НОРМАТИВНИЙ ДОКУМЕНТ
СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем

НД ТЗІ 2.3-025-24

Том 3

Додаток А
Методика оцінювання груп заходів захисту класів PL, PM, PS, PT, RA, SA, SC, SI та SR

Адміністрація Держспецзв’язку

Київ 2024

Додаток А

В додатку А тому 3 подається методика оцінювання заходів захисту для інформаційних систем (ІС) та інформації в державних органах, на підприємствах, в організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої визначена в законі та не становить державної таємниці, а саме класи: PL, PM, PS, PT, RA, SA, SC, SI та SR на наступних сторінках:

XII. КЛАС ЗАХОДІВ ЗАХИСТУ PL – ПЛАНУВАННЯ БЕЗПЕКИ

PL-1	**ПОЛІТИКИ ТА ПРОЦЕДУРИ ПЛАНУВАННЯ БЕЗПЕКИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PL-01_ODP[01]	**визначено персонал або ролі, до яких має бути доведена політика планування безпеки;**
	PL-01_ODP[02]	**визначено персонал або ролі, на які поширюватимуться процедури планування безпеки;**
	PL-01_ODP[03]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {рівень організації; рівень місії/бізнес-процесу; рівень системи};**
	PL-01_ODP[04]	**визначено посадову особу, яка керуватиме політикою та процедурами планування безпеки;**
	PL-01_ODP[05]	**визначено періодичність перегляду та оновлення поточної політики планування безпеки;**
	PL-01_ODP[06]	**є події, які потребують перегляду та оновлення поточної політики планування безпеки;**
	PL-01_ODP[07]	**визначена частота, з якою переглядаються та оновлюються поточні процедури планування безпеки;**
	PL-01_ODP[08]	**є події, які потребують перегляду та оновлення процедур планування безпеки;**
	PL-01a.[01]	розроблена та задокументована політика планування безпеки.
	PL-01a.[02]	поширюється політика планування безпеки на **<PL-01_ODP[01] персонал або ролі>**;
	PL-01a.[03]	розроблені та задокументовані процедури планування безпеки, що сприяють впровадженню політики планування та пов'язаних з нею засобів контролю планування;
	PL-01a.[04]	поширюються процедури планування безпеки на **<PL-01_ODP[02] персонал або ролі>**;
	PL-01a.01(a)[01]	відповідає політика планування безпеки **<PL-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** меті;
	PL-01a.01(a)[02]	політика планування безпеки **<PL-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** враховує сферу застосування;
	PL-01a.01(a)[03]	**<PL-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** політика планування звертається до ролей;
	PL-01a.01(a)[04]	політика планування безпеки <**PL-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** стосується обов'язків;
	PL-01a.01(a)[05]	політика планування безпеки **<PL-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** враховує зобов'язання керівництва;

	PL-01a.01(a)[06]	політика планування безпеки **<PL-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** передбачає координацію між організаційними одиницями;
	PL-01a.01(a)[07]	політика планування безпеки **<PL-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** стосується комплаєнсу;
	PL-01a.01(b)	відповідає політика планування безпеки **<PL-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** чинному законодавству, виконавчим наказам, директивам, положенням, політикам, стандартам і настановам;
	PL-01b.	призначений персонал організації з планування безпки **<PL-01_ODP[04] посадова особа>** для управління розробкою, документуванням та розповсюдженням політики та процедур планування;
	PL-01c.01[01]	переглядається та оновлюється поточна політика планування безпеки **<PL-01_ODP[05] частота>**;
	PL-01c.01[02]	переглядається та оновлюється поточна політика планування після **<PL-01_ODP[06] подій>**;
	PL-01c.02[01]	переглядаються та оновлюються поточні процедури планування **<PL-01_ODP[07] частота>**;
	PL-01c.02[02]	переглядаються та оновлюються поточні процедури планування безпеки після **<PL-01_ODP[08] подій>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика та процедури планування; план захисту інформації системи; план забезпечення конфіденційності; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за планування; персонал організації, відповідальний за інформаційну безпеку та конфіденційність].	

PL-2	**ПЛАНИ ЗАХИСТУ ІНФОРМАЦІЇ ТА ПЕРСОНАЛЬНИХ ДАНИХ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PL-02_ODP[01]	**призначені особи або групи, з якими пов'язана діяльність з безпекою та конфіденційністю, що впливає на систему, яка потребує планування та координації;**
	PL-02_ODP[02]	**призначено персонал або ролі для отримання розповсюджуваних копій планів захисту інформації та конфіденційності системи;**
	PL-02_ODP[03]	**визначено періодичність перегляду планів захисту інформації та конфіденційності системи;**
	PL-02a.01[01]	розроблено план захисту інформації, який відповідає архітектурі підприємства організації;

	PL-02a.01[02]	розроблено план конфіденційності для системи, який відповідає архітектурі підприємства організації;
	PL-02a.02[01]	розроблено план захисту інформації, який чітко визначає складові компоненти системи;
	PL-02a.02[02]	розроблено для системи план забезпечення конфіденційності, який чітко визначає складові компоненти системи;
	PL-02a.03[01]	розроблено план захисту інформації системи, який описує операційний контекст системи з точки зору місії та бізнес-процесів;
	PL-02a.03[02]	розроблено для системи план забезпечення конфіденційності, який описує операційний контекст системи з точки зору місії та бізнес-процесів;
	PL-02a.04[01]	розроблено план захисту інформації, який визначає осіб, що виконують системні ролі та обов'язки;
	PL-02a.04[02]	розроблено для системи план забезпечення конфіденційності, який визначає осіб, що виконують ролі та обов'язки в системі;
	PL-02a.05[01]	розроблено план захисту інформації, який визначає типи інформації, що обробляється, зберігається та передається системою;
	PL-02a.05[02]	розроблено план конфіденційності для системи, який визначає типи інформації, що обробляється, зберігається та передається системою;
	PL-02a.06[01]	розроблено план захисту інформації, який передбачає категоризацію безпеки системи, включаючи відповідне обґрунтування;
	PL-02a.06[02]	розроблено для системи план забезпечення конфіденційності, який передбачає категоризацію системи за рівнем безпеки, включаючи обґрунтування;
	PL-02a.07[01]	розроблено план захисту інформації, який описує будь-які конкретні загрози для системи, що викликають потенційні ризики для рганізації;
	PL-02a.07[02]	розроблено план конфіденційності для системи, який описує будь-які конкретні загрози для системи, що викликають потенційні ризики для організації;
	PL-02a.08[01]	розроблено план захисту інформації, який містить результати оцінки ризиків конфіденційності для систем, що обробляють інформацію, яка ідентифікує особу;
	PL-02a.08[02]	розроблено для системи план забезпечення конфіденційності, який містить результати оцінки ризиків конфіденційності для систем, що обробляють інформацію, яка ідентифікує особу;
	PL-02a.09[01]	розроблено план захисту інформації, який описує операційне середовище системи та будь-які залежності або зв'язки з іншими системами чи компонентами системи;

	PL-02a.09[02]	розроблено для системи план забезпечення конфіденційності, який описує робоче середовище системи та будь-які залежності або зв'язки з іншими системами чи компонентами системи;
	PL-02a.10[01]	розроблено план захисту інформації, який містить огляд вимог до безпеки системи;
	PL-02a.10[02]	розроблено для системи план забезпечення конфіденційності, який містить огляд вимог до конфіденційності системи;
	PL-02a.11[01]	розроблено план захисту інформації, який визначає будь-які відповідні базові рівні контролю або обмеження, якщо такі є;
	PL-02a.11[02]	розроблено для системи план забезпечення конфіденційності, який визначає будь-які відповідні базові рівні контролю або обмеження, якщо такі є;
	PL-02a.12[01]	розроблено план захисту інформації, який описує наявні або заплановані засоби контролю для виконання вимог безпеки, включаючи обґрунтування будь-яких рішень щодо адаптації;
	PL-02a.12[02]	розроблено для системи план забезпечення конфіденційності, який описує наявні або заплановані засоби контролю для виконання вимог щодо конфіденційності, включаючи обґрунтування будь-яких рішень, пов'язаних з адаптацією;
	PL-02a.13[01]	розроблено план захисту інформації, який включає визначення ризиків для архітектури безпеки та проектних рішень;
	PL-02a.13[02]	розроблено план забезпечення конфіденційності для системи, який включає визначення ризиків для архітектури конфіденційності та проектних рішень;
	PL-02a.14[01]	розроблено захисту інформації, який включає діяльність, пов'язану з безпекою, що впливає на систему і потребує планування та координації з **<PL-02_ODP[01] окремими особами або групами>**;
	PL-02a.14[02]	розроблено для системи план забезпечення конфіденційності, який включає діяльність, пов'язану з конфіденційністю, що впливає на систему і потребує планування та координації з **<PL-02_ODP[01] окремими особами або групами>**;
	PL-02a.15[01]	розроблено план захисту інформації, який розглядається та затверджується уповноваженою посадовою особою або призначеним представником до початку реалізації плану;
	PL-02a.15[02]	розроблено план забезпечення конфіденційності для системи, який перевіряється та затверджується уповноваженою посадовою особою або призначеним представником перед впровадженням плану.
	PL-02b.[01]	розповсюджуються копії планів серед **<PL-02_ODP[02] персонал або ролі>**;
	PL-02b.[02]	повідомляються наступні зміни до планів **<PL-02_ODP[02] персонал або ролі>**;
	PL-02c.	переглядаються плани **<PL-02_ODP[03] частота>**;

	PL-02d.[01]	оновлюються плани відповідно до змін у системі та середовищі діяльності;
	PL-02d.[02]	оновлюються плани для вирішення проблем, виявлених під час реалізації плану;
	PL-02d.[03]	оновлюються плани для вирішення проблем, виявлених під час контрольних оцінок;
	PL-02e.[01]	захищені плани від несанкціонованого розголошення;
	PL-02e.[02]	захищені плани від несанкціонованої модифікації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР Політика планування безпеки; процедури, що стосуються розробки та реалізації плану захисту інформації; процедури, що стосуються огляду та оновлення планів захисту інформації; документація з архітектури підприємства; план захисту інформації системи; записи оглядів та оновлень планів захисту інформації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за планування безпеки та виконання плану; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для розробки, перегляду, оновлення, затвердження плану захисту інформації; автоматизовані механізми, що підтримують план захисту інформації системи].	

PL-2(1)	**КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - ДИВЕРСИФІКАЦІЯ ПОСТАЧАЛЬНИКІВ**
	[Вилучено: включено до PL-7]

PL-2(2)	**ПЛАНИ ЗАХИСТУ ІНФОРМАЦІЇ ТА ПЕРСОНАЛЬНИХ ДАНИХ - ФУНКЦІОНАЛЬНА АРХІТЕКТУРА**
	[Вилучено: включено до PL-8].

