розмежування обов’язків |
| | | AC-6 | Мінімізація повноважень |
| FMT_SMR.3 | Ролі управління безпекою<br>Очікувані ролі | AC-6(1) | Мінімізація повноважень — Авторизований доступ до функцій безпеки |
| | | AC-6(2) | Мінімізація повноважень — Непривілейований доступ до незахищених функцій |
| FPR_ANO.1 | Анонімність | Н\А | |
| FPR_ANO.2 | Анонімність<br>Анонімність, що не вимагає інформації | Н\А | |
| FPR_PSE.1 | Псевдонімність | Н\А | |
| FPR_PSE.2 | Псевдонімність<br>Оборотна псевдонімність | Н\А | |
| FPR_PSE.3 | Псевдонімність<br>Реверсивна псевдонімність | Н\А | |
| FPR_UNL.1 | Незв’язність | Н\А | |
| FPR_UNO.1 | Неспостережливість | Н\А | |
| FPR_UNO.2 | Неспостережливість<br>Виділення інформації, що впливає на неспостережливість | Н\А | |
| FPR_UNO.3 | Неспостережливість<br>Неспостережливість без витребування інформації | Н\А | |
| FPR_UNO.4 | Неспостережливість<br>Авторизована спостережливість користувача | Н\А | |
| FPT_FLS.1 | Відмова безпеки<br>Невдача зі збереженням безпечного стану | SC-7(18) | Захист периметра — Збій у безпеці |
| | | SC-24 | Уведення у відомий стан |

| Вимоги ISO/IEC 15408 | | Каталог заходів захисту | |
|---|---|---|---|
| FPT_ITA.1 | Наявність експортованих даних TSF<br>Доступність між TSF у межах визначеного показника доступності | CP-10(4) | Відновлення та відтворення системи — Відновлення у рамках часового періоду |
| | | SC-5 | Захист від атак «Відмова в обслуговуванні» |
| | | SC-5(2) | Захист від атак «Відмова в обслуговуванні» — Продуктивність, пропускна здатність і надмірність |
| | | SC-5(3) | Захист від атак «Відмова в обслуговуванні» — Виявлення та моніторинг |
| FPT_ITC.1 | Конфіденційність експортованих даних TSF<br>Конфіденційність між TSF під час передачі | SC-8 | Конфіденційність та цілісність передачі |
| | | SC-8(1) | Конфіденційність та цілісність передачі — Криптографічний захист |
| FPT_ITI.1 | Цілісність експортованих даних TSF<br>Виявлення модифікації між TSF | SC-8 | Конфіденційність тацілісність передачі |
| | | SC-8(1) | Конфіденційність та цілісність передачі — Криптографічний захист |
| | | SI-7 | Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації |
| | | SI-7(1) | Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації — Перевірка цілісності |
| | | SI-7(5) | Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації — Автоматичні відповіді про порушення цілісності |
| | | SI-7(6) | Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації — Криптографічний захист |
| FPT_ITI.2 | Цілісність експортованих даних TSF<br>Виявлення та виправлення модифікацій між ФТС | SC-8 | Конфіденційність та цілісність передачі |
| | | SC-8(1) | Конфіденційність та цілісність передачі — Криптографічний захист |
| | | SI-7 | Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації |

| Вимоги ISO/IEC 15408 | | Каталог заходів захисту | |
|---|---|---|---|
| | | SI-7(1) | Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації — Перевірка цілісності |
| | | SI-7(5) | Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації — Автоматичні відповіді про порушення цілісності |
| | | SI-7(6) | Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації — Криптографічний захист |
| FPT_ITT.1 | Внутрішня передача даних TSE TSF<br>Основний внутрішній захист від передачі даних TSF | SC-8 | Конфіденційність та цілісність передачі |
| | | SC-8(1) | Конфіденційність та цілісність передачі — Криптографічний захист |
| FPT_ITT.2 | Внутрішня передача даних TSE TSF<br>Розділення передачі даних TSF | AC-4(21) | Управління інформаційними потоками — Фізичне та логічне відділення інформаційних потоків |
| | | SC-8 | Конфіденційність та цілісність передачі |
| | | SC-8(1) | Конфіденційність та цілісність передачі — Криптографічний захист |
| FPT_ITT.3 | Внутрішня передача даних TSE TSF<br>Моніторинг цілісності даних TSF | SI-7 | Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації |
| | | SI-7(1) | Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації — Перевірка цілісності |
| | | SI-7(5) | Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації — Автоматичні відповіді про порушення цілісності |
| | | SI-7(6) | Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації — Криптографічний захист |

| Вимоги ISO/IEC 15408 | | Каталог заходів захисту | |
|---|---|---|---|
| FPT_PHP.1 | Фізичний захист TSF<br>Пасивне виявлення фізичної атаки | PE-3(5) | Керування фізичним доступом — Захист від злому |
| | | PE-6(2) | Моніторинг фізичного доступу — Автоматичні розпізнавання вторгнень і відповідна реакція |
| | | SA-18 | Захист і виявлення підробки |
| FPT_PHP.2 | Фізичний захист TSF<br>Повідомлення про фізичну атаку | PE-3(5) | Керування фізичним доступом — Захист від злому |
| | | PE-6(2) | Моніторинг фізичного доступу — Автоматичні розпізнавання вторгнень і відповідна реакція |
| | | SA-18 | Захист та виявлення підробки |
| FPT_PHP.3 | Фізичний захист TSF<br>Опір фізичній атаці | PE-3(5) | Керування фізичним доступом — Захист від злому |
| | | SA-18 | Захист і виявлення підробки |
| FPT_RCV.1 | Довірене відновлення<br>Ручне відновлення | CP-10 | Відновлення та відтворення системи |
| | | CP-12 | Безпечний режим |
| FPT_RCV.2 | Довірене відновлення<br>Автоматизоване відновлення | CP-10 | Відновлення та відтворення системи |
| | | CP-12 | Безпечний режим |
| FPT_RCV.3 | Довірене відновлення<br>Автоматичне відновлення без зайвих втрат | CP-10 | Відновлення та відтворення системи |
| | | CP-12 | Безпечний режим |
| FPT_RCV.4 | Довірене відновлення<br>Функція відновлення | SC-24 | Уведення у відомий стан |
| | | SI-6 | Перевірка функцій безпеки та приватності |
| | | SI-10(3) | Перевірка вводу інформації — Передбачувана поведінка |
| FPT_RPL.1 | Виявлення відтворення | IA-2(8) | Ідентифікація та автентифікація (користувачів організації) — Доступ до облікових записів – стійкість до відтворення |
| | | SC-23 | Автентифікація сесії |
| | | SI-3(9) | Захист від шкідливого коду — Автентифікація віддалених команд |
| FPT_SSP.1 | Державний протокол синхронізації<br>Просте довірене визнання | Н/А | |
| FPT_SSP.2 | Державний протокол синхронізації<br>Взаємне підтвердження довіри | Н/А | |
| FPT_STM.1 | Марки часу<br>Надійні позначки часу | AU-8 | Позначка часу |

| Вимоги ISO/IEC 15408 | | Каталог заходів захисту | |
|---|---|---|---|
| FPT_TDC.1 | Узгодженість даних між TSF<br>Основна узгодженість даних між TSF | AC-16(7) | Атрибути безпеки та приватності - Послідовна інтерпретація атрибутів |
| | | AC-16(8) | Атрибути безпеки та приватності — Техніки та технології пов’язання атрибутів |
| FPT_TEE.1 | Тестування зовнішніх організацій | SI-6 | Перевірка функцій безпеки та приватності |
| FPT_TRC.1 | Внутрішня узгодженість реплікації даних TSE TSF<br>Внутрішня узгодженість TSF | SI-7 | Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації |
| FPT_TST.1 | Tsf самотест<br>тестування tsf | SI-6 | Перевірка функцій безпеки та приватності |
| | | SI-7 | Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації |
| FRU_FLT.1 | Відмовостійкість<br>Понижена толерантність помилок | AU-15 | Альтернативна можливість аудиту |
| | | CP-11 | Альтернативні протоколи зв’язку |
| | | SC-24 | Уведення у відомий стан |
| | | SI-13 | Передбачуване запобігання збоїв |
| | | SI-13(1) | Запобігання передбачуваним збоям — Відповідальність за передачу функцій компонентів |
| | | SI-7(16) | Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації — Термін виконання процесу без нагляду |
| | | SI-13(3) | Запобігання передбачуваним збоям — Ручна передача функцій компонентів |
| | | SI-13(4) | Запобігання передбачуваним збоям — Встановлення резервних компонентів та оповіщення |
| | | SI-13(5) | Запобігання передбачуваним збоям — Можливість аварійного перемикання |
| FRU_FLT.2 | Відмовостійкість<br>Обмежена толерантність до помилок | AU-15 | Альтернативна можливість аудиту |
| | | CP-11 | Альтернативні протоколи зв’язку |