PL-3	**ОНОВЛЕННЯ ПЛАНІВ ЗАХИСТУ ІНФОРМАЦІЇ ТА ПЕРСОНАЛЬНИХ ДАНИХ**
	[Вилучено: включено до PL-2]

PL-4	**ПРАВИЛА ПОВЕДІНКИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PL-04_ODP[01]	**визначено періодичність перегляду та оновлення правил поведінки;**
	PL-04_ODP[02]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРА:{<PL-04_ODP[03] частота>; коли правила переглядаються або оновлюються};**
	PL-04_ODP[03]	**визначена періодичність перегляду та повторного**

		підтвердження правил поведінки (якщо вибрано);
	PL-04a.[01]	встановлені правила, які описують обов'язки та очікувану поведінку щодо використання інформації та системи, безпеки та конфіденційності для осіб, яким потрібен доступ до системи;
	PL-04a.[02]	надаються правила, які описують обов'язки та очікувану поведінку щодо використання інформації та системи, безпеки та конфіденційності, особам, які отримують доступ до системи;
	PL-04b.	отримано перед наданням доступу до інформації та системи задокументоване підтвердження від таких осіб про те, що вони прочитали, зрозуміли та згодні дотримуватися правил поведінки;
	PL-04c.	переглядаються та оновлюються правила поведінки **<PL-04_ODP[01] частота>**;
	PL-04d.	потрібно особам, які визнали попередню версію правил поведінки, прочитати та повторно визнати **<PL-04_ODP[02] ЗНАЧЕННЯ ВИБРАНОГО ПАРАМЕТРА(ів)>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування безпеки; процедури, що стосуються правил поведінки користувачів системи; правила поведінки; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за встановлення, перегляд та оновлення правил поведінки; персонал організації, який є уповноваженими користувачами системи та має підписані правила поведінки; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для встановлення правил поведінки; автоматизовані механізми підтримки та, або реалізації встановлення правил поведінки].	

PL-4(1)	**ПРАВИЛА ПОВЕДІНКИ - ОБМЕЖЕННЯ НА СОЦІАЛЬНІ МЕДІА ТА МЕРЕЖУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PL-04(01)(a)	включають правила поведінки обмеження на використання соціальних медіа, соціальних мереж та зовнішніх сайтів/додатків;
	PL-04(01)(b)	включають правила поведінки обмеження на розміщення інформації про організацію на публічних веб-сайтах;
	PL-04(01)(c)	включають правила поведінки обмеження на використання наданих організацією ідентифікаторів (наприклад, адрес електронної пошти) та секретів автентифікації (наприклад, паролів) для створення облікових записів на зовнішніх сайтах/додатках.

	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування безпеки; процедури, що стосуються правил поведінки користувачів системи; правила поведінки; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за встановлення, перегляд та оновлення правил поведінки; персонал організації, який є уповноваженими користувачами системи та має підписані правила поведінки; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для встановлення правил поведінки; автоматизовані механізми підтримки та, або реалізації встановлення правил поведінки].

PL-5	**ОЦІНКА 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**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PL-07_ODP	**визначена періодичність перегляду та оновлення концепцію експлуатації системи;**
	PL-07a.	розроблено концепцію експлуатації системи, що описує, як організація має намір експлуатувати систему з точки зору інформаційної безпеки та конфіденційності;
	PL-07b.	переглядається та оновлюється концепція експлуатації системи **<PL-07_ODP частота>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування безпеки; процедури, що стосуються розробки концепції експлуатації; процедури, що стосуються огляду та оновлення системи концепції експлуатації; захист концепції експлуатації для системи; план захисту інформації системи; записи про огляди та оновлення концепції експлуатації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за планування безпеки та виконання плану; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для розробки, перегляду та оновлення системи безпеки концепції експлуатації; автоматизовані механізми, що підтримують та, або впроваджують розробку, огляд та оновлення системи безпеки концепції експлуатації].	

PL-8	**АРХІТЕКТУРА БЕЗПЕКИ ТА ПРИВАТНОСТІ**

	МЕТА ОЦІНКИ: Визначити, чи:	
	PL-08_ODP	**потрібно переглядати та оновлювати частоту, щоб відображати зміни в архітектурі підприємства;**
	PL-08a.01	описує архітектура безпеки системи вимоги та підходи до захисту конфіденційності, цілісності та доступності організаційної інформації;
	PL-08a.02	описує архітектура конфіденційності вимоги та підходи до обробки персональних даних з метою мінімізації ризиків для приватного життя людей;
	PL-08a.03[01]	описує архітектура безпеки системи те, як вона інтегрована в архітектуру підприємства та підтримує її;
	PL-08a.03[02]	описує архітектура конфіденційності системи те, як вона інтегрована в архітектуру підприємства та підтримує її;
	PL-08a.04[01]	описує архітектура безпеки системи будь-які припущення та залежності від зовнішніх систем та сервісів;
	PL-08a.04[02]	описує архітектура конфіденційності системи будь-які припущення та залежності від зовнішніх систем і сервісів;
	PL-08b.	переглядаються та оновлюються зміни в архітектурі підприємства **<PL-08_ODP частота>** для відображення змін в архітектурі підприємства;
	PL-08c.[01]	заплановані зміни в архітектурі відображені в плані безпеки;
	PL-08c.[02]	відображені заплановані зміни в архітектурі в плані конфіденційності;
	PL-08c.[03]	заплановані зміни архітектури відображені в Концепції діяльності концепції експлуатації системи;
	PL-08c.[04]	заплановані зміни в архітектурі відображені в аналізі критичності;
	PL-08c.[05]	відображені заплановані зміни архітектури в організаційних процедурах;
	PL-08c.[06]	заплановані зміни в архітектурі відображаються на закупівлях та придбанні.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування безпеки та конфіденційності; процедури розробки архітектури інформаційної безпеки та конфіденційності; процедури перегляду та оновлення архітектури інформаційної безпеки та конфіденційності; документація з архітектури підприємства; документація з архітектури інформаційної безпеки та конфіденційності; план захисту інформації системи; план конфіденційності; концепція експлуатації системи з безпеки та конфіденційності для системи; записи про перегляд та оновлення архітектури інформаційної безпеки та конфіденційності; інші відповідні документи або записи].	

	Співбесіда: [ВИБІР: Персонал організації, відповідальний за планування безпеки та конфіденційності та впровадження планів; персонал організації, відповідальний за розробку архітектури інформаційної безпеки та конфіденційності; персонал організації, відповідальний за інформаційну безпеку та конфіденційність]. **Перевірка:** [ВИБІР: Процеси організації розробки, перегляду та оновлення архітектури інформаційної безпеки та конфіденційності; механізми підтримки та/або реалізації розробки, перегляду та оновлення архітектури інформаційної безпеки та конфіденційності].

PL-8(1)	**АРХІТЕКТУРА БЕЗПЕКИ ТА ПРИВАТНОСТІ - «ГЛИБОКА ОБОРОНА»**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PL-08(01)_ODP[01]	**визначені елементи керування, що підлягають розподілу;**
	PL-08(01)_ODP[02]	**визначені місця та архітектурні рівні;**
	PL-08(01)(a)[01]	архітектура безпеки системи розроблена з використанням підходу «глибокої оборони», який розподіляє **<PL-08(01)_ODP[01] елементи керування>** за **<PL-08(01)_ODP[02] місцями та архітектурними рівнями>**;
	PL-08(01)(a)[02]	архітектура конфіденційності системи розроблена з використанням підходу глибокого захисту, який розподіляє **<PL-08(01)_ODP[01] елементи керування>** за **<PL-08(01)_ODP[02] місцями та архітектурними рівнями>**;
	PL-08(01)(b)[01]	архітектура безпеки системи розроблена з використанням підходу «глибокої оборони», який гарантує, що виділені засоби контролю працюють скоординовано і взаємно підсилюють один одного;
	PL-08(01)(b)[02]	архітектура конфіденційності системи розроблена з використанням підходу «глибокої оборони», який гарантує, що виділені засоби контролю працюють скоординовано і взаємно підкріплюють один одного.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування безпеки; процедури, що стосуються розвитку архітектури інформаційної безпеки; документація з архітектури підприємства; документація архітектури інформаційної безпеки; план захисту інформації системи; захист концепції експлуатації для системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за планування безпеки та виконання плану; персонал організації, відповідальний за розробку архітектури інформаційної безпеки; персонал організації, який відповідає за придбання; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для отримання гарантій захисту	

	інформації від різних постачальників].

PL-8(2)	**АРХІТЕКТУРА БЕЗПЕКИ ТА ПРИВАТНОСТІ - РІЗНОМАНІТНІСТЬ ПОСТАЧАЛЬНИКІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PL-08(02)_ODP[01]	**визначені елементи керування, що підлягають розподілу;**
	PL-08(02)_ODP[02]	**визначені локації та архітектурні рівні;**
	PL-08(02)	потрібно отримувати **<PL-08(02)_ODP[01] елементи керування>**, призначені для **<PL-08(02)_ODP[02] локацій та архітектурних рівнів>**, від різних постачальників.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування безпеки; процедури, що стосуються розвитку архітектури інформаційної безпеки; документація з архітектури підприємства; документація архітектури інформаційної безпеки; план захисту інформації системи; захист концепції експлуатації для системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за планування безпеки та виконання плану; персонал організації, відповідальний за розробку архітектури інформаційної безпеки; персонал організації, який відповідає за придбання; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для отримання гарантій захисту інформації від різних постачальників].	

PL-9	**ЦЕНТРАЛІЗОВАНЕ УПРАВЛІННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PL-09_ODP	**визначені засоби контролю безпеки та конфіденційності і пов'язані з ними процеси, якими слід централізовано керувати;**
	PL-09	здійснюється централізоване управління **<PL-09_ODP контролями та пов'язаними з ними процесами>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування безпеки; процедури, що стосуються розробки та реалізації плану захисту інформації; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за планування безпеки та виконання плану; персонал організації, відповідальний за планування,	

	реалізацію центрального управління контролем безпеки та супутніми процесами; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для централізованого управління системами контролю безпеки та пов'язаними з ними процесами; автоматизовані механізми, що підтримують та, або впроваджують централізоване управління контролем безпеки та супутніми процесами].

PL-10	**ВИБІР БАЗОВОГО ПРОФІЛЮ БЕЗПЕКИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PL-10	вибрано базовий профіль безпеки для системи.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування безпеки та конфіденційності; процедури розробки та впровадження плану захисту інформації та конфіденційності системи; процедури перегляду та оновлення плану захисту інформації та конфіденційності системи; проектна документація системи; документація з архітектури та конфігурації системи; рішення про категоризацію системи; типи інформації, що зберігається, передається та обробляється системою; інформація про елементи/компоненти системи; аналіз потреб зацікавлених сторін; перелік вимог щодо безпеки та конфіденційності, що висуваються до системи, елементів системи та середовища функціонування; перелік контрактних вимог, що висуваються до зовнішніх постачальників системи або елемента системи; аналіз впливу на бізнес або аналіз критичності; оцінка ризиків; стратегія управління ризиками; організаційна політика безпеки та конфіденційності; затверджені або санкціоновані на федеральному рівні або на рівні організації базові рівні або накладки; план захисту інформації системи; план конфіденційності; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за планування безпеки та конфіденційності та впровадження планів; персонал організації, відповідальний за інформаційну безпеку та конфіденційність; персонал організації, відповідальний за діяльність з управління ризиками в організації].	

PL-11	**НАЛАШТУВАННЯ БАЗОВОГО ПРОФІЛЮ БЕЗПЕКИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PL-11	налаштуватовано вибраний базовий профіль безпеки, застосовуючи вказані дії для налаштування.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика планування безпеки та конфіденційності; процедури розробки та впровадження плану захисту інформації та конфіденційності системи; процедури перегляду та оновлення плану захисту інформації та конфіденційності системи; проектна документація системи;	

	документація з архітектури та конфігурації системи; рішення про категоризацію системи; типи інформації, що зберігається, передається та обробляється системою; інформація про елементи/компоненти системи; аналіз потреб зацікавлених сторін; перелік вимог щодо безпеки та конфіденційності, що висуваються до системи, елементів системи та середовища функціонування; перелік контрактних вимог, що висуваються до зовнішніх постачальників системи або елемента системи; аналіз впливу на бізнес або аналіз критичності; оцінка ризиків; стратегія управління ризиками; організаційна політика безпеки та конфіденційності; затверджені або санкціоновані на федеральному рівні або на рівні організації базові рівні або накладки; план захисту інформації системи; план конфіденційності; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за планування безпеки та конфіденційності та впровадження планів; персонал організації, відповідальний за інформаційну безпеку та конфіденційність; персонал організації, відповідальний за діяльність з управління ризиками в організації].

XIII. КЛАС ЗАХОДІВ ЗАХИСТУ PM – МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

PM-1	**ПРОГРАМА (КОНЦЕПЦІЯ) ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PM-01_ODP[01]	**визначено періодичність перегляду та оновлення плану програми (концепції) з інформаційної безпеки в масштабах всієї організації;**
	PM-01_ODP[02]	**визначені події, які спричиняють перегляд та оновлення загальноорганізаційного плану програми (концепції) з інформаційної безпеки;**
	PM-01a.[01]	розроблено план програми (концепцію) з інформаційної безпеки для всієї організації;
	PM-01a.[02]	поширено план програми (концепцію) з інформаційної безпеки;
	PM-01a.01[01]	містить план програми (концепція) з інформаційної безпеки огляд вимог до програми безпеки;
	PM-01a.01[02]	містить план програми (концепція) з інформаційної безпеки опис наявних або запланованих засобів управління програмою безпеки для виконання цих вимог;
	PM-01a.01[03]	містить план програми (концепція) з інформаційної безпеки опис загальних засобів контролю, що існують або заплановані для виконання цих вимог;
	PM-01a.02[01]	передбачає план програми (концепція) з інформаційної безпеки визначення та розподіл ролей
	PM-01a.02[02]	включає план програми (концепція) з інформаційної безпеки визначення та розподіл обов'язків;
	PM-01a.02[03]	включає план програми (концепція) з інформаційної безпеки визначення та розподіл обов'язків;
	PM-01a.02[04]	передбачена в плані програми (концепції) з інформаційної безпеки координація між підрозділами організації;
	PM-01a.02[05]	передбачено в плані програми (концепції) з інформаційної безпеки питання відповідності нормативним вимогам;
	PM-01a.03	відображає план програми (концепція) з інформаційної безпеки координацію між підрозділами організації, відповідальними за інформаційну безпеку;
	PM-01a.04	затверджено план програми (концепцію) з інформаційної безпеки вищою посадовою особою, яка несе відповідальність та підзвітність за ризики, що загрожує діяльності організації (включаючи місії, функції, імідж та репутацію), активам організації, окремим особам, іншим організаціям та державі в цілому;

	PM-01b.[01]	переглядається та оновлюється план програми (концепція) з інформаційної безпеки <**PM-01_ODP[01] частота**>;
	PM-01b.[02]	переглядається та оновлюється план програми (концепція) з інформаційної безпеки після <**PM-01_ODP[02] подій**>;
	PM-01c.[01]	захищений план програми (концепція) з інформаційної безпеки від несанкціонованого розголошення;
	PM-01c.[02]	захищений план програми (концепція) з інформаційної безпеки від несанкціонованої модифікації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: План програми інформаційної безпеки; процедури, що стосуються розробки та реалізації плану програми; процедури, що стосуються огляду та оновлення програмних планів; процедури, що стосуються координації плану програми з відповідними структурами; процедури затвердження програмних планів; записи оглядів та оновлень програмних планів; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для розробки, перегляду, оновлення, затвердження плану програм інформаційної безпеки; автоматизовані механізми підтримки та, або реалізації плану програми інформаційної безпеки].	

PM-2	**РОЛІ ПРОГРАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PM-02[01]	призначено старшу посадову особу з питань інформаційної безпеки в установі;
	PM-02[02]	надано посадовій особі з інформаційної безпеки відомства повноваження та ресурси для координації загальноорганізаційної програми (концепції) з інформаційної безпеки;
	PM-02[03]	має старша посадова особа з питань інформаційної безпеки відомства місію та ресурси для розробки загальноорганізаційної програми інформаційної безпеки;
	PM-02[04]	забезпечено старшу посадову особу з інформаційної безпеки відомства необхідним та ресурсами для впровадження загальноорганізаційної програми інформаційної безпеки;
	PM-02[05]	забезпечено старшу посадову особу з інформаційної безпеки відомства необхідним та ресурсами для підтримки загальноорганізаційної програми (концепції) з інформаційної безпеки.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ:	

	Дослідження: [ВИБІР: План програми інформаційної безпеки; процедури, що стосуються розробки та реалізації плану програми; процедури, що стосуються огляду та оновлення програмних планів; процедури, що стосуються координації плану програми з відповідними структурами; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; старший працівник інформаційної безпеки; персонал організації, який відповідає за інформаційну безпеку].

PM-3	**РЕСУРСИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ПРИВАТНОСТІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PM-03a.[01]	включені ресурси, необхідні для реалізації програми (концепції) з інформаційної безпеки, до капітального планування та інвестиційних запитів, а всі винятки задокументовані;
	PM-03a.[02]	включені ресурси, необхідні для реалізації програми забезпечення конфіденційності, в капітальне планування та інвестиційні запити, а всі винятки задокументовані;
	PM-03b.[01]	підготовлена документація, необхідна для врахування програми (концепції) з інформаційної безпеки в капітальному плануванні та інвестиційних запитах, відповідно до чинних законів, виконавчих наказів, директив, політик, положень, стандартів;
	PM-03b.[02]	підготовлена документація, необхідна для врахування програми конфіденційності в капітальному плануванні та інвестиційних запитах, відповідно до чинних законів, виконавчих наказів, директив, політик, нормативних актів, стандартів;
	PM-03c.[01]	виділяються ресурси на інформаційну безпеку відповідно до запланованих витрат;
	PM-03c.[02]	виділяються ресурси на забезпечення конфіденційності відповідно до запланованих витрат.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: План програми інформаційної безпеки; приклади для планування капіталу та інвестицій; процедури планування капіталу та інвестицій; документація про винятки з вимог капітального планування; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за планування програм інформаційної безпеки; персонал організації, відповідальний за планування капіталу та інвестиції; персонал організації, який відповідає за інформаційну безпеку].	

	Перевірка: [ВИБІР: Процеси організації для планування капіталу та інвестицій; автоматизовані механізми, що підтримують процес планування реалізації програми інформаційної безпеки та приватності].

PM-4	**ПЛАН ДІЙ ТА ЕТАПИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PM-04a.01[01]	існує процес, що забезпечує розробку планів дій та етапів для програми з інформаційної безпеки та пов'язаних з нею організаційних систем;
	PM-04a.01[02]	існує процес, який забезпечує підтримку планів дій та етапів програми з інформаційної безпеки та пов'язаних з нею організаційних систем;
	PM-04a.01[03]	існує процес, що забезпечує розробку планів дій та етапів для програми конфіденційності та пов'язаних з нею організаційних систем;
	PM-04a.01[04]	існує процес, який забезпечує підтримку планів дій та етапів для програми конфіденційності та пов'язаних з нею організаційних систем;
	PM-04a.01[05]	існує процес, що забезпечує розробку планів дій та етапів для програми управління ризиками ланцюга постачання та пов'язаних з нею організаційних систем;
	PM-04a.01[06]	існує процес, який забезпечує дотримання планів дій та етапів програми управління ризиками ланцюга поставок та пов'язаних з нею організаційних систем;
	PM-04a.02[01]	існує процес, який гарантує, що плани дій та етапи програми з інформаційної безпеки та пов'язані з нею системи організації документують коригувальні заходи з управління ризиками інформаційної безпеки для адекватного реагування на ризики для операцій та активів організації, окремих осіб, інших організацій та держави;
	PM-04a.02[02]	існує процес, який гарантує, що плани дій та етапи програми з забезпечення конфіденційності та пов'язані з нею системи організації документують коригувальні дії з управління ризиками конфіденційності для адекватного реагування на ризики для операцій та активів організації, окремих осіб, інших організацій та держави;
	PM-04a.02[03]	існує процес, який гарантує, що плани дій та етапи програми з управління ризиками ланцюга постачання та пов'язані з нею системи організації документують коригувальні заходи з управління ризиками ланцюга постачання для адекватного реагування на ризики для операцій та активів організації, окремих осіб, інших організацій та держави;

	PM-04a.03[01]	існує процес, який гарантує, що плани дій та основні етапи програм з управління ризиками інформаційної безпеки та пов'язаних з ними організаційних систем звітуються відповідно до встановлених вимог до звітності;
	PM-04a.03[02]	існує процес, який гарантує, що плани дій та основні етапи програм з управління ризиками для приватності та пов'язаних з ними організаційних систем звітуються відповідно до встановлених вимог до звітності;
	PM-04a.03[03]	існує процес, який гарантує, що плани дій та основні етапи програм з управління ризиками ланцюга постачання та пов'язані з ними системи організації звітуються відповідно до встановлених вимог до звітності;
	PM-04b.[01]	переглядаються плани дій та проміжні результати на предмет відповідності стратегії управління ризиками організації;
	PM-04b.[02]	переглядаються плани дій та етапи на предмет відповідності загальноорганізаційним пріоритетам реагування на ризики.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: План програми інформаційної безпеки; плани дій та етапи; процедури, що стосуються планів дій та етапів розробки та обслуговування; процедури, що стосуються планів дій та звітування про етапи; процедури перегляду планів дій та етапів для узгодження зі стратегією управління ризиками та пріоритетами реагування на ризик; результати оцінки ризику, пов'язані з планами дій та етапами; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за розробку, підтримку, перегляд та звітування про плани дій та етапи; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для розробки плану дій та етапів, огляду, супроводу, звітності; автоматизовані механізми, що підтримують плани дій та етапи].	