| Вимоги ISO/IEC 15408 | | Каталог заходів захисту | |
|---|---|---|---|
| | | SC-24 | Уведення у відомий стан |
| | | SI-13 | Передбачуване запобігання збоям |
| | | SI-13(1) | Запобігання передбачуваним збоям — Відповідальність за передачу функцій компонентів |
| | | SI-7(16) | Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації — Термін виконання процесу без нагляду |
| | | SI-13(3) | Запобігання передбачуваним збоям — Ручна передача функцій компонентів |
| | | SI-13(4) | Запобігання передбачуваним збоям — Встановлення резервних компонентів та оповіщення |
| | | SI-13(5) | Запобігання передбачуваним збоям — Можливість аварійного перемикання |
| FRU_PRS.1 | Пріоритет обслуговування<br>Обмежений пріоритет обслуговування | SC-6 | Доступність ресурсів |
| FRU_PRS.2 | Пріоритет обслуговування<br>Повний пріоритет обслуговування | SC-6 | Доступність ресурсів |
| FRU_RSA.1 | Розподіл ресурсів<br>Максимальні квоти | SC-6 | Доступність ресурсів |
| FRU_RSA.2 | Розподіл ресурсів<br>Мінімальна та максимальна квоти | SC-6 | Доступність ресурсів |
| FTA_LSA.1 | Обмеження на область вибору атрибутів | AC-2(6) | Управління обліковими записами — Динамічне управління привілеями |
| | | AC-2(11) | Управління обліковими записами — Умови використання |
| FTA_MCS.1 | Обмеження на декілька паралельних сесій | AC-10 | Управління паралельною сесією |
| FTA_MCS.2 | Обмеження на декілька паралельних сесій<br>Обмеження користувача на кілька одночасних сесій | AC-10 | Управління паралельною сесією |
| FTA_SSL.1 | Блокування та припинення сесії<br>Блокування сеансу, започаткованого TSF | AC-11 | Блокування пристрою |
| | | AC-11(1) | Блокування пристрою — Приховані дисплеї |

| Вимоги ISO/IEC 15408 | | Каталог заходів захисту | |
|---|---|---|---|
| FTA_SSL.2 | Блокування та припинення сесії<br>Блокування, ініційоване користувачем | AC-11 | Блокування пристрою |
| | | AC-11(1) | Блокування пристрою — Приховані дисплеї |
| FTA_SSL.3 | Блокування та припинення сесії<br>Ініційоване TSF припинення сесії | AC-12 | Припинення сеансу |
| | | SC-10 | Відключення мережі |
| FTA_SSL.4 | Блокування та припинення сесії<br>Припинення ініційоване користувачем | AC-12(1) | Припинення сеансу — Ініційоване користувачем блокування |
| FTA_TAB.1 | TOE Банери доступу<br>Банери доступу до TOE за замовчуванням | AC-8 | Попередження про використання системи |
| FTA_TAH.1 | TOE Історія доступу | AC-9 | Сповіщення про попередній вхід (доступ) |
| | | AC-9(1) | Сповіщення про попередній вхід (доступ) — Невдалі спроби входу до системи |
| FTA_TSE.1 | Створення сесії TOE | AC-2(11) | Управління обліковими записами — Умови використання |
| FTP_ITC.1 | Довірений канал між TSF | IA-3(1) | Ідентифікація та автентифікація пристроїв — Криптографічна двобічна автентифікація |
| | | SC-8 | Конфіденційність та цілісність передачі |
| | | SC-8(1) | Конфіденційність та цілісність передачі — Криптографічний захист |
| FTP_TRP.1 | Довірений канал зв’язку | SC-11 | Довірений канал зв’язку |
| | | | |
| **Вимоги до гарантій безпеки** | | | |
| ASE_INT.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7 | St вступ | SA-4 | Процес закупівель |
| ASE_CCL.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7 | Заяви про відповідність | PL-2 | Плани захисту інформації та персональних даних |
| | | SA-4(7) | Процес закупівель — Затверджені профілі захисту |
| ASE_SPD.1 EAL1 EAL2 | Визначення проблеми безпеки | PL-2 | Плани захисту інформації та персональних даних |
| | | SA-4 | Процес закупівель |

| Вимоги ISO/IEC 15408 | | Каталог заходів захисту | |
|---|---|---|---|
| EAL3 EAL4 EAL5 EAL6 EAL7 | | | |
| ASE_OBJ.1 EAL1 | Цілі безпеки<br>Цілі безпеки для операційного середовища | PL-2 | Плани захисту інформації та персональних даних |
| | | SA-4 | Процес закупівель |
| ASE_OBJ.2 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7 | Цілі безпеки | PL-2 | Плани захисту інформації та персональних даних |
| | | SA-4 | Процес закупівель |
| ASE_ECD.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7 | Визначення розширених компонентів | Н/А | |
| ASE_REQ.1 EAL1 | Вимоги безпеки<br>Заявлені вимоги безпеки | PL-2 | Плани захисту інформації та персональних даних |
| | | SA-4 | Процес закупівель |
| ASE_REQ.2 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7 | Вимоги безпеки<br>Похідні вимоги безпеки | PL-2 | Плани захисту інформації та персональних даних |
| | | SA-4 | Процес закупівель |
| ASE_TSS.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7 | Зведена специфікація TOE | PL-2 | Плани захисту інформації та персональних даних |
| | | SA-4(1) | Процес закупівель — Функціональні властивості заходів |
| ASE_TSS.2 | Технічна характеристика TOE<br>Технічна характеристика TOE з підсумком архітектурного дизайну | PL-2 | Плани захисту інформації та персональних даних |
| | | SA-4(1) | Процес закупівель — Функціональні властивості заходів |
| | | SA-4(2) | Процес закупівель — Розробка та впровадження інформації для заходів |
| | | SA-17 | Проєкт і архітектура безпеки розробника |
| ADV_ARC.1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7 | Архітектура безпеки<br>Опис архітектури безпеки | AC-25 | Диспетчер доступу |
| | | SA-17 | Проєкт і архітектура безпеки розробника |
| | | SA-18 | Захист і виявлення підробки |
| | | SC-3 | Ізоляція функцій безпеки |
| | | SC-3(1) | Ізоляція функцій безпеки — Розділення апаратного забезпечення |
| | | SC-3(3) | Ізоляція функцій безпеки — Мінімізація функціональності небезпеки |
| | | SC-41 | Доступ до портів і пристроїв введення/виведення |

| Вимоги ISO/IEC 15408 | | Каталог заходів захисту | |
|---|---|---|---|
| ADV_FSP.1 EAL1 | Функціональна специфікація Основні функціональні характеристики | SA-4(1) | Процес закупівель — Функціональні властивості заходів |
| | | SA-4(2) | Процес закупівель — Розробка та впровадження інформації для заходів |
| ADV_FSP.2 EAL2 | Функціональна специфікація Функціональна специфікація для забезпечення безпеки | SA-4(1) | Процес закупівель — Функціональні властивості заходів |
| | | SA-4(2) | Процес закупівель — Розробка та впровадження інформації для заходів |
| | | SA-17(4) | Проєкт і архітектура безпеки розробника — Неформальна відповідність |
| ADV_FSP.3 EAL3 | Функціональна специфікація Функціональна специфікація з повним резюме | SA-4(1) | Процес закупівель — Функціональні властивості заходів |
| | | SA-4(2) | Процес закупівель — Розробка та впровадження інформації для заходів |
| | | SA-17(4) | Проєкт і архітектура безпеки розробника — Неформальна відповідність |
| ADV_FSP.4 EAL4 | Функціональна специфікація Повна функціональна специфікація | SA-4(1) | Процес закупівель — Функціональні властивості заходів |
| | | SA-4(2) | Процес закупівель — Розробка та впровадження інформації для заходів |
| | | SA-17(4) | Проєкт і архітектура безпеки розробника — Неформальна відповідність |
| ADV_FSP.5 EAL5 EAL6 | Функціональна специфікація Повна напівформальна функціональна специфікація з додатковою інформацією про помилки | SA-4(1) | Процес закупівель — Функціональні властивості заходів |
| | | SA-4(2) | Процес закупівель — Розробка та впровадження інформації для заходів |
| | | SA-17(4) | Проєкт і архітектура безпеки розробника — Неформальна відповідність |
| ADV_FSP.6 EAL7 | Функціональна специфікація Повна напівформальна функціональна специфікація з додатковою формальною специфікацією | SA-4(1) | Процес закупівель — Функціональні властивості заходів |
| | | SA-4(2) | Процес закупівель — Розробка та впровадження інформації для заходів |
| | | SA-17(3) | Проєкт і архітектура безпеки розробника — Формальна відповідність |

| Вимоги ISO/IEC 15408 | | Каталог заходів захисту | |
|---|---|---|---|
| | | SA-17(4) | Проєкт і архітектура безпеки розробника — Неформальна відповідність |
| ADV_IMP.1<br>EAL4<br>EAL5 | Представництво з реалізації<br>Представництво TSF щодо впровадження | SA-4(2) | Процес закупівель — Розробка та впровадження інформації для управління |
| ADV_IMP.2<br>EAL6<br>EAL7 | Представництво з реалізації<br>Повне картографування представництва щодо впровадження TSF | SA-4(2) | Процес закупівель — Розробка та впровадження інформації для заходів |
| | | SA-17(3) | Проєкт і архітектура безпеки розробника — Формальна відповідність |
| ADV_INT.1 | Внутрішня TSF<br>Добре структурована підмножина внутрішніх служб TSF | SA-8 | Безпека та приватність принципів інжинірингу (проєктування) |
| | | SC-3(3) | Ізоляція функцій безпеки — Мінімізація функціональності |
| | | SC-3(4) | Ізоляція функцій безпеки — З'єднання модулів і зв'язність |
| | | SC-3(5) | Ізоляція функцій безпеки — Багаторівнева структура |
| ADV_INT.2 EAL5 | Внутрішня TSF<br>Добре структуровані внутрішні служби | SA-8 | Безпека та приватність принципів інжинірингу (проєктування) |
| | | SC-3(3) | Ізоляція функцій безпеки — Мінімізація функціональності |
| | | SC-3(4) | Ізоляція функцій безпеки — З'єднання модулів і зв'язність |
| | | SC-3(5) | Ізоляція функцій безпеки — Багаторівнева структура |
| ADV_INT.3 EAL6<br>EAL7 | Внутрішня TSF<br>Мінімальна складність внутрішньої структури | SA-8 | Безпека та приватність принципів інжинірингу (проєктування) |
| | | SA-17(5) | Проєкт і архітектура безпеки розробника — Концептуальний проєкт |
| | | SC-3(3) | Ізоляція функцій безпеки — Мінімізація функціональності |
| | | SC-3(4) | Ізоляція функцій безпеки — З'єднання модулів і зв'язність |
| | | SC-3(5) | Ізоляція функцій безпеки — Багаторівнева структура |
| | | AC-25 | Диспетчер доступу |

| Вимоги ISO/IEC 15408 | | Каталог заходів захисту | |
|---|---|---|---|
| ADV_SPM.1<br>EAL6<br>EAL7 | Моделювання політики безпеки<br>Формальна модель політики безпеки TOE | SA-17(1) | Проєкт і архітектура безпеки розробника — Формальна модель політики |
| | | SA-17(3) | Проєкт і архітектура безпеки розробника — Формальна відповідність |
| ADV_TDS.1<br>EAL2 | Дизайн TOE<br>Основний дизайн | SA-4(2) | Процес закупівель — Розробка та впровадження інформації для заходів |
| | | SA-17 | Проєкт і архітектура безпеки розробника |
| ADV_TDS.2<br>EAL3 | Дизайн TOE<br>Архітектурний дизайн | SA-4(2) | Процес закупівель — Розробка та впровадження інформації для заходів |
| | | SA-17 | Проєкт і архітектура безпеки розробника |
| ADV_TDS.3<br>EAL4 | Дизайн TOE<br>Основний модульний дизайн | SA-4(2) | Процес закупівель — Розробка та впровадження інформації для заходів |
| | | SA-17 | Проєкт і архітектура безпеки розробника |
| ADV_TDS.4<br>EAL5 | Дизайн TOE<br>Напівформальне модульне проєктування | SA-4(2) | Процес закупівель — Розробка та впровадження інформації для заходів |
| | | SA-17 | Проєкт і архітектура безпеки розробника |
| | | SA-4(2) | Процес закупівель — Розробка та впровадження інформації для заходів |
| | | SA-17(4) | Проєкт і архітектура безпеки розробника — Неформальна відповідність |
| ADV_TDS.5<br>EAL6 | Дизайн TOE<br>Повний напівформальний модульний дизайн | SA-4(2) | Процес закупівель — Розробка та впровадження інформації для заходів |
| | | SA-17 | Проєкт і архітектура безпеки розробника |
| | | SA-17(2) | Проєкт і архітектура безпеки розробника — Компоненти, що необхідні для забезпечення безпеки |
| | | SA-17(4) | Проєкт і архітектура безпеки розробника — Неформальна відповідність |
| ADV_TDS.6<br>EAL7 | Дизайн TOE<br>Повний напівформальний модульний дизайн з формальною презентацією дизайну високого рівня | SA-4(2) | Процес закупівель — Розробка та впровадження інформації для заходів |
| | | SA-17 | Проєкт і архітектура безпеки розробника |
| | | SA-17(2) | Проєкт і архітектура безпеки розробника — Компоненти, |

| Вимоги ISO/IEC 15408 | | Каталог заходів захисту | |
|---|---|---|---|
| | | | що необхідні для забезпечення безпеки |
| | | SA-17(3) | Проєкт і архітектура безпеки розробника — Формальна відповідність |
| | | SA-17(4) | Проєкт і архітектура безпеки розробника — Неформальна відповідність |
| AGD_OPE.1<br>EAL1<br>EAL2<br>EAL3 EAL4<br>EAL5 EAL6<br>EAL7 | Оперативне керівництво користувача | SA-5 | Системна документація |
| AGD_PRE.1<br>EAL1<br>EAL2<br>EAL3 EAL4<br>EAL5 EAL6<br>EAL7 | Підготовчі процедури | SA-5 | Системна документація |
| ALC_CMC.1<br>EAL1 | Можливості cm маркування toe | CM-9 | План управління конфігурацією |
| | | SA-10 | Управління конфігурацією розробника |
| ALC_CMC.2<br>EAL2 | Можливості CM Використання системи CM | CM-9 | План управління конфігурацією |
| | | SA-10 | Управління конфігурацією розробника |
| ALC_CMC.3<br>EAL3 | Можливості CM Контроль авторизації | CM-3 | Управління змінами конфігурації |
| | | CM-9 | План управління конфігурацією |
| | | SA-10 | Управління конфігурацією розробника |
| ALC_CMC.4<br>EAL4<br>EAL5 | Можливості CM Підтримка виробництва, процедури приймання та автоматизація | CM-3 | Управління змінами конфігурації |
| | | CM-3(1) | Управління змінами конфігурації — Автоматизована документація, повідомлення та заборона внесення змін |
| | | CM-3(3) | Управління змінами конфігурації — Автоматизована реалізація змін |
| | | CM-9 | План управління конфігурацією |
| | | SA-10 | Управління конфігурацією розробника |
| ALC_CMC.5<br>EAL6 | Можливості CM Розширена підтримка | CM-3 | Управління змінами конфігурації |

| Вимоги ISO/IEC 15408 | | Каталог заходів захисту | |
|---|---|---|---|
| EAL7 | | CM-3(1) | Управління змінами конфігурації — Автоматизована документація, повідомлення та заборона внесення змін |
| | | CM-3(2) | Управління змінами конфігурації — Тестування, валідація та документація змін |
| | | CM-3(3) | Управління змінами конфігурації — Автоматизована реалізація змін |
| | | CM-9 | План управління конфігурацією |
| | | SA-10 | Управління конфігурацією розробника |
| ALC_CMS.1<br>EAL1 | Область застосування CM<br>Покриття TOE CM | CM-9 | План управління конфігурацією |
| | | SA-10 | Управління конфігурацією розробника |
| ALC_CMS.2<br>EAL2 | Область застосування CM<br>Частини покриття TOE CM | CM-9 | План управління конфігурацією |
| | | SA-10 | Управління конфігурацією розробника |
| ALC_CMS.3<br>EAL3 | Область застосування CM<br>Впровадження представництва покриття CM | CM-9 | План управління конфігурацією |
| | | SA-10 | Управління конфігурацією розробника |
| ALC_CMS.4<br>EAL4 | Область застосування CM<br>Проблема відстеження покриття CM | CM-9 | План управління конфігурацією |
| | | SA-10 | Управління конфігурацією розробника |
| ALC_CMS.5<br>EAL5<br>EAL6<br>EAL7 | Область застосування CM<br>Інструменти розробки покриття CM | CM-9 | План управління конфігурацією |
| | | SA-10 | Управління конфігурацією розробника |
| ALC_DEL.1<br>EAL2 EAL3<br>EAL4 EAL5<br>EAL6 EAL7 | Постачання<br>Процедури постачання | MP-5 | Транспортування носіїв інформації |
| | | SA-10(1) | Управління конфігурацією розробника — Перевірка цілісності програмного забезпечення та мікропрограм |
| | | SA-10(6) | Управління конфігурацією розробника — Довірене постачання |
| | | SA-18 | Захист і виявлення підробки |
| | | SA-19 | Справжність компонента |
| ALC_DVS.1<br>EAL3 | | SA-1 | Політика та процедури придбання системи та послуг |