PM-5	**ІНВЕНТАРИЗАЦІЯ СИСТЕМИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PM-05_ODP	**визначена періодичність оновлення переліку систем організації;**
	PM-05[01]	розроблено перелік систем організації;
	PM-05[02]	оновлюється перелік систем організації **<PM-05_ODP frequency>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: План програми інформаційної безпеки; інвентаризація системи; процедури, що стосуються розробки та обслуговування інвентаризації	

	системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; персонал організації, відповідальний за розробку та ведення інвентаризації системи; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації з розробки та обслуговування інвентаризації системи; автоматизовані механізми підтримки інвентаризації системи].

PM-5(1)	**ІНВЕНТАРИЗАЦІЯ СИСТЕМИ - ІНВЕНТАРИЗАЦІЯ ПЕРСОНАЛЬНИХ ДАНИХ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PM-05(01)_ODP	**визначено періодичність оновлення інвентаризації систем, додатків та проектів, які обробляють інформацію, що ідентифікує особу;**
	PM-05(01)[01]	проведено інвентаризацію всіх систем, додатків та проектів, які обробляють персональну інформацію;
	PM-05(01)[02]	ведеться інвентаризація всіх систем, додатків та проектів, які обробляють персональну інформацію;
	PM-05(01)[03]	оновлюється інвентаризація всіх систем, додатків та проектів, які обробляють персональну інформацію **<PM-05(01)_ODP_частота>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: План програми інформаційної безпеки; інвентаризація системи; процедури, що стосуються розробки та обслуговування інвентаризації системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; персонал організації, відповідальний за розробку та ведення інвентаризації системи; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації з розробки та обслуговування інвентаризації системи; автоматизовані механізми підтримки інвентаризації системи].	

PM-6	**ПОКАЗНИКИ ПРОДУКТИВНОСТІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PM-06[01]	розроблені заходи з інформаційної безпеки;
	PM-06[02]	здійснюється моніторинг заходів з інформаційної безпеки;

	PM-06[03]	звітують про результати виконання заходів з інформаційної безпеки;
	PM-06[04]	розроблені заходи щодо забезпечення конфіденційності результатів діяльності;
	PM-06[05]	відстежуються показники ефективності, що стосуються конфіденційності;
	PM-06[06]	повідомляються результати вимірювань приватності продуктивності.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: План програми інформаційної безпеки; заходи інформаційної безпеки; процедури, що стосуються розробки, моніторингу та звітності про заходи інформаційної безпеки; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за планування програм захисту інформації та несе відповідальність за виконання плану; персонал організації, відповідальний за розробку, моніторинг та звітування про заходи інформаційної безпеки; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для розробки, моніторингу та звітування про заходи інформаційної безпеки; автоматизовані механізми, що підтримують розробку, моніторинг та звітування про заходи інформаційної безпеки].	

PM-7	**АРХІТЕКТУРА ПІДПРИЄМСТВА**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PM-07[01]	розроблена архітектура підприємства з урахуванням інформаційної безпеки;
	PM-07[02]	підтримується архітектура підприємства з урахуванням інформаційної безпеки;
	PM-07[03]	розроблена архітектура підприємства з урахуванням конфіденційності;
	PM-07[04]	підтримується архітектура підприємства з урахуванням конфіденційності;
	PM-07[05]	розроблена архітектура підприємства з урахуванням ризиків для діяльності та активів організації, окремих осіб, інших організацій та держави в цілому;
	PM-07[06]	підтримується архітектура підприємства з урахуванням ризиків, що виникають в результаті цього для операцій та активів організації, окремих осіб, інших організацій та держави.,
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ:	

	Дослідження: [ВИБІР: План програми інформаційної безпеки; заходи інформаційної безпеки; процедури, що стосуються розробки, моніторингу та звітності про заходи інформаційної безпеки; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за планування програм захисту інформації та несе відповідальність за виконання плану; персонал організації, відповідальний за розробку, моніторинг та звітування про заходи інформаційної безпеки; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для розробки, моніторингу та звітування про заходи інформаційної безпеки; автоматизовані механізми, що підтримують розробку, моніторинг та звітування про заходи інформаційної безпеки].

PM-7(1)	**АРХІТЕКТУРА ПІДПРИЄМСТВА - РОЗВАНТАЖЕННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PM-07(01)_ODP	**визначені несуттєві функції або послуги, які потрібно розвантажити;**
	PM-07(01)	**<PM-07(01)_ODP несуттєві функції або послуги>** вивантажуються на інші системи, компоненти системи або зовнішнього постачальника.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: План програми інформаційної безпеки; план програми конфіденційності; документація з архітектури підприємства; процедури, що стосуються розвитку архітектури підприємства; процедури визначення та розвантаження функцій або послуг; результати оцінки ризиків архітектури підприємства; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за планування програм інформаційної безпеки та конфіденційності та впровадження планів; персонал організації, відповідальний за розробку архітектури підприємства; персонал організації, відповідальний за оцінку ризиків архітектури підприємства; персонал організації, відповідальний за інформаційну безпеку та конфіденційність]. **Перевірка**: [ВИБІР: Процеси організації розробки архітектури підприємства; механізми підтримки архітектури підприємства та її розвитку; механізми розвантаження функцій та сервісів].	

PM-8	**ПЛАН ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PM-08[01]	враховані питання інформаційної безпеки при розробці плану захисту критичної інфраструктури та ключових ресурсів;

	PM-08[02]	розглядаються питання інформаційної безпеки в документації плану захисту критичної інфраструктури та ключових ресурсів;
	PM-08[03]	враховані питання інформаційної безпеки в оновленому плані захисту критичної інфраструктури та ключових ресурсів;
	PM-08[04]	враховані питання конфіденційності при розробці плану захисту критичної інфраструктури та ключових ресурсів;
	PM-08[05]	розглядаються питання конфіденційності в документації плану захисту критичної інфраструктури та ключових ресурсів;
	PM-08[06]	враховані питання конфіденційності в оновленому плані захисту критичної інфраструктури та ключових ресурсів.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: План програми інформаційної безпеки; план захисту критичної інфраструктури та ключових ресурсів; процедури, що стосуються розробки, документації та оновлення критичної інфраструктури та плану захисту ключових ресурсів; Національний план захисту інфраструктури; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за планування програм захисту інформації та несе відповідальність за виконання плану; персонал організації, відповідальний за розробку, документування та оновлення критичної інфраструктури та плану захисту ключових ресурсів; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для розробки, документування та оновлення критичної інфраструктури та плану захисту ключових ресурсів; автоматизовані механізми, що підтримують розробку, документацію та оновлення критичної інфраструктури та плану захисту ключових ресурсів].	

PM-9	**СТРАТЕГІЯ УПРАВЛІННЯ РИЗИКАМИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PM-09_ODP	**визначено періодичність перегляду та оновлення стратегії управління ризиками;**
	PM-09a.01	розроблена комплексна стратегія управління ризиками безпеки для операцій та активів організації, окремих осіб, інших організацій та держави, пов'язаних з експлуатацією та використанням організаційних систем;
	PM-09a.02	розроблена комплексна стратегія управління ризиками для приватності осіб, що виникають внаслідок санкціонованої обробки інформації, що ідентифікує особу;
	PM-09b.	стратегія управління ризиками послідовно впроваджується в

		організації;
	PM-09c.	переглядається та оновлюється стратегія управління ризиками **<PM-09_ODP частота>** або в міру необхідності у зв'язку з організаційними змінами.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: План програми інформаційної безпеки; процедури, що стосуються управління (тобто документації, відстеження та звітування) процесу авторизації безпеки; документи дозволу безпеки; списки або інша документація про ролі та обов'язки процесу авторизації безпеки; результати оцінки ризиків, що стосуються процесу санкціонування безпеки та загальноорганізаційної програми управління ризиками; стратегія управління організаційними ризиками; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; персонал організації, відповідальний за управління процесом авторизації безпеки; уповноважені посадові особи; власники системи, старший працівник інформаційної безпеки; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для авторизації безпеки; автоматизовані механізми, що підтримують процес авторизації безпеки].	

PM-10	**ПРОЦЕС АВТОРИЗАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PM-10a.[01]	**управляється стан безпеки систем організації і середовищ, в яких ці системи працюють, за допомогою процесів авторизації;**
	PM-10a.[02]	управляється стан конфіденційності організаційних систем і середовищ, в яких ці системи працюють, за допомогою процесів авторизації;
	PM-10b.	призначені особи для виконання конкретних ролей та обов'язків в рамках процесу управління організаційними ризиками;
	PM-10c.	інтегровані процеси авторизації в загальноорганізаційну програму управління ризиками.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: План програми інформаційної безпеки; процедури, що стосуються управління (тобто документації, відстеження та звітування) процесу авторизації безпеки; документи дозволу безпеки; списки або інша документація про ролі та обов'язки процесу авторизації безпеки; результати оцінки ризиків, що стосуються процесу санкціонування безпеки та загальноорганізаційної програми управління ризиками; стратегія управління організаційними ризиками; інші	

	відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; персонал організації, відповідальний за управління процесом авторизації безпеки; уповноважені посадові особи; власники системи, старший працівник інформаційної безпеки; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для авторизації безпеки; автоматизовані механізми, що підтримують процес авторизації безпеки].

PM-11	**ВИЗНАЧЕННЯ ЗАВДАНЬ ТА ПРОЦЕСІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PM-11_ODP	**визначено періодичність перегляду завдань та бізнес-процесів;**
	PM-11a.[01]	завдання та бізнес-процеси організації визначені з урахуванням інформаційної безпеки;
	PM-11a.[02]	завдання та бізнес-процеси організації визначені з урахуванням права на приватність;
	PM-11a.[03]	завдання та бізнес-процеси організації визначені з урахуванням ризиків для діяльності організації, її активів, окремих осіб, інших організацій та держави в цілому;
	PM-11b.[01]	визначені потреби в захисті інформації, що випливають з визначених завдань та бізнес-процесів;
	PM-11b.[02]	визначені потреби в обробці персональних даних, що випливають з визначеної місії та бізнес-процесів;
	PM-11c.	переглядаються завдання та бізнес-процеси **<PM-11_ODP частота>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: План програми захисту інформації; стратегія управління ризиками; процедури визначення потреб у захисті місії, бізнесу; результати оцінки ризику, що стосуються визначення потреб місії, бізнесу у захисті; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; персонал організації, відповідальний за місію, процеси; персонал організації, відповідальний за визначення потреб у захисті інформації для місій, процесів; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для визначення місії, процесів та їхніх потреб у захисті інформації].	

PM-12	ПРОГРАМА ІНСАЙДЕРСЬКОЇ ЗАГРОЗИ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PM-12	впроваджено програму інсайдерської (внутрішньої) загрози, яка передбачає наявність команди з обробки інцидентів, пов’язаних з внутрішньою дисципліною.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ: **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за планування та реалізацію програми інформаційної безпеки та конфіденційності; персонал організації, відповідальний за програму протидії внутрішнім загрозам; члени міждисциплінарної групи з обробки інцидентів, пов'язаних з внутрішніми загрозами; юрисконсульт; персонал організації, відповідальний за інформаційну безпеку та конфіденційність]. **Перевірка:** [ВИБІР: Процеси організації впровадження програми протидії внутрішнім загрозам та міждисциплінарної групи з протидії інцидентам, пов'язаним з внутрішніми загрозами; механізми підтримки та/або впровадження програми протидії внутрішнім загрозам та міждисциплінарної групи з протидії інцидентам, пов'язаним з внутрішніми загрозами].	

PM-13	БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРАЦІВНИКІВ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PM-13[01]	існує програма розвитку та вдосконалення спеціалістів з питань безпеки;
	PM-13[02]	створена програма розвитку та вдосконалення спеціалістів з питань приватності.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: План програми інформаційної безпеки; документація щодо розробки та вдосконалення співробітників з питань інформаційної безпеки; процедури розробки та вдосконалення співробітників з питань інформаційної безпеки; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; персонал організації, відповідальний за програму розвитку та вдосконалення співробітників з питань інформаційної безпеки; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для впровадження програми розвитку та вдосконалення співробітників з питань інформаційної безпеки; автоматизовані механізми підтримки та, або реалізації програми розвитку та вдосконалення	

	співробітників з питань інформаційної безпеки].

PM-14	**ТЕСТУВАННЯ, НАВЧАННЯ ТА МОНІТОРИНГ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PM-14a.01[01]	впроваджено процес, який забезпечує розробку планів організації для проведення тестування, навчання та моніторингу безпеки, пов'язаних з системами організації;
	PM-14a.01[02]	підтримується впроваджений процес, який гарантує, що плани організації щодо проведення тестування, навчання та моніторингу безпеки, пов'язані з системами організації;
	PM-14a.01[03]	впроваджено процес, який забезпечує розробку планів організації для проведення тестування, навчання та моніторингу конфіденційності, пов'язаних з системами організації;
	PM-14a.01[04]	підтримуються впроваджений процес, який гарантує, що плани організації щодо проведення тестування, навчання та моніторингу конфіденційності, пов'язані з системами організації;
	PM-14a.02[01]	продовжує виконуватися впроваджений процес, який гарантує, що організаційні плани щодо проведення тестування, навчання та моніторингу безпеки, пов'язані з системами організації;
	PM-14a.02[02]	впроваджено процес, який гарантує, що організаційні плани щодо проведення тестування, навчання та моніторингу конфіденційності, пов'язані з системами організації, продовжують виконуватися;
	PM-14b.[01]	перевіряються плани атестації на відповідність стратегії управління ризиками організації;
	PM-14b.[02]	переглядаються навчальні плани на предмет відповідності стратегії управління ризиками організації;
	PM-14b.[03]	переглядаються плани моніторингу на предмет відповідності стратегії управління ризиками організації;
	PM-14b.[04]	перевіряються плани тестування на відповідність загальноорганізаційним пріоритетам реагування на ризики;
	PM-14b.[05]	переглядаються навчальні плани на предмет відповідності загальноорганізаційним пріоритетам реагування на ризики;
	PM-14b.[06]	переглядаються плани моніторингу на предмет відповідності загальноорганізаційним пріоритетам реагування на ризики.

	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: План програми інформаційної безпеки; плани проведення тестування, навчання та моніторингу безпеки; організаційні процедури, що стосуються розробки та підтримки планів проведення тестування, навчання та моніторингу безпеки; стратегія управління ризиками; процедури перегляду планів проведення тестування, навчання та моніторингу безпеки на відповідність стратегії управління ризиками та пріоритетам реагування на ризик; результати оцінки ризику, пов'язані з проведенням перевірок безпеки, навчання та моніторингу; докази того, що плани проведення заходів з тестування, навчання та моніторингу безпеки виконуються своєчасно; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за розробку та підтримку планів проведення тестування, навчання та моніторингу безпеки; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для розробки та підтримки планів проведення тестування, навчання та моніторингу безпеки; автоматизовані механізми, що підтримують розробку та підтримку планів проведення тестування, навчання та моніторингу безпеки].

PM-15	**КОНТАКТИ З ГРУПАМИ ТА АСОЦІАЦІЯМИ З ПИТАНЬ БЕЗПЕКИ ІНФОРМАЦІЇ ТА ПРИВАТНОСТІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PM-15a.[01]	встановлено та інституціоналізовано контакт з окремими групами та асоціаціями у спільноті безпеки для сприяння постійному навчанню та тренінгам з питань безпеки для персоналу організації;
	PM-15a.[02]	встановлено та інституціоналізовано контакт з окремими групами та асоціаціями в межах спільноти з питань приватності, щоб сприяти постійній освіті та навчанню персоналу організації з питань приватності;
	PM-15b.[01]	встановлені та інституціоналізовані контакти з окремими групами та асоціаціями в рамках спільноти безпеки для підтримання актуальності рекомендованих практик, методів та технологій безпеки;
	PM-15b.[02]	встановлені та інституціоналізовані контакти з окремими групами та асоціаціями в межах спільноти безпеки, щоб бути в курсі рекомендованих практик, методів і технологій забезпечення конфіденційності;
	PM-15c.[01]	встановлені та інституціоналізовані контакти з окремими групами та асоціаціями всередині безпекового співтовариства для обміну поточною інформацією про безпеку, включаючи

		загрози, вразливості та інциденти;
	PM-15c.[02]	встановлено та інституціоналізовано контакт з окремими групами та асоціаціями в межах спільноти з питань конфіденційності для обміну поточною інформацією про конфіденційність, зокрема про загрози, вразливості та інциденти.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: План програми захисту інформації; стратегія управління ризиками; процедури контактів з групами безпеки та асоціаціями; докази встановленого та інституціоналізованого контакту з групами безпеки та асоціаціями; списки або інша документація про контакти та, або членство в групах безпеки та асоціаціях; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; персонал організації, відповідальний за встановлення та організацію контактів з групами безпеки та асоціаціями; персонал організації, який відповідає за інформаційну безпеку; персонал із вибраних груп та асоціацій, з якими організація встановила та інституціоналізувала контакти]. **Перевірка:** [ВИБІР: Процеси організації для встановлення та інституціоналізації контактів із групами безпеки та асоціаціями; автоматизовані механізми, що підтримують контакти з групами безпеки та асоціаціями].	

PM-16	**ПРОГРАМА ІНФОРМУВАННЯ ПРО ЗАГРОЗИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PM-16	впроваджена програма інформування про загрози, яка передбачає можливість обміну інформацією між організаціями для розвідки загроз.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: План програми захисту інформації; документація програми інформування про загрози; процедури для програми інформування про загрози; результати оцінки ризику, що стосуються інформування про загрози; перелік чи інша документація щодо можливості організації обміну інформацією між організаціями; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; персонал організації, відповідальний за програму інформування про загрози; персонал організації, відповідальний за можливості міжорганізаційного обміну інформацією; персонал організації, який відповідає за інформаційну безпеку; персонал, з яким організація передає інформацію про інформування про загрози]. **Перевірка:** [ВИБІР: Процеси організації для реалізації програми інформування про загрози; Процеси організації для впровадження міжорганізаційної можливості	

	обміну інформацією; автоматизовані механізми підтримки та, або реалізації програми інформування про загрози; автоматизовані механізми, що підтримують та, або реалізують можливості міжорганізаційного обміну інформацією].

PM-16(1)	**ПРОГРАМА ІНФОРМУВАННЯ ПРО ЗАГРОЗИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PM-16(01)	automated mechanisms are employed to maximize the effectiveness of sharing threat intelligence information.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: План програми захисту інформації; документація програми інформування про загрози; процедури для програми інформування про загрози; результати оцінки ризику, що стосуються інформування про загрози; перелік чи інша документація щодо можливості організації обміну інформацією між організаціями; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; персонал організації, відповідальний за програму інформування про загрози; персонал організації, відповідальний за можливості міжорганізаційного обміну інформацією; персонал організації, який відповідає за інформаційну безпеку; персонал, з яким організація передає інформацію про інформування про загрози]. **Перевірка:** [ВИБІР: Процеси організації для реалізації програми інформування про загрози; автоматизовані механізми підтримки та, або реалізації програми інформування про загрози; автоматизовані механізми, що підтримують та, або реалізують можливості міжорганізаційного обміну інформацією; автоматизовані засоби для максимізації ефективності обміну інформацією про виявлені загрози].	

PM-17	**ЗАХИСТ ПУБЛІЧНОЇ ІНФОРМАЦІЇ У ЗОВНІШНІХ СИСТЕМАХ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PM-17_ODP[01]	**визначена періодичність перегляду та оновлення політики;**
	PM-17_ODP[02]	**визначено періодичність перегляду та оновлення процедур;**
	PM-17a.[01]	розроблено політику, яка гарантує, що вимоги щодо захисту публічної (некласифікованої) інформації, яка обробляється, зберігається або передається в зовнішніх системах, виконуються відповідно до чинних законів, виконавчих наказів, директив, політик, нормативних актів та стандартів;

	PM-17a.[02]	встановлені процедури для забезпечення виконання вимог щодо захисту публічної (некласифікованої) інформації, яка обробляється, зберігається або передається в зовнішніх системах, відповідно до чинних законів, наказів, директив, політик, нормативно-правових актів та стандартів;
	PM-17b.[01]	переглядається та оновлюється політика **<PM-17_ODP[01] частота>**;
	PM-17b.[02]	переглядаються та оновлюються процедури **<PM-17_ODP[02] частота>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика щодо контрольованої публічної інформації; процедури щодо контрольованої публічної інформації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації з відповідальністю за контрольовану публічну інформацію; персонал організації з відповідальністю за інформаційну безпеку].	