| Вимоги ISO/IEC 15408 | | Каталог заходів захисту | |
|---|---|---|---|
| EAL4<br>EAL5 | Безпека розвитку<br>Визначення заходів безпеки | SA-3 | Життєвий цикл розробки системи |
| | | SA-12 | Керування ризиками ланцюга постачання |
| ALC_DVS.2<br>EAL6<br>EAL7 | Безпека розвитку<br>Достатність заходів безпеки | CM-5 | Обмеження доступу до змін |
| | | SA-3 | Життєвий цикл розробки системи |
| | | SA-12 | Керування ризиками ланцюга постачання |
| ALC_FLR.1 | Виправлення недоліків<br>Основні виправлення недоліків | SA-10 | Управління конфігурацією розробника |
| | | SA-11 | Тестування та оцінювання розробника |
| | | SI-2 | Виправлення дефектів |
| ALC_FLR.2 | Виправлення недоліків<br>Процедури повідомлення про недоліки | SA-10 | Управління конфігурацією розробника |
| | | SA-11 | Тестування та оцінювання розробника |
| | | SI-2 | Виправлення дефектів |
| ALC_FLR.3 | Виправлення недоліків<br>Систематичне виправлення недоліків | SA-10 | Управління конфігурацією розробника |
| | | SA-11 | Тестування та оцінювання розробника |
| | | SI-2 | Виправлення дефектів |
| ALC_LCD.1<br>EAL3<br>EAL4<br>EAL5 EAL6 | Визначення життєвого циклу<br>Розробник визначив модель життєвого циклу | SA-3 | Життєвий цикл розробки системи |
| | | SA-15 | Процеси, стандарти та інструменти розробки |
| ALC_LCD.2<br>EAL7 | Визначення життєвого циклу<br>Вимірна модель життєвого циклу | SA-3 | Життєвий цикл розробки системи |
| | | SA-15 | Процеси, стандарти та інструменти розробки |
| ALC_TAT.1<br>EAL4 | Інструменти та Техніка<br>Добре продумані інструменти розробки | SA-15 | Процеси, стандарти та інструменти розробки |
| ALC_TAT.2<br>EAL5 | Інструменти та Техніка<br>Відповідність стандартам реалізації | SA-15 | Процеси, стандарти та інструменти розробки |
| ALC_TAT.3<br>EAL6<br>EAL7 | Інструменти та Техніка<br>Відповідність стандартам реалізації — усі деталі | SA-15 | Процеси, стандарти та інструменти розробки |
| ATE_COV.1 | Покриття<br>Наявність покриття | SA-11 | Тестування та оцінювання розробника |
| EAL2 | | SA-11(7) | Тестування та оцінювання розробника — Перевірка обсягу тестування та оцінювання |
| ATE_COV.2<br>EAL3 | Покриття<br>Аналіз покриття | SA-11 | Тестування та оцінювання розробника |

| Вимоги ISO/IEC 15408 | | Каталог заходів захисту | |
|---|---|---|---|
| EAL4<br>EAL5 | | SA-11(7) | Тестування та оцінювання розробника — Перевірка обсягу тестування та оцінювання |
| ATE_COV.3<br>EAL6<br>EAL7 | Покриття<br>Ретельний аналіз покриття | SA-11 | Тестування та оцінювання розробника |
| | | SA-11(7) | Тестування та оцінювання розробника — Перевірка обсягу тестування та оцінювання |
| ATE_DPT.1 EAL3 | Глибина<br>Тестування: Основний дизайн | SA-11 | Тестування та оцінювання розробника |
| | | SA-11(7) | Тестування та оцінювання розробника — Перевірка обсягу тестування та оцінювання |
| ATE_DPT.2 EAL4 | Глибина<br>Тестування: Модулі посилення безпеки | SA-11 | Тестування та оцінювання розробника |
| | | SA-11(7) | Тестування та оцінювання розробника — Перевірка обсягу тестування та оцінювання |
| ATE_DPT.3 EAL5<br>EAL6 | Глибина<br>Тестування: Модульний дизайн | SA-11 | Тестування та оцінка розробника |
| | | SA-11(7) | Тестування та оцінювання розробника — Перевірка обсягу тестування та оцінювання |
| ATE_DPT.4 EAL7 | Глибина<br>Тестування: представлення впровадження | SA-11 | Тестування та оцінювання розробника |
| | | SA-11(7) | Тестування та оцінювання розробника — Перевірка обсягу тестування та оцінювання |
| ATE_FUN.1<br>EAL2<br>EAL3<br>EAL4 EAL5 | Функціональні тести<br>Функціональне тестування | SA-11 | Тестування та оцінювання розробника |
| ATE_FUN.2<br>EAL6<br>EAL7 | Функціональні тести<br>Замовлене функціональне тестування | SA-11 | Тестування та оцінювання розробника |
| ATE_IND.1 EAL1 | Незалежне тестування<br>Незалежне тестування — відповідність | CA-2 | Оцінювання |
| | | CA-2(1) | Оцінювання — Незалежні експерти |
| | | SA-11(3) | Тестування та оцінювання розробника — Незалежна перевірка планів оцінювання та доказів |
| ATE_IND.2 EAL2<br>EAL3<br>EAL4 EAL5 EAL6 | Незалежне тестування<br>Незалежне тестування — зразок | CA-2 | Оцінювання |
| | | CA-2(1) | Оцінювання — Незалежні експерти |

| Вимоги ISO/IEC 15408 | | Каталог заходів захисту | |
|---|---|---|---|
| | | SA-11(3) | Тестування та оцінювання розробника – Незалежна перевірка планів оцінювання та доказів |
| ATE_IND.3<br>EAL7 | Незалежне тестування<br>Незалежне тестування — завершено | CA-2 | Оцінювання |
| | | CA-2(1) | Оцінювання — Незалежні експерти |
| | | SA-11(3) | Тестування та оцінювання розробника — Незалежна перевірка планів оцінювання та доказів |
| AVA_VAN.1<br>EAL1 | Аналіз вразливості<br>Обстеження вразливості | CA-2 | Оцінювання — Спеціалізовані оцінювання |
| | | CA-8 | Тестування на проникнення |
| | | RA-3 | Оцінювання ризику |
| | | SA-11(2) | Тестування та оцінювання розробника — Моделювання загроз і аналіз вразливостей |
| | | SA-11(5) | Тестування та оцінювання розробника — Тестування на проникнення |
| AVA_VAN.2<br>EAL2<br>EAL3 | Аналіз вразливості | CA-2(2) | Оцінювання — Спеціалізовані оцінювання |
| | | CA-8 | Тестування на проникнення |
| | | RA-3 | Оцінювання ризику |
| | | SA-11(2) | Тестування та оцінювання розробника — Моделювання загроз і аналіз вразливостей |
| | | SA-11(5) | Тестування та оцінювання розробника — Тестування на проникнення |
| AVA_VAN.3<br>EAL4 | Аналіз вразливості<br>Сфокусований аналіз вразливості | CA-2(2) | Оцінювання — Спеціалізовані оцінювання |
| | | CA-8 | Тестування на проникнення |
| | | RA-3 | Оцінювання ризику |
| | | SA-11(2) | Тестування та оцінювання розробника — Моделювання загроз та аналіз вразливостей |
| | | SA-11(5) | Тестування та оцінювання розробника — Тестування на проникнення |
| AVA_VAN.4<br>EAL5 | Аналіз вразливості<br>Методичний аналіз вразливості | CA-2(2) | Оцінювання — Спеціалізовані оцінювання |
| | | CA-8 | Тестування на проникнення |
| | | RA-3 | Оцінювання ризику |
| | | SA-11(2) | Тестування та оцінювання розробника — Моделювання загроз і аналіз вразливостей |
| | | SA-11(5) | Тестування та оцінювання розробника — Тестування на проникнення |

| Вимоги ISO/IEC 15408 | | Каталог заходів захисту | |
|---|---|---|---|
| AVA_VAN.5<br>EAL6<br>EAL7 | Аналіз вразливості<br>Розширений методичний аналіз вразливості | CA-2(2) | Оцінювання — Спеціалізовані оцінювання |
| | | CA-8 | Тестування на проникнення |
| | | RA-3 | Оцінювання ризику |
| | | SA-11(2) | Тестування та оцінювання розробника — Моделювання загроз і аналіз вразливостей |
| | | SA-11(5) | Тестування та оцінювання розробника — Тестування на проникнення |
| ACO_COR.1 | Обґрунтування складу | SA-17 | Проєкт і архітектура безпеки розробника |
| ACO_DEV.1 | Докази розвитку<br>Функціональний опис | SA-17 | Проєкт і архітектура безпеки розробника |
| ACO_DEV.2 | Докази розвитку<br>Основні докази дизайну | SA-17 | Проєкт і архітектура безпеки розробника |
| ACO_DEV.3 | Докази розвитку<br>Детальні докази дизайну | SA-17 | Проєкт і архітектура безпеки розробника |
| ACO_REL.1 | Довіра залежному компоненту<br>Основна інформація про опору | SA-17 | Проєкт і архітектура безпеки розробника |
| ACO_REL.2 | Довіра залежному компоненту Інформація про довіру | SA-17 | Проєкт і архітектура безпеки розробника |
| ACO_CTT.1 | Складене тестування TOE<br>Тестування інтерфейсу | SA-11 | Тестування та оцінювання розробника |
| ACO_CTT.2 | Складене тестування TOE<br>Ретельне тестування інтерфейсу | SA-11 | Тестування та оцінювання розробника |
| ACO_VUL.1 | Аналіз вразливості складу<br>Огляд вразливості складу | CA-2 | Оцінювання — Спеціалізовані оцінювання |
| | | CA-8 | Тестування на проникнення |
| | | RA-3 | Оцінювання ризику |
| | | SA-11 | Тестування та оцінювання розробника |
| ACO_VUL.2 | Аналіз вразливості складу | CA-2 | Оцінювання — Спеціалізовані оцінювання |
| | | CA-8 | Тестування на проникнення |
| | | RA-3 | Оцінювання ризику |
| | | SA-11 | Тестування та оцінювання розробника |
| ACO_VUL.3 | Аналіз вразливості складу<br>Розширений огляд вразливості складу | CA-2 | Оцінювання — Спеціалізовані оцінювання |
| | | CA-8 | Тестування на проникнення |
| | | RA-3 | Оцінювання ризику |
| | | SA-11 | Тестування та оцінювання розробника |

## Додаток Г
## ВІДОБРАЖЕННЯ ВИМОГ НД ТЗІ 3.6-006-2021 ТА ВИМОГИ НД ТЗІ 2.5-004- 99

Таблицю Г.1 побудовано за принципом можливості розповсюдження та/або перетину окремих складників критеріїв, наведених у НД ТЗІ 2.5-004-99, та заходів захисту, що визначені в цьому НД ТЗІ. Як приклад надамо пояснення першої позиції таблиці Г.1. Згідно з класом заходів захисту АС-1, пунктами «а» та «с» передбачаються такі заходи захисту:

a. Розробити, задокументувати та поширити [*Призначення: серед визначеного організацією персоналу або ролей*]:

1. політику (правила) управління доступом, яка:

(a) містить мету, сферу застосування, ролі, обов'язки, зобов'язання керівництва, координацію між організаційними підрозділами та систему контролю відповідності (compliances);

(b) відповідає чинному законодавству, нормативним документам, директивам, нормам, політикам, стандартам і керівним документам;

2. процедури, що сприяють реалізації політики управління доступом і відповідних заходів управління доступом.

b. Призначити посаду [*Призначення: визначену організацією посадову особу*] для управління політикою та процедурами управління доступом.

c. Переглянути й оновити:

1. поточну політику управління доступом [*Призначення: з визначеною організацією частотою*];

2. поточні процедури управління доступом [*Призначення: з визначеною організацією частотою*];

Аналогічні заходи, серед сукупності інших заходів, передбачені в КА (Адміністративна конфіденційність) у частині про те, що комплекс засобів захисту повинен надавати можливість адміністратору або користувачу, який має відповідні повноваження для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити конкретних користувачів і/або групи користувачів/процесів, які мають (не мають) право одержувати інформацію від об'єкта. Таким чином, вимоги та мета наведених пунктів, що визначені в цьому НД ТЗІ та НД ТЗІ 2.5-004-99, перетинається в частині необхідності розробки політик і процедур управління доступом, який є складовим і необхідним елементом адмвініструванні об'єкта, що захищається.

Як бачимо з наведеного прикладу, у двох категоріях (заходів захисту та критерії захищеності) маються спільні окремі складники, які повинні бути/виконуватися в обох випадках. При побудові таблиці Г.1 проводився аналіз складових заходів і критеріїв, виконувався пошук спільних складників, і в разі наявності відповідні категорії вказувалися в таблиці, а за відсутності — проставлявся «-».

Таблиця Г.1 — Принцип можливості розповсюдження та/або перетину окремих складових критеріїв, наведених у НД ТЗІ 2.5-004-99 та заходів захисту, що визначені в Каталозі ЗЗІ та ПД, який наведений в цьому НД ТЗІ

| **Каталог ЗЗІ та ПД** | | | **НД ТЗІ 2.5-004-99** | |
|---|---|---|---|---|
| Шифр | Назва | | Шифр | Назва |
| | УПРАВЛІННЯ ДОСТУПОМ (АС) | | | |
| АС-1 | Політика та процедури управління доступом | АС-1 a<br>АС-1 c | КА-1-4 | Адміністративна конфіденційність |
| | | АС-1 b<br>АС-1 d | - | |
| | | АС-1 e | ДВ-1-3 | Відновлення після збоїв |
| АС-2 | Управління обліковими записами | АС-2 a<br>АС-2 c | КА-1-4 | Адміністративна конфіденційність |
| | | АС-2 b<br>АС-2 d<br>АС-2 e<br>АС-2 h<br>АС-2 i<br>АС-2 j<br>АС-2 k<br>АС-2 l | - | |
| | | АС-2 f | НО-1-3 | Розподіл обов’язків |
| | | АС-2 g | НР-1-5 | Критерії спостережності — Реєстрація |
| АС-3 | Забезпечення доступу | | КД-1-4<br>КА-1-4<br><br>КО-1 | Довірча конфіденційність<br>Адміністративна конфіденційність<br>Повторне використання об’єктів |
| АС-4 | Управління інформаційними потоками | | - | |
| АС-5 | Розмежування обов’язків | АС-5 a<br>АС-5 c | КД-1-4<br>КА-1-4 | Довірча конфіденційність<br>Адміністративна конфіденційність |
| | | АС-5 b | НО-1 | Розподіл обов’язків (у частині наявності комплексу засобів захисту функціоналу щодо реалізації політики розподілу обов’язків) |
| АС-6 | Мінімізація повноважень | | НО-2<br><br>НО-3 | Розподіл обов’язків адміністраторів<br>Розподіл обов’язків на підставі привілеїв |
| АС-7 | Невдалі спроби входу в систему | | - | |
| АС-8 | Попередження про використання системи | | - | |
| АС-9 | Сповіщення про попередній вхід (доступ) | | - | |
| АС-10 | Управління паралельною сесією | | - | |

| Каталог ЗЗІ та ПД | | | НД ТЗІ 2.5-004-99 | |
|---|---|---|---|---|
| Шифр | Назва | | Шифр | Назва |
| AC-11 | Блокування пристрою | | - | |
| AC-12 | Припинення сеансу | | - | |
| AC-13 | Нагляд і огляд — управління доступом | Вилучено | | |
| AC-14 | Дозволені дії без ідентифікації або автентифікації | | - | |
| AC-15 | Автоматизоване маркування | Вилучено | | |
| AC-16 | Атрибути безпеки та приватності | | - | |
| AC-17 | Віддалений доступ | | - | |
| AC-18 | Бездротовий доступ | | - | |
| AC-19 | Контроль доступу для мобільних пристроїв | | - | |
| AC-20 | Використання зовнішніх систем | | ЦВ-1-3 | Цілісність при обміні (у частині контролю цілісності) |
| AC-21 | Розповсюдження інформації | | ЦВ-1-3 | Цілісність при обміні (у частині контролю цілісності) |
| AC-22 | Публічно доступний контент | | - | |
| AC-23 | Захист від несанкціонованого інтелектуального аналізу даних | | - | |
| AC-24 | Рішення щодо управління доступом | | - | |
| AC-25 | Диспетчер доступу | | - | |
| | ОБІЗНАНІСТЬ І НАВЧАННЯ (AT) | | | |
| AT-1 | Політика та процедури підвищення обізнаності та навчання | | - | |
| AT-2 | Навчання з підвищення обізнаності | | - | |
| AT-3 | Рольове навчання | | - | |
| AT-4 | Навчальні записи | | - | |
| AT-5 | Контакти з групами безпеки та асоціаціями | Вилучено | | |
| AT-6 | Відгуки про проведені навчання | | - | |
| | АУДИТ І ПІДЗВІТНІСТЬ (AU) | | | |
| AU-1 | Політика та процедури аудиту та підзвітності | | - | |
| AU-2 | Події аудиту | AU-2 a<br>AU-2 d | НР-1-5 | Реєстрація |
| | | AU-2 b | НР-1 | Зовнішній аналіз |
| | | AU-2 c | - | |
| AU-3 | Зміст записів аудиту | | НР-1-5 | Реєстрація |
| AU-4 | Місткість сховища записів аудиту | | - | |

| Каталог ЗЗІ та ПД | | | НД ТЗІ 2.5-004-99 | |
|---|---|---|---|---|
| Шифр | Назва | | Шифр | Назва |
| AU-5 | Реагування на відмови обробки даних аудиту | | НР-3<br>НР-4<br>НР-5 | Сигналізація про небезпеку<br>Детальна реєстрація<br>Аналіз у реальному часі |
| AU-6 | Огляд, аналіз і звітність аудиту | AU-6 a<br>AU-6 b | НР-1-5 | Реєстрація |
| | | AU-6 c | - | |
| AU-7 | Скорочення записів аудиту та формування звіту | | - | |
| AU-8 | Позначка часу | | НР-1-5 | Реєстрація |
| AU-9 | Захист інформації аудиту | | НР-2<br>НР-3<br>НР-4<br>НР-5 | Захищений журнал<br>Сигналізація про небезпеку<br>Детальна реєстрація<br>Аналіз у реальному часі |
| AU-10 | Неспростовність | | НИ-1-3<br><br>НВ-1-3<br><br>НА-1-2<br><br>НП-1-2 | Ідентифікація і автентифікація<br>Ідентифікація і автентифікація при обміні<br>Автентифікація відправника<br>Автентифікація отримувача |
| AU-11 | Збереження записів аудиту | | - | |
| AU-12 | Генерація даних аудиту | | - | |
| AU-13 | Моніторинг розкриття інформації | | - | |
| AU-14 | Аудит сесії | | - | |
| AU-15 | Альтернативна можливість аудиту | | - | |
| AU-16 | Міжорганізаційний аудит | | - | |
| ОЦІНЮВАННЯ, АКРЕДИТАЦІЯ ТА МОНІТОРИНГ (CA) | | | | |
| CA-1 | Політика та процедури оцінювання, акредитації та моніторингу | | - | |
| CA-2 | Оцінювання | | - | |
| CA-3 | Взаємодія систем | CA-3 a | НК-1-2 | Достовірний канал |
| | | CA-3 b<br>CA-3 c | - | |
| CA-4 | Сертифікація безпеки | Вилучено | | |
| CA-5 | План усунення недоліків та контрольні показники | | - | |
| CA-6 | Акредитація | CA-6 a<br>CA-6 c | - | |
| | | CA-6 b | НИ-1-3<br><br>НВ-1-3<br><br>НА-1-2 | Ідентифікація і автентифікація<br>Ідентифікація і автентифікація при обміні |