PM-18	**ПРОГРАМА (КОНЦЕПЦІЯ) ЗАБЕЗПЕЧЕННЯ ПРИВАТНОСТІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PM-18_ODP	**визначена періодичність оновлення плану програми (концепції) приватності;**
	PM-18a.[01]	розроблено загальноорганізаційний план програми (концепції) приватності, який містить огляд програми приватності організації;
	PM-18a.01[01]	план програми (концепції) приватності містить опис структури програми конфіденційності;
	PM-18a.01[02]	план програми (концепції) приватності містить опис ресурсів, призначених для реалізації програми конфіденційності;
	PM-18a.02[01]	план програми (концепції) приватності містить огляд вимог до програми конфіденційності;
	PM-18a.02[02]	план програми (концепції) приватності містить опис наявних або запланованих засобів контролю для управління програмою (концепцією) приватності для виконання вимог програми;
	PM-18a.02[03]	план програми (концепції) приватності містить опис загальних засобів контролю, що діють або заплановані для виконання вимог програми конфіденційності;

	PM-18a.03[01]	в плані програми (концепції) приватності передбачена роль старшої посадової особи організації з питань приватності;
	PM-18a.03[02]	план програми (концепції) приватності включає визначення та призначення ролей інших посадових осіб і співробітників, відповідальних за забезпечення приватності, та їхні обов'язки;
	PM-18a.04[01]	план програми (концепції) приватності описує зобов'язання керівництва;
	PM-18a.04[02]	в плані програми (концепції) приватності описано дотримання вимог;
	PM-18a.04[03]	план програми (концепція) приватності описує стратегічні цілі та завдання програми приватності;
	PM-18a.05	план програми (концепція) приватності відображає координацію між підрозділами організації, відповідальними за різні аспекти приватності;
	PM-18a.06	затверджено план програми (концепцію) приватності вищою посадовою особою, яка несе відповідальність і підзвітність за ризики для приватності, яких зазнають операції організації (включно з місією, функціями, іміджем і репутацією), активи організації, окремі особи, інші організації та держава;
	PM-18a.[02]	поширюється план програми (концепція) приватності;
	PM-18b.[01]	оновлено план програми (концепцію) приватності **<PM-18_ODP частота>**;
	PM-18b.[02]	оновлюється план програми (концепція) приватності відповідно до змін у державному законодавстві та політиці щодо приватності;
	PM-18b.[03]	оновлюється план програми (концепція) приватності відповідно до змін в організації;
	PM-18b.[04]	оновлюється план програми (концепція) приватності забезпечення приватності для вирішення проблем, виявлених під час реалізації плану або оцінок контролю за дотриманням приватності.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: План програми з питань конфіденційності; процедури розробки та впровадження плану програми; процедури перегляду, оновлення та затвердження плану програми; процедури узгодження плану програми з відповідними організаціями; записи про перегляд, оновлення та затвердження плану програми; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: персонал організації, відповідальний за планування та реалізацію програми забезпечення конфіденційності; персонал організації,	

	відповідальний за забезпечення конфіденційності].

PM-19	**КЕРІВНІ РОЛІ ПРОГРАМИ ПРИВАТНОСТІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PM-19[01]	визначена періодичність оновлення плану програми приватності;
	PM-19[02]	розроблено загальноорганізаційний план програми приватності, який містить огляд програми приватності для організації;
	PM-19[03]	містить план програми приватності опис структури програми приватності;
	PM-19[04]	містить план програми приватності опис ресурсів, призначених для реалізації програми приватності;
	PM-19[05]	містить план програми приватності огляд вимог до програми приватності;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: План програми інформаційної безпеки; процедури, що стосуються розробки та реалізації плану програми; процедури, що стосуються огляду та оновлення програмних планів; процедури, що стосуються координації плану програми з відповідними структурами; процедури затвердження програмних планів; записи оглядів та оновлень програмних планів; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для розробки, перегляду, оновлення, затвердження плану програм інформаційної безпеки; автоматизовані механізми підтримки та, або реалізації плану програми інформаційної безпеки].	

PM-20	**СИСТЕМА ЗАПИСІВ ПРОГРАМИ ПРИВАТНОСТІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PM-20[01]	ведеться центральна вебсторінка на головному загальнодоступному вебсайті організації;
	PM-20[02]	слугує вебсторінка основним джерелом інформації про програму приватності організації;

	PM-20a.[01]	забезпечує вебсторінка доступ громадськості до інформації про діяльність організації, пов'язану із захистом приватності;
	PM-20a.[02]	забезпечує вебсторінка можливість громадськості спілкуватися з вищим посадовцем організації з питань приватності;
	PM-20b.[01]	забезпечує вебсторінка публічний доступ до інформації організації щодо приватності;
	PM-20b.[02]	забезпечує вебсторінка публічний доступ до звітів про приватність організації;
	PM-20c.	є на веб-сторінці загальнодоступні адреси електронної пошти та/або номери телефонів, щоб громадськість могла надавати зворотній зв'язок та/або направляти запитання до відділів з питань приватності.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: План програми інформаційної безпеки; процедури, що стосуються розробки та реалізації плану програми; процедури, що стосуються огляду та оновлення програмних планів; процедури, що стосуються координації плану програми з відповідними структурами; процедури затвердження програмних планів; записи оглядів та оновлень програмних планів; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для розробки, перегляду, оновлення, затвердження плану програм інформаційної безпеки; автоматизовані механізми підтримки та, або реалізації плану програми інформаційної безпеки].	

PM-20(1)	**СИСТЕМА ЗАПИСІВ ПРОГРАМИ ПРИВАТНОСТІ - ПОЛІТИКА ПРИВАТНОСТІ ВЕБСАЙТІВ, ДОДАТКІВ І ЦИФРОВИХ ПОСЛУГ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PM-20(01)[01]	розроблені та розміщені політики приватності на всіх зовнішніх веб-сайтах;
	PM-20(01)[02]	розроблені та розміщені політики приватності в усіх мобільних додатках;
	PM-20(01)[03]	розроблені та розміщені політики приватності на всіх інших цифрових сервісах;

	PM-20(01)(a)[01]	політика приватності написана простою мовою;
	PM-20(01)(a)[02]	політика приватності організована таким чином, щоб її було легко зрозуміти та орієнтуватися в ній;
	PM-20(01)(b)[01]	надає політика приватності інформацію, необхідну громадськості для прийняття поінформованого рішення про те, чи взаємодіяти з організацією;
	PM-20(01)(b)[02]	надає політика приватності інформацію, необхідну громадськості для прийняття поінформованого рішення про те, як взаємодіяти з організацією;
	PM-20(01)(c)[01]	оновлюється політика приватності щоразу, коли організація вносить суттєві зміни в описані в ній практики;
	PM-20(01)(c)[02]	містить політика приватності позначку часу/дати, щоб інформувати громадськість про дату останніх змін.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: План програми конфіденційності; політика конфіденційності на веб-сайті агентства, в мобільних додатках та/або інших цифрових сервісах]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за розповсюдження інформації про програму конфіденційності; персонал організації, відповідальний за конфіденційність]. **Перевірка**: [ВИБІР: Організаційні процедури та практики надання дозволів, проведення, управління та перегляду обробки інформації, що ідентифікує особу; організаційні процедури та практики поширення інформації про програму конфіденційності; механізми, що підтримують поширення інформації про програму конфіденційності].	

PM-21	**ОБЛІК РОЗКРИТТЯ ПЕРСОНАЛЬНИХ ДАНИХ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PM-21a.	розроблений і ведеться точний облік розкриття персональних даних;
	PM-21a.01[01]	облік включає дату кожного розкриття інформації;
	PM-21a.01[02]	облік відображає характер кожного розкриття інформації;

	PM-21a.01[03]	відображає звітність мету кожного розкриття інформації;
	PM-21a.02[01]	містить звітність ім'я особи або організації, в якій було зроблено розкриття;
	PM-21a.02[02]	містить звітність адресу або іншу контактну інформацію особи чи організації, якою було здійснено розкриття;
	PM-21b.	зберігається облік розкриттів протягом усього періоду зберігання інформації, що ідентифікує особу, або протягом п'яти років після розкриття, залежно від того, який з цих термінів довший
	PM-21c.	надається облік розкриття персональних даних особи, якої стосується інформація.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: План програми конфіденційності; політика та процедури розкриття інформації; записи про розкриття інформації; журнали аудиту; політика та процедури Закону про конфіденційність; система сповіщення про записи; правила винятків із Закону про конфіденційність]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за програму конфіденційності; персонал організації, відповідальний за конфіденційність]. **Перевірка**: [ВИБІР: Процеси організації для розкриття інформації; механізми, що підтримують облік розкриття інформації, включаючи комерційні послуги, які надають повідомлення та попередження].	

PM-22	**УПРАВЛІННЯ ЯКІСТЮ ПЕРСОНАЛЬНИХ ДАНИХ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PM-22[01]	розроблені та задокументовані загальноорганізаційні політики управління якістю персональних даних;
	PM-22[02]	розроблені та задокументовані загальноорганізаційні процедури управління якістю персональних даних;
	PM-22a.[01]	передбачено в політиці перевірку точності інформації, що ідентифікує особу, протягом усього життєвого циклу інформації;
	PM-22a.[02]	передбачено в політиці перегляд актуальності інформації, що ідентифікує особу, протягом життєвого циклу інформації;
	PM-22a.[03]	передбачено в політиці перевірку своєчасності інформації, що ідентифікує особу, протягом усього життєвого циклу інформації;

	PM-22a.[04]	передбачено в політиці перевірку повноти інформації, що ідентифікує особу, протягом життєвого циклу інформації;
	PM-22a.[05]	передбачено в процедурах перевірку точності інформації, що ідентифікує особу, протягом усього життєвого циклу інформації;
	PM-22a.[06]	передбачено в процедурах перегляд актуальності інформації, що ідентифікує особу, протягом усього життєвого циклу інформації;
	PM-22a.[07]	процедури передбачають перевірку своєчасності інформації, що ідентифікує особу, протягом усього життєвого циклу інформації;
	PM-22a.[08]	передбачено в процедурах перевірку повноти інформації, що ідентифікує особу, протягом життєвого циклу інформації;
	PM-22b.[01]	передбачено в політиці виправлення або видалення неточної або застарілої персональної інформації, що ідентифікує особу;
	PM-22b.[02]	передбачено в процедурах виправлення або видалення неточної або застарілої персональної інформації;
	PM-22c.[01]	передбачено в політиці розсилання повідомлень про виправлену або видалену персональну інформацію фізичним особам або іншим відповідним суб'єктам;
	PM-22c.[02]	передбачено в процедурах повідомлення про виправлення або видалення персональних даних фізичним особам або іншим відповідним суб'єктам;
	PM-22d.[01]	передбачено в політиці оскарження негативних рішень щодо запитів на виправлення або видалення;
	PM-22d.[02]	передбачені процедури оскарження негативних рішень щодо запитів на виправлення або видалення.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: План програми інформаційної безпеки; процедури, що стосуються розробки та реалізації плану програми; процедури, що стосуються огляду та оновлення програмних планів; процедури, що стосуються координації плану програми з відповідними структурами; процедури затвердження програмних планів; записи оглядів та оновлень програмних планів; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для розробки, перегляду, оновлення,	

	затвердження плану програм інформаційної безпеки; автоматизовані механізми підтримки та, або реалізації плану програми інформаційної безпеки].

PM-23	**ОРГАН УПРАВЛІННЯ ПЕРСОНАЛЬНИМИ ДАНИМИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PM-23_ODP[01]	**визначені ролі органу управління персональними даними;**
	PM-23_ODP[02]	**визначені обов'язки органу управління персональними даними;**
	PM-23	створено орган управління даними, що складається з **<PM-23_ODP[01] ролей>** з **<PM-23_ODP[02] обов'язками>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: План програми інформаційної безпеки; процедури, що стосуються розробки та реалізації плану програми; процедури, що стосуються огляду та оновлення програмних планів; процедури, що стосуються координації плану програми з відповідними структурами; процедури затвердження програмних планів; записи оглядів та оновлень програмних планів; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Посадові особи, які входять до складу органу управління персональними даними (наприклад, головний спеціаліст з питань інформації, старший спеціаліст з питань інформаційної безпеки агентства та старший спеціаліст агентства з питань приватності)].	