| Каталог ЗЗІ та ПД | | | НД ТЗІ 2.5-004-99 | |
|---|---|---|---|---|
| Шифр | Назва | | Шифр | Назва |
| | | | НП-1-2 | Автентифікація відправника<br>Автентифікація отримувача |
| CA-7 | Безперервний моніторинг | CA-7 a<br>CA-7 b<br>CA-7 c | НЦ-1-3<br>НТ-1-3 | Цілісність комплексу засобів захисту<br>Самотестування |
| | | CA-7 d | НТ-3 | Самотестування в реальному часі |
| | | CA-7 e<br>CA-7 f<br>CA-7 g | - | |
| CA-8 | Тестування на проникнення | | - | |
| CA-9 | Внутрішні з’єднання системи | | - | |
| УПРАВЛІННЯ КОНФІГУРАЦІЄЮ (CM) | | | | |
| CM-1 | Політика та процедури управління конфігурацією | CM-1 a<br>CM-1 b<br>CM-1 c | - | |
| | | CM-1 d | Г-1-7 | Керування конфігурацією |
| | | CM-1 e | ДВ-1-3 | Відновлення після збоїв |
| CM-2 | Базова конфігурація | | | 10.5 Документація |
| CM-3 | Управління змінами конфігурації | | | Середовище розробки: Керування конфігурацією; Визначення конфігурації; Регулювання конфігурації; Облік стану; Перевірка якості конфігурації |
| CM-4 | Аналіз впливу на безпеку та приватність | | - | |
| CM-5 | Обмеження доступу до змін | | | Середовище розробки: Керування конфігурацією; Визначення конфігурації; Регулювання конфігурації; Облік стану |
| CM-6 | Налаштування конфігурації | CM-6 a | | Середовище розробки: Визначення конфігурації |
| | | CM-6 b | Г-1-7 | Середовище розробки: Керування конфігурацією |
| | | CM-6 c | Г-4-7 | Середовище розробки: Керування конфігурацією |
| | | CM-6 d | | Середовище розробки: Облік стану |
| CM-7 | Мінімально необхідна функціональність | | | Середовище розробки: Перевірка якості конфігурації |
| CM-8 | Інвентаризація компонентів системи | | - | |
| CM-9 | План управління конфігурацією | | | Середовище розробки: Процес розробки |

| Каталог ЗЗІ та ПД | | | НД ТЗІ 2.5-004-99 | |
|---|---|---|---|---|
| Шифр | Назва | | Шифр | Назва |
| СМ-10 | Обмеження використання програмного забезпечення | | - | |
| СМ-11 | Встановлене користувачем програмне забезпечення | | | Середовище розробки: Керування конфігурацією |
| СМ-12 | Розташування інформації | | - | |
| СМ-13 | Відображення дій даних | | - | |
| СМ-14 | Підписані компоненти | | - | |
| ПЛАНУВАННЯ БЕЗПЕРЕРВНОЇ РОБОТИ (СР) | | | | |
| СР-1 | Політика та процедури планування безперервної роботи | | - | |
| СР-2 | План забезпечення безперервної роботи та відновлення функціонування | | - | |
| СР-3 | Навчання із забезпечення безперервної роботи | | - | |
| СР-4 | Тестування плану забезпечення безперервної роботи та відновлення функціонування | | - | |
| СР-5 | Оновлення плану забезпечення безперервної роботи та відновлення функціонування | Вилучено | | |
| СР-6 | Альтернативне місце зберігання | | ДВ-1-3 | Відновлення після збоїв |
| СР-7 | Альтернативний майданчик роботи | | ДВ-1-3<br>ДЗ-2<br>ДЗ-3 | Відновлення після збоїв<br>Обмежена гаряча заміна<br>Гаряча заміна будь-якого компонента |
| СР-8 | Комунікаційні послуги | | - | |
| СР-9 | Резервне копіювання | | ДВ-1-3 | Відновлення після збоїв |
| СР-10 | Відновлення та відтворення системи | | ДВ-1-3 | Відновлення після збоїв |
| СР-11 | Альтернативні протоколи зв’язку | | - | |
| СР-12 | Безпечний режим | | ДВ-1-3 | Відновлення після збоїв |
| СР-13 | Альтернативні механізми безпеки | | - | |
| ІДЕНТИФІКАЦІЯ І АВТЕНТИФІКАЦІЯ (ІА) | | | | |
| ІА-1 | Політика та процедури ідентифікації та автентифікації | | | 10.5 Документація |
| ІА-2 | Ідентифікація та автентифікація (користувачів організації) | | НИ-1-3 | Ідентифікація і автентифікація |
| ІА-3 | Ідентифікація і автентифікація пристроїв | | НИ-1-3 | Ідентифікація і автентифікація |
| ІА-4 | Управління ідентифікацією | | НИ-1-3 | Ідентифікація і автентифікація |
| ІА-5 | Управління автентифікатором | | НИ-1-3<br><br>НВ-1-3 | Ідентифікація і автентифікація<br>Ідентифікація і автентифікація при обміні |

| Каталог ЗЗІ та ПД | | | НД ТЗІ 2.5-004-99 | |
|---|---|---|---|---|
| Шифр | Назва | | Шифр | Назва |
| | | | НА-1-2<br>НП-1-2 | Автентифікація відправника<br>Автентифікація отримувача |
| IA-6 | Зворотний зв’язок автентифікатора | | - | |
| IA-7 | Автентифікація криптографічного модуля | | НИ-1-3<br>НВ-1-3<br>НА-1-2<br>НП-1-2 | Ідентифікація і автентифікація<br>Ідентифікація і автентифікація при обміні<br>Автентифікація відправника<br>Автентифікація отримувача |
| IA-8 | Ідентифікація та автентифікація (неорганізаційні користувачі) | | - | |
| IA-9 | Послуги ідентифікації та автентифікації | | НИ-1-3<br>НВ-1-3<br>НА-1-2<br>НП-1-2 | Ідентифікація і автентифікація<br>Ідентифікація і автентифікація при обміні<br>Автентифікація відправника<br>Автентифікація отримувача |
| IA-10 | Адаптивна автентифікація | | - | |
| IA-11 | Повторна автентифікація | | - | |
| IA-12 | Перевірка справжності (ідентичності) | IA-12 a<br>IA-12 b | НИ-1-3<br>НВ-1-3<br>НА-1-2<br>НП-1-2 | Ідентифікація і автентифікація<br>Ідентифікація і автентифікація при обміні<br>Автентифікація відправника<br>Автентифікація отримувача |
| | | IA-12 c | НВ-1-3 | Ідентифікація і автентифікація при обміні |
| РЕАГУВАННЯ НА ІНЦИДЕНТИ (IR) | | | | |
| IR-1 | Політика та процедури реагування на інциденти | IR-1 a<br>IR-1 c<br>IR-1 e | | 10.5 Документація |
| | | IR-1 b<br>IR-1 d | - | |
| IR-2 | Навчання з реагування на інциденти | | - | |
| IR-3 | Перевірка реагувань на інциденти | | - | |
| IR-4 | Обробка інциденту | IR-4 a | ДВ-1-3 | Відновлення після збоїв (у частині ліквідації та відновлення) |
| | | IR-4 b<br>IR-4 c<br>IR-4 d | - | |
| IR-5 | Моніторинг інциденту | | НР-3<br>НР-4 | Сигналізація про небезпеку<br>Детальна реєстрація |

| Каталог ЗЗІ та ПД | | | НД ТЗІ 2.5-004-99 | |
|---|---|---|---|---|
| Шифр | Назва | | Шифр | Назва |
| | | | HP-5 | Аналіз у реальному часі |
| IR-6 | Звітність про інциденти | | - | |
| IR-7 | Підтримка реагування на інциденти | | - | |
| IR-8 | План реагування на інцидент | IR-8 a<br>IR-8 b | | 10.5 Документація |
| | | IR-8 c<br>IR-8 d<br>IR-8 e | - | |
| IR-9 | Реагування на витік інформації | | - | |
| IR-10 | Інтегрована команда аналізу інформаційної безпеки | | - | |
| ТЕХНІЧНЕ ОБСЛУГОВУВАННЯ (MA) | | | | |
| MA-1 | Політика та процедури технічного обслуговування | MA-1 a<br>MA-1 b<br>MA-1 d | | 10.5 Документація |
| | | MA-1 c<br>MA-1 e | - | |
| MA-2 | Контрольоване обслуговування | | - | |
| MA-3 | Інструменти для обслуговування | | - | |
| MA-4 | Віддалене обслуговування | | - | |
| MA-5 | Технічний персонал | | - | |
| MA-6 | Своєчасне обслуговування | | - | |
| MA-7 | Технічне обслуговування в польових умовах | | - | |
| ЗАХИСТ НОСІЇВ ІНФОРМАЦІЇ (MP) | | | | |
| MP-1 | Політика та процедури щодо захисту носіїв інформації | MP-1 a<br>MP-1 e | | 10.5 Документація |
| | | MP-1 b<br>MP-1 c<br>MP-1 d | - | |
| MP-2 | Доступ до носіїв інформації | | - | |
| MP-3 | Маркування носіїв інформації | | - | |
| MP-4 | Зберігання носіїв інформації | | - | |
| MP-5 | Транспортування носіїв інформації | | - | |
| MP-6 | Знищення інформації на носіях інформації | | - | |
| MP-7 | Використання носіїв інформації | | - | |
| MP-8 | Зниження категорії безпеки носіїв інформації | | - | |
| ФІЗИЧНИЙ ЗАХИСТ І ЗАХИСТ РОБОЧОГО СЕРЕДОВИЩА (PE) | | | | |
| PE-1 | Політика та процедури фізичного захисту та захисту робочого середовища | PE-1 a<br>PE-1 c<br>PE-1 e | | 10.5 Документація |