PM-24	**ОРГАН З ПИТАНЬ ЦІЛІСНОСТІ ДАНИХ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PM-24	створено орган з питань цілісності даних;
	PM-24a.	розглядає орган з питань цілісності даних пропозиції щодо проведення або участі у відповідній програмі;
	PM-24b.	проводить орган з питань цілісності даних щорічну перевірку всіх програм співставлення, в яких агентство брало участь.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: План програми інформаційної безпеки; процедури, що стосуються розробки та реалізації плану програми; процедури, що стосуються огляду та оновлення програмних планів; процедури, що стосуються координації плану програми з відповідними структурами; процедури затвердження	

	програмних планів; записи оглядів та оновлень програмних планів; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Посадові особи, які входять до складу органу управління персональними даними (наприклад, головний спеціаліст з питань інформації, старший спеціаліст з питань інформаційної безпеки агентства та старший спеціаліст агентства з питань приватності)].

PM-25	**МІНІМІЗАЦІЯ КІЛЬКОСТІ ПЕРСОНАЛЬНИХ ДАНИХ, ЩО ВИКОРИСТОВУЮТЬСЯ ПІД ЧАС ТЕСТУВАННЯ, НАВЧАННЯ ТА ДОСЛІДЖЕНЬ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PM-25_ODP[01]	**визначено періодичність перегляду політик, які стосуються використання персональних даних для внутрішнього тестування, навчання та досліджень;**
	PM-25_ODP[02]	**визначено періодичність оновлення політик, які стосуються використання персональних даних для внутрішнього тестування, навчання та досліджень;**
	PM-25_ODP[03]	**визначено періодичність перегляду процедур, які стосуються використання персональних даних для внутрішнього тестування, навчання та досліджень;**
	PM-25_ODP[04]	**визначено періодичність оновлення процедур, які стосуються використання персональних даних для внутрішнього тестування, навчання та досліджень;**
	PM-25a.[01]	розроблені та задокументовані політики, які регулюють використання персональних даних для внутрішнього тестування;
	PM-25a.[02]	розроблені та задокументовані політики, які стосуються використання персональних даних для внутрішнього навчання
	PM-25a.[03]	розроблені та задокументовані політики, які регулюють використання персональних даних для внутрішніх досліджень;
	PM-25a.[04]	розроблені та задокументовані процедури, які стосуються використання персональних даних для внутрішнього тестування;
	PM-25a.[05]	розроблені та задокументовані процедури, які стосуються використання персональних даних для внутрішнього навчання;

	PM-25a.[06]	розроблені та задокументовані процедури, які стосуються використання персональних даних для внутрішніх досліджень;
	PM-25a.[07]	впроваджено політику, яка регулює використання персональних даних для внутрішнього тестування;
	PM-25a.[08]	впроваджуються політики, які стосуються використання персональних даних для навчання;
	PM-25a.[09]	впроваджуються політики, які стосуються використання персональної інформації для досліджень;
	PM-25a.[10]	впроваджені процедури, які стосуються використання персональних даних для внутрішнього тестування;
	PM-25a.[11]	впроваджені процедури, які стосуються використання персональної інформації для навчання;
	PM-25a.[12]	впроваджені процедури, які стосуються використання особистої інформації для досліджень;
	PM-25b.[01]	обмежено або зведено до мінімуму кількість персональних даних, що використовуються для цілей внутрішнього тестування;
	PM-25b.[02]	обмежено або зведено до мінімуму обсяг інформації, що ідентифікує особу, яка використовується для внутрішніх навчальних цілей;
	PM-25b.[03]	обмежено або зведено до мінімуму обсяг персональних даних, що використовуються для внутрішніх досліджень;
	PM-25c.[01]	дозволено використання персональних даних для внутрішнього тестування;
	PM-25c.[02]	дозволено використання персональних даних для внутрішнього навчання;
	PM-25c.[03]	дозволено необхідне використання персональних даних для внутрішніх досліджень;
	PM-25d.[01]	переглядаються політики **<PM-25_ODP[01] частота>**;
	PM-25d.[02]	оновлюються політики **<PM-25_ODP[02] частота>**;
	PM-25d.[03]	переглядаються процедури **<PM-25_ODP[03] частота>**;
	PM-25d.[04]	оновлюються процедури **<PM-25_ODP[04] частота>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: План програми інформаційної безпеки; процедури, що	

	стосуються розробки та реалізації плану програми; процедури, що стосуються огляду та оновлення програмних планів; процедури, що стосуються координації плану програми з відповідними структурами; процедури затвердження програмних планів; записи оглядів та оновлень програмних планів; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для розробки, перегляду, оновлення, затвердження плану програм інформаційної безпеки; автоматизовані механізми підтримки та, або реалізації плану програми інформаційної безпеки].

PM-26	**УПРАВЛІННЯ СКАРГАМИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PM-26_ODP[01]	**визначено період часу, протягом якого мають бути розглянуті скарги (в тому числі звернення або питання) від фізичних осіб;**
	PM-26_ODP[02]	**визначено період часу, протягом якого мають бути оброблені скарги (в тому числі звернення або питання) від фізичних осіб;**
	PM-26_ODP[03]	**визначено часовий період для підтвердження отримання скарг;**
	PM-26_ODP[04]	**визначено термін для відповіді на скарги;**
	PM-26[01]	впроваджено процес отримання скарг, занепокоєнь або запитань від фізичних осіб про безпеку та конфіденційність в організації;
	PM-26[02]	впроваджено процес реагування на скарги, занепокоєння або запитання від фізичних осіб про безпеку та конфіденційність в організації;
	PM-26a.[01]	включає процес управління скаргами механізми, які є простими у використанні для громадськості;
	PM-26c.[02]	включає процес управління скаргами механізми, які є легкодоступними для громадськості;
	PM-26b.	містить процес управління скаргами всю інформацію, необхідну для успішного подання скарг;
	PM-26c.[01]	включає процес управління скаргами механізми відстеження, які гарантують, що всі скарги будуть розглянуті протягом **<PM-26_ODP[01] періоду часу>**;

	PM-26c.[02]	включає процес управління скаргами механізми відстеження, щоб гарантувати, що всі скарги розглядаються протягом **<PM-26_ODP[02] часового періоду>**;
	PM-26d.	передбачає процес управління скаргами підтвердження отримання скарг, занепокоєнь або запитань від фізичних осіб протягом **<PM-26_ODP[03] часового періоду**>;
	PM-26e.	включає процес управління скаргами реагування на скарги, занепокоєння або питання від фізичних осіб протягом **<PM-26_ODP[04] часового періоду**>.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: План програми інформаційної безпеки; процедури, що стосуються розробки та реалізації плану програми; процедури, що стосуються огляду та оновлення програмних планів; процедури, що стосуються координації плану програми з відповідними структурами; процедури затвердження програмних планів; записи оглядів та оновлень програмних планів; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для розробки, перегляду, оновлення, затвердження плану програм інформаційної безпеки; автоматизовані механізми підтримки та, або реалізації плану програми інформаційної безпеки].	

PM-27	**ЗВІТНІСТЬ З ПИТАНЬ ЗАБЕЗПЕЧЕННЯ ПРИВАТНОСТІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PM-27_ODP[01]	**визначені звіти з питань забезпечення приватності;**
	PM-27_ODP[02]	**визначені органи нагляду за дотриманням приватності;**
	PM-27_ODP[03]	**визначені посадові особи, відповідальні за контроль і дотриманням програми приватності;**
	PM-27_ODP[04]	**визначена періодичність перегляду та оновлення звітів про приватність;**
	PM-27a.	розроблено <**PM-27_ODP[01] звіти з питань приватності**>;
	PM-27a.01	передаються звіти з питань забезпечення приватності до **<PM-27_ODP[02] наглядових органів>**, щоб продемонструвати підзвітність законодавчим, регуляторним та політичним мандатам щодо приватності;

	PM-27a.02[01]	поширюються звіти про конфіденційність серед **<PM-27_ODP[03] посадових осіб>**;
	PM-27a.02[02]	поширюються звіти з питань забезпечення приватності серед іншого персоналу, відповідального за контроль за дотриманням програми конфіденційності;
	PM-27b.	переглядаються та оновлюються звіти з питань забезпечення приватності **<PM-27_ODP[04] частота**>.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: План програми інформаційної безпеки; процедури, що стосуються розробки та реалізації плану програми; процедури, що стосуються огляду та оновлення програмних планів; процедури, що стосуються координації плану програми з відповідними структурами; процедури затвердження програмних планів; записи оглядів та оновлень програмних планів; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; персонал організації, який відповідає за інформаційну безпеку].	

PM-28	**ОЦІНКА РИЗИКІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PM-28_ODP[01]	**визначено персонал, який отримуватиме результати визначення ризиків;**
	PM-28_ODP[02]	**визначено періодичність перегляду та оновлення міркувань щодо структуризації ризиків;**
	PM-28a.01[01]	визначені та задокументовані припущення, що впливають на оцінку ризиків;
	PM-28a.01[02]	визначені та задокументовані припущення, що впливають на реагування ризиків;
	PM-28a.01[03]	визначені та задокументовані припущення, що впливають на моніторинг ризиків;
	PM-28a.02[01]	визначені та задокументовані обмеження, що впливають на оцінку ризиків;
	PM-28a.02[02]	визначені та задокументовані обмеження, що впливають на реагування на ризики;
	PM-28a.02[03]	визначені та задокументовані обмеження, що впливають на моніторинг ризиків;

	PM-28a.03[01]	визначені та задокументовані пріоритети, які розглядаються організацією для управління ризиками;
	PM-28a.03[02]	визначені та задокументовані компроміси, які розглядаються організацією для управління ризиками;
	PM-28a.04	визначена та задокументована організаційна толерантність до ризиків;
	PM-28b.	поширюються результати діяльності з фреймворкінгу ризиків серед персоналу **<PM-28_ODP[01]>**;
	PM-28c.	переглядаються та оновлюються міркування щодо фреймінгу ризиків **<PM-28_ODP[02] частота>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: План програми інформаційної безпеки; процедури, що стосуються розробки та реалізації плану програми; процедури, що стосуються огляду та оновлення програмних планів; процедури, що стосуються координації плану програми з відповідними структурами; процедури затвердження програмних планів; записи оглядів та оновлень програмних планів; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для розробки, перегляду, оновлення, затвердження плану програм інформаційної безпеки; автоматизовані механізми підтримки та, або реалізації плану програми інформаційної безпеки].	

PM-29	**РОЛІ КЕРІВНИКІВ ПРОГРАМИ УПРАВЛІННЯ РИЗИКАМИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PM-29a.[01]	призначено старшу посадову особу, відповідальну за управління ризиками;
	PM-29a.[02]	узгоджує старша посадова особа, відповідальна за управління ризиками, процеси управління інформаційною безпекою та конфіденційністю з процесами стратегічного, операційного та бюджетного планування;
	PM-29b.[01]	створена посада (функція) ризик-менеджера;
	PM-29b.[02]	розглядає та аналізує керівник з управління ризиками (функція) ризики з точки зору всієї організації;
	PM-29b.[03]	забезпечує керівник (функція) з управління ризиками узгоджене управління ризиками в межах всієї організації.