| Каталог ЗЗІ та ПД | | | НД ТЗІ 2.5-004-99 | |
|---|---|---|---|---|
| Шифр | Назва | | Шифр | Назва |
| | | PE-1 b<br>PE-1d | - | |
| PE-2 | Авторизація фізичного доступу | | - | |
| PE-3 | Керування фізичним доступом | PE-3 b | НР-1-5 | Реєстрація |
| | | PE-3 a<br>PE-3 c<br>PE-3 d<br>PE-3 e<br>PE-3 f<br>PE-3 g | - | |
| PE-4 | Контроль доступу до джерел і ліній електроживлення | | - | |
| PE-5 | Контроль доступу для пристроїв виведення інформації | | - | |
| PE-6 | Моніторинг фізичного доступу | | - | |
| PE-7 | Контроль відвідувачів | Вилучено | | |
| PE-8 | Реєстр доступу відвідувачів | | - | |
| PE-9 | Енергетичне обладнання та кабелі | | - | |
| PE-10 | Аварійне відключення | | - | |
| PE-11 | Аварійне енергозабезпечення | | - | |
| PE-12 | Аварійне освітлення | | - | |
| PE-13 | Протипожежний захист | | - | |
| PE-14 | Контроль температури та вологості | | - | |
| PE-15 | Захист від пошкодження водою | | - | |
| PE-16 | Доставлення та видалення | | - | |
| PE-17 | Альтернативне робоче місце | | - | |
| PE-18 | Розташування компонентів системи | | - | |
| PE-19 | Витік інформації | | КК-1-3 | Аналіз прихованих каналів |
| PE-20 | Моніторинг і відстеження активів | | - | |
| PE-21 | Захист від електромагнітного імпульсу | | - | |
| PE-22 | Маркування компонентів | | - | |
| PE-23 | Розташування об’єкта | | - | |
| ПЛАНУВАННЯ БЕЗПЕКИ (PL) | | | | |
| PL-1 | Політики та процедури планування безпеки | PL-1 a<br>PL-1 d<br>PL-1 e | | 10.5 Документація |
| | | PL-1 b<br>PL-1 c | - | |
| PL-2 | Плани захисту інформації та персональних даних | | - | |

| Каталог ЗЗІ та ПД | | | НД ТЗІ 2.5-004-99 | |
|---|---|---|---|---|
| Шифр | Назва | | Шифр | Назва |
| PL-3 | Оновлення планів захисту інформації та персональних даних | Вилучено | | |
| PL-4 | Правила поведінки | | - | |
| PL-5 | Оцінювання впливу на приватність | Вилучено | | |
| PL-6 | Планування діяльності, пов'язаної з безпекою | Вилучено | | |
| PL-7 | Концепція експлуатації | | - | |
| PL-8 | Архітектура безпеки та приватності | | - | |
| PL-9 | Централізоване управління | | - | |
| PL-10 | Вибір базового профілю безпеки | | - | |
| PL-11 | Налаштування базового профілю безпеки | | Г-1-7 | Середовище функціонування |
| МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ (PM) | | | | |
| PM-1 | Програма (концепція) інформаційної безпеки | | - | |
| PM-2 | Ролі програми інформаційної безпеки | | - | |
| PM-3 | Ресурси забезпечення інформаційної безпеки та приватності | | - | |
| PM-4 | План дій та етапи | | - | |
| PM-5 | Інвентаризація системи | | - | |
| PM-6 | Показники продуктивності | | - | |
| PM-7 | Архітектура підприємства | | | |
| PM-8 | План захисту критичної інфраструктури | | - | |
| PM-9 | Стратегія управління ризиками | | - | |
| PM-10 | Процес акредитації | | - | |
| PM-11 | Визначення завдань і процесів | | - | |
| PM-12 | Програма інсайдерської загрози | | - | |
| PM-13 | Безпека та приватність працівників | | - | |
| PM-14 | Тестування, навчання та моніторинг | | - | |
| PM-15 | Контакти з групами й асоціаціями | | - | |
| PM-16 | Програма інформування про загрози | | - | |
| PM-17 | Захист публічної інформації на зовнішніх системах | | - | |
| PM-18 | Програма (концепція) забезпечення приватності | | - | |
| PM-19 | Ролі програми приватності | | - | |
| PM-20 | Система записів | | - | |

| Каталог ЗЗІ та ПД | | | НД ТЗІ 2.5-004-99 | |
|---|---|---|---|---|
| Шифр | Назва | | Шифр | Назва |
| PM-21 | Поширення інформації про програму забезпечення приватності | | - | |
| PM-22 | Облік розкриття персональних даних | | - | |
| PM-23 | Управління якістю персональних даних | | - | |
| PM-24 | Комісія з управління даними | | - | |
| PM-25 | Комісія з питань цілісності даних | | - | |
| PM-26 | Мінімізація персональних даних, що використовуються під час тестування, навчання та досліджень | | - | |
| PM-27 | Індивідуальний контроль доступу | | - | |
| PM-28 | Управління скаргами | | - | |
| PM-29 | Інвентаризація персональних даних | | - | |
| PM-30 | Звіт про приватність | | - | |
| PM-31 | План управління ризиком ланцюга постачання | | - | |
| PM-32 | Визначення ризиків | | - | |
| КАДРОВА БЕЗПЕКА (PS) | | | | |
| PS-1 | Політика та процедури кадрової безпеки | | - | |
| PS-2 | Визначення посадового ризику | | - | |
| PS-3 | Перевірка персоналу | | - | |
| PS-4 | Звільнення персоналу | | - | |
| PS-5 | Переведення персоналу | | - | |
| PS-6 | Угоди про доступ | | - | |
| PS-7 | Безпека зовнішнього персоналу | | - | |
| PS-8 | Кадрові санкції | | - | |
| PS-9 | Опис позицій | | - | |
| ПОВНОВАЖЕННЯ НА ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ (PT) | | | | |
| PT-1 | Політика та процедури обробки персональних даних | | - | |
| PT-2 | Повноваження на обробку персональних даних | | - | |
| PT-3 | Цілі обробки персональних даних | | - | |
| PT-4 | Згода на обробку персональних даних | | - | |
| PT-5 | Повідомлення про конфіденційність | | - | |

| Каталог ЗЗІ та ПД | | | НД ТЗІ 2.5-004-99 | |
|---|---|---|---|---|
| Шифр | Назва | | Шифр | Назва |
| PT-6 | Система записів повідомлень про конфіденційність | | - | |
| PT-7 | Спеціальні категорії персональних даних | | - | |
| PT-8 | Вимоги до відповідності | | - | |
| ОЦІНЮВАННЯ РИЗИКУ (RA) | | | | |
| RA-1 | Політика та процедури оцінювання ризику | | - | |
| RA-2 | Категоріювання безпеки | | - | |
| RA-3 | Оцінювання ризику | | - | |
| RA-4 | Оновлення оцінювання ризику | Вилучено | | |
| RA-5 | Сканування вразливостей | | - | |
| RA-6 | Заходи протидії технічній розвідці | | - | |
| RA-7 | Реагування на ризик | | - | |
| RA-8 | Оцінка впливу на приватність | | - | |
| RA-9 | Аналіз критичності | | - | |
| RA-10 | Активний пошук загроз | | - | |
| ПРИДБАННЯ СИСТЕМИ ТА ПОСЛУГ (SA) | | | | |
| SA-1 | Політика та процедури придбання системи та послуг | | - | |
| SA-2 | Розподіл ресурсів | | - | |
| SA-3 | Життєвий цикл розробки системи | | - | |
| SA-4 | Процес закупівель | | - | |
| SA-5 | Системна документація | | - | |
| SA-6 | Обмеження щодо використання програмного забезпечення | Вилучено | | |
| SA-7 | Встановлене користувачем програмне забезпечення | Вилучено | | |
| SA-8 | Безпека та приватність принципів інжинірингу (проєктування) | | - | |
| SA-9 | Зовнішні послуги для системи | | - | |
| SA-10 | Управління конфігурацією розробника | SA-10 b<br>SA-10 c | Г-1-7 | Середовище функціонування |
| | | SA-10 a<br>SA-10 d<br>SA-10 e | - | |
| SA-11 | Тестування та оцінювання розробника | | - | |
| SA-12 | Керування ризиками ланцюга постачання | | - | |
| SA-13 | Довірчість | Вилучено | | |

| Каталог ЗЗІ та ПД | | | НД ТЗІ 2.5-004-99 | |
|---|---|---|---|---|
| Шифр | Назва | | Шифр | Назва |
| SA-14 | Аналіз критичності | Вилучено | | |
| SA-15 | Процеси, стандарти та інструменти розробки | | - | |
| SA-16 | Навчання, що надається розробниками | | - | |
| SA-17 | Проєкт і архітектура безпеки розробника | SA-17 b<br>SA-17 c | Г-1-7 | Послідовність розробки |
| | | SA-17 a | - | |
| SA-18 | Захист і виявлення підробки | | - | |
| SA-19 | Справжність компонента | | - | |
| SA-20 | Індивідуальна розробка критичних компонентів | | - | |
| SA-21 | Перевірка розробника | | - | |
| SA-22 | Компоненти системи, що не підтримуються | | - | |
| SA-23 | Спеціалізація | | - | |
| СИСТЕМНИЙ ТА КОМУНІКАЦІЙНИЙ ЗАХИСТ (SC) | | | | |
| SC-1 | Політика та процедури захисту системи та комунікацій | SC-1 a<br>SC-1 e | | 10.5 Документація |
| | | SC-1 b<br>SC-1 c<br>SC-1 d | - | |
| SC-2 | Розділення додатків | | - | |
| SC-3 | Ізоляція функцій безпеки | | - | |
| SC-4 | Інформація в загальних ресурсах системи | | ДР-1-3<br>КО-1 | Використання ресурсів<br>Повторне використання об’єктів |
| SC-5 | Захист від атак «Відмова в обслуговуванні» | | - | |
| SC-6 | Доступність ресурсів | | ДР-1-3 | Використання ресурсів |
| SC-7 | Захист периметра | | - | |
| SC-8 | Конфіденційність та цілісність передачі | | КД-1-4<br>КА-1-4<br><br>КВ-1-4<br><br>ЦД-1-4<br>ЦА-1<br>ЦВ-1-3 | Довірча конфіденційність<br>Адміністративна конфіденційність<br>Конфіденційність при обміні<br>Довірча цілісність<br>Адміністративна цілісність<br>Цілісність при обміні |
| SC-9 | Конфіденційність передачі | Вилучено | | |
| SC-10 | Відключення мережі | | - | |
| SC-11 | Довірений канал зв’язку | SC-11 a | КД-1-4<br>КА-1-4 | Довірча конфіденційність |

| Каталог ЗЗІ та ПД | | | НД ТЗІ 2.5-004-99 | |
|---|---|---|---|---|
| Шифр | Назва | | Шифр | Назва |
| | | | КВ-1-4 | Адміністративна конфіденційність Конфіденційність при обміні |
| | | SC-11 b | НА-1-2<br>НП-1-2 | Автентифікація відправника Автентифікація отримувача |
| SC-12 | Встановлення та управління криптографічними ключами | | - | |
| SC-13 | Криптографічний захист | | - | |
| SC-14 | Захист громадського доступу | Вилучено | | |
| SC-15 | Спільні обчислювальні пристрої та застосунки | | - | |
| SC-16 | Передача атрибутів безпеки та приватності | | - | |
| SC-17 | Сертифікати інфраструктури відкритих ключів | | - | |
| SC-18 | Мобільний код | | - | |
| SC-19 | Інтернет-протокол голосового зв’язку | | | |
| SC-20 | Безпечний сервіс регулювання імені/адреси (уповноважене джерело) | | - | |
| SC-21 | Безпечний сервіс регулювання імені/адреси (рекурсивний або кешувальний перетворювач) | | - | |
| SC-22 | Архітектура та забезпечення служби імен/адрес | | - | |
| SC-23 | Автентифікація сесії | | НИ-1-3<br>НВ-1-3<br>НА-1-3<br>НП-1-2 | Ідентифікація і автентифікація Ідентифікація і автентифікація при обміні Автентифікація відправника Автентифікація отримувача |
| SC-24 | Введення у відомий стан | | - | |
| SC-25 | Тонкі вузли | | - | |
| SC-26 | Приманка для зловмисників (honeypots) | | - | |
| SC-27 | Незалежні від платформи застосунки | | - | |
| SC-28 | Захист інформації в стані спокою | | - | |
| SC-29 | Гетерогенність | | - | |
| SC-30 | Маскування та хибний напрям | | - | |
| SC-31 | Аналіз прихованого каналу | | КК-1-3 | Аналіз прихованих каналів |
| SC-32 | Поділ системи на частини | | - | |

| Каталог ЗЗІ та ПД | | | НД ТЗІ 2.5-004-99 | |
|---|---|---|---|---|
| Шифр | Назва | | Шифр | Назва |
| SC-33 | Підготовка цілісності передачі | Вилучено | | |
| SC-34 | Незмінювані виконавчі програми | | - | |
| SC-35 | Розпізнавання приманок для зловмисників (honeyclient) | | - | |
| SC-36 | Розподілена обробка та зберігання | | НЦ-2<br>НЦ-3 | КЗЗ з гарантованою цілісністю<br>КЗЗ з функціями диспетчера доступу |
| SC-37 | Позасмугові канали | | - | |
| SC-38 | Безпека операцій | | | 10.3 Послідовність розробки |
| SC-39 | Ізоляція процесу | | - | |
| SC-40 | Захист бездротового з’єднання | | - | |
| SC-41 | Доступ до портів і пристроїв введення/виведення | | - | |
| SC-42 | Можливості датчика та дані | | - | |
| SC-43 | Обмеження використання | | ДР-1-3 | Використання ресурсів |
| SC-44 | Екрановані камери | | - | |
| SC-45 | Синхронізація системи з часом | | - | |
| SC-46 | Забезпечення виконання міждоменної політики | | - | |
| SC-47 | Альтернативний шлях зв'язку | | - | |
| SC-48 | Переміщення датчика | | - | |
| SC-49 | Примусове апаратне розділення та політика забезпечення виконання | | - | |
| SC-50 | Примусове програмне розділення та політика забезпечення виконання | | - | |
| SC-51 | Апаратний захист | | - | |
| ЦІЛІСНІСТЬ СИСТЕМИ ТА ІНФОРМАЦІЇ (SI) | | | | |
| SI-1 | Політика та процедури цілісності інформації | SI-1 a (перше)<br>SI-1 d | | 10.5 Документація |
| | | SI-1 a (друге)<br>SI-1 b<br>SI-1 c | - | |
| SI-2 | Виправлення дефектів | | - | |
| SI-3 | Захист від шкідливого коду | | - | |
| SI-4 | Моніторинг системи | | - | |
| SI-5 | Попередження, рекомендації та директиви з безпеки | | - | |
| SI-6 | Перевірка функцій безпеки та приватності | | НТ-1-3 | Самотестування |

| Каталог ЗЗІ та ПД | | | НД ТЗІ 2.5-004-99 | |
|---|---|---|---|---|
| Шифр | Назва | | Шифр | Назва |
| SI-7 | Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації | | НТ-1-3 | Самотестування |
| SI-8 | Захист від спаму | | - | |
| SI-9 | Обмеження на введення інформації | Вилучено | | |
| SI-10 | Перевірка вводу інформації | | - | |
| SI-11 | Обробка помилок | | ДС-1-3 | Стійкість до відмов |
| SI-12 | Управління та збереження інформації | | - | |
| SI-13 | Передбачуване запобігання збоям | | - | |
| SI-14 | Нестійкість | | - | |
| SI-15 | Фільтрація вихідних даних | | - | |
| SI-16 | Захист пам’яті | | КО-1 | Повторне використання об’єктів |
| SI-17 | Відмовостійкі процедури | | ДС-1-3<br>ДВ-1-3 | Стійкість до відмов<br>Відновлення після збоїв |
| SI-18 | Операції забезпечення якості даних | | - | |
| SI-19 | Деідентифікація | | - | |
| SI-20 | Псування | | - | |
| SI-21 | Оновлення інформації | | - | |
| SI-22 | Різновиди інформації | | - | |
| SI-23 | Фрагментація інформації | | - | |
| УПРАВЛІННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ(SR) | | | | |
| SR-1 | Політика та процедури управління ризиками ланцюга постачання | | - | |
| SR-2 | План управління ризиками ланцюга постачання | | - | |
| SR-3 | Контроль ланцюга постачання і процесів | | - | |
| SR-4 | Походження | | - | |
| SR-5 | Стратегії придбання, інструменти і методи | | - | |
| SR-6 | Оцінка постачальників | | - | |
| SR-7 | Безпека операцій ланцюга постачання | | - | |
| SR-8 | Повідомлення про порушення ланцюга постачання | | - | |
| SR-9 | Захист від злому та виявлення | | - | |
| SR-10 | Перевірка системи та компонентів системи | | - | |
| SR-11 | Автентичність компоненту | | - | |

| Каталог ЗЗІ та ПД | | | НД ТЗІ 2.5-004-99 | |
|---|---|---|---|---|
| Шифр | Назва | | Шифр | Назва |
| SR-12 | Утилізація компоненту | | - | |