	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: План програми інформаційної безпеки; процедури, що стосуються розробки та реалізації плану програми; процедури, що стосуються огляду та оновлення програмних планів; процедури, що стосуються координації плану програми з відповідними структурами; процедури затвердження програмних планів; записи оглядів та оновлень програмних планів; інші відповідні документи або записи]. **Перевірка:** [ВИБІР: Процеси організації для розробки, перегляду, оновлення, затвердження плану програм інформаційної безпеки; автоматизовані механізми підтримки та, або реалізації плану програми інформаційної безпеки].

PM-30	**ПЛАН УПРАВЛІННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PM-30_ODP	**призначено старшу посадову особу, відповідальну за управління ризиками ланцюга постачання;**
	PM-30a.[01]	узгоджує старша посадова особа, відповідальна за управління ризиками ланцюга постачання, процеси управління інформаційною безпекою та конфіденційністю з процесами стратегічного, операційного та бюджетного планування;
	PM-30a.[02]	створена посада (функція) ризик-менеджер;
	PM-30a.[03]	розглядає та аналізує керівник з управління ризиками (функція) ризики з точки зору всієї організації;
	PM-30a.[04]	забезпечує керівник (функція) з управління ризиками узгоджене управління ризиками в межах всієї організації.
	PM-30a.[05]	стратегія управління ризиками ланцюга постачання враховує ризики, пов'язані з придбанням систем;
	PM-30a.[06]	стратегія управління ризиками ланцюга поставок враховує ризики, пов'язані з придбанням компонентів системи;
	PM-30a.[07]	стратегія управління ризиками ланцюга поставок враховує ризики, пов'язані з придбанням системних послуг;
	PM-30a.[08]	тратегія управління ризиками ланцюга поставок враховує ризики, пов'язані з обслуговуванням систем;
	PM-30a.[09]	стратегія управління ризиками ланцюга поставок враховує ризики, пов'язані з обслуговуванням компонентів системи;
	PM-30a.[10]	стратегія управління ризиками ланцюга поставок враховує ризики, пов'язані з обслуговуванням системних послуг;

	PM-30a.[11]	враховує стратегія управління ризиками ланцюга постачання ризики, пов'язані з утилізацією систем;
	PM-30a.[12]	враховує стратегія управління ризиками ланцюга постачання ризики, пов'язані з утилізацією компонентів системи;
	PM-30a.[13]	стратегія управління ризиками ланцюга поставок враховує ризики, пов'язані з утилізацією системних послуг;
	PM-30b.	стратегія управління ризиками ланцюга поставок послідовно впроваджується в організації;
	PM-30c.	переглядається та оновлюється стратегія управління ризиками ланцюга постачання **<PM-30_ODP частота>** або в міру необхідності у зв'язку з організаційними змінами
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: План програми інформаційної безпеки; процедури, що стосуються розробки та реалізації плану програми; процедури, що стосуються огляду та оновлення програмних планів; процедури, що стосуються координації плану програми з відповідними структурами; процедури затвердження програмних планів; записи оглядів та оновлень програмних планів; інші відповідні документи або записи]. **Перевірка:** [ВИБІР: Процеси організації для розробки, перегляду, оновлення, затвердження плану програм інформаційної безпеки; автоматизовані механізми підтримки та, або реалізації плану програми інформаційної безпеки].	

PM-30(1)	**ПЛАН УПРАВЛІННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ – ПОСТАЧАННЯ КРИТИЧНОВАЖЛИВИХ ТОВАРІВ АБО ТОВАРІВ, ЩО МАЮТЬ ВАЖЛИВЕ ЗНАЧЕННЯ ДЛЯ ДІЯЛЬНОСТІ ОРГАНІЗАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PM-30(01)[01]	визначені постачальники критично важливих технологій, продуктів і послуг, що мають вирішальне значення для виконання завдань;
	PM-30(01)[02]	є пріоритетними постачальники критично важливих технологій, продуктів та послуг;
	PM-30(01)[03]	оцінюються постачальники критично важливих технологій, продуктів та послуг.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: План управління ризиками ланцюга постачання; загальноорганізаційна стратегія управління ризиками; документи з управління ризиками підприємства; документи з обліку запасів або постачальників;	

	документація з оцінки та визначення пріоритетів; документи або записи про критичні або важливі для місії технології, продукти та послуги; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за управління ризиками ланцюга постачання; персонал організації, відповідальний за інформаційну безпеку; персонал організації, відповідальний за закупівлю; персонал організації, відповідальний за управління ризиками підприємства]. **Перевірка**: [ВИБІР: Процеси організації ідентифікації, визначення пріоритетів та оцінки критичних або важливих для місії технологій, продуктів та послуг; організаційні процеси ведення інвентаризації постачальників; організаційний процес асоціювання постачальників з критичними або важливими для місії технологіями, продуктами та послугами [електронний ресурс].

PM-31	**ПЛАН БЕЗПЕРЕРВНОГО МОНІТОРИНГУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PM-31_ODP[01]	**визначені параметри для безперервного моніторингу в масштабах всієї організації;**
	PM-31_ODP[02]	**визначено періодичність моніторингу;**
	PM-31_ODP[03]	**визначена періодичність оцінки ефективності контролю;**
	PM-31_ODP[04]	**визначено персонал або ролі для звітування про стан безпеки систем організації;**
	PM-31_ODP[05]	**визначено персонал або ролі для звітування про стан конфіденційності систем організації;**
	PM-31_ODP[06]	**визначено періодичність звітування про стан безпеки систем організації;**
	PM-31_ODP[07]	**визначено періодичність звітування про стан конфіденційності систем організації;**
	PM-31	розроблена загальноорганізаційна стратегія безперервного моніторингу;
	PM-31a.	впроваджуються програми безперервного моніторингу, які включають встановлення **<PM-31_ODP[01] параметрів>**, що підлягають моніторингу;
	PM-31b.[01]	впроваджено програми безперервного моніторингу, які встановлюють **<PM-31_ODP[02] частоту>** для моніторингу;
	PM-31b.[02]	впроваджуються програми безперервного моніторингу, які встановлюють **<PM-31_ODP[03] частоту>** для оцінки ефективності контролю;

	PM-31c.	впроваджуються програми безперервного моніторингу, які включають моніторинг **<PM-31_ODP[01] параметрів>** на постійній основі відповідно до стратегії безперервного моніторингу;
	PM-31d.[01]	впроваджуються програми безперервного моніторингу, які включають співставлення інформації, отриманої в результаті контрольних оцінок та моніторингу;
	PM-31d.[02]	впроваджуються програми постійного моніторингу, які включають аналіз інформації, отриманої в результаті контрольних оцінок та моніторингу;
	PM-31e.[01]	впроваджуються програми безперервного моніторингу, які передбачають заходи реагування на аналіз інформації, отриманої в результаті оцінки результатів контролю;
	PM-31e.[02]	впроваджуються програми безперервного моніторингу, які передбачають заходи реагування на результати аналізу інформації, отриманої під час моніторингу;
	PM-31f.[01]	впроваджено програми безперервного моніторингу, які передбачають звітування про стан безпеки систем організації перед **<PM-31_ODP[04] персонал або ролі>** **<PM-31_ODP[06] частота>**;
	PM-31f.[02]	впроваджені програми безперервного моніторингу, які передбачають звітування про стан конфіденційності організаційних систем перед **<PM-31_ODP[05] персонал або ролі>** **<PM-31_ODP[07] частота>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: План програми інформаційної безпеки; процедури, що стосуються розробки та реалізації плану програми; процедури, що стосуються огляду та оновлення програмних планів; процедури, що стосуються координації плану програми з відповідними структурами; процедури затвердження програмних планів; записи оглядів та оновлень програмних планів; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для розробки, перегляду, оновлення, затвердження плану програм інформаційної безпеки; автоматизовані механізми підтримки та, або реалізації плану програми інформаційної безпеки].	

PM-32	**ПРИЗНАЧЕННЯ**
	МЕТА ОЦІНКИ: Визначити, чи:

	PM-32_ODP	**визначені системи або компоненти системи, що підтримують важливі для місії послуги або функції;**
	PM-32	аналізуються допоміжні послуги або функції, необхідні для виконання місії, для забезпечення того, щоб інформаційні ресурси використовувалися відповідно до їхнього призначення.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: План програми інформаційної безпеки; процедури, що стосуються розробки та реалізації плану програми; процедури, що стосуються огляду та оновлення програмних планів; процедури, що стосуються координації плану програми з відповідними структурами; процедури затвердження програмних планів; записи оглядів та оновлень програмних планів; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за планування програм захисту інформації та відповідальність за виконання плану; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для розробки, перегляду, оновлення, затвердження плану програм інформаційної безпеки; автоматизовані механізми підтримки та, або реалізації плану програми інформаційної безпеки].	

XIV. КЛАС ЗАХОДІВ ЗАХИСТУ PS – КАДРОВА БЕЗПЕКА

PS-1	**ПОЛІТИКА ТА ПРОЦЕДУРИ КАДРОВОЇ БЕЗПЕКИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PS-01_ODP[01]	**визначено персонал або ролі, на які поширюється політика кадрової безпеки;**
	PS-01_ODP[02]	**визначено персонал або ролі, на які поширюються процедури кадрової безпеки;**
	PS-01_ODP[03]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {рівень організації; рівень місії/бізнес-процесу; рівень системи};**
	PS-01_ODP[04]	**визначено посадову особу, яка керуватиме політикою та процедурами кадрової безпеки;**
	PS-01_ODP[05]	**визначена періодичність перегляду та оновлення поточної політики кадрової безпеки;**
	PS-01_ODP[06]	**є події, які вимагають перегляду та оновлення поточної політики кадрової безпеки;**
	PS-01_ODP[07]	**визначено періодичність перегляду та оновлення поточних процедур кадрової безпеки;**
	PS-01_ODP[08]	**є події, які вимагають перегляду та оновлення процедур безпеки персоналу;**
	PS-01a.[01]	розроблена та задокументована політика безпеки персоналу;
	PS-01a.[02]	поширюється політика безпеки персоналу на **<PS-01_ODP[01] персонал або ролі>**;
	PS-01a.[03]	розроблені та задокументовані процедури кадрової безпеки, що сприяють впровадженню політики кадрової безпеки та пов'язаних з нею засобів контролю кадрової безпеки;
	PS-01a.[04]	поширюються процедури безпеки персоналу на **<PS-01_ODP[02] персонал або ролі>**;
	PS-01a.01(a)[01]	політика безпеки персоналу **<PS-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)**> відповідає меті;
	PS-01a.01(a)[02]	політика безпеки персоналу **<PS-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** звертається до сфери дії;
	PS-01a.01(a)[03]	політика безпеки персоналу **<PS-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** стосується ролей;

	PS-01a.01(a)[04]	політика безпеки персоналу **<PS-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** враховує обов'язки;
	PS-01a.01(a)[05]	політика безпеки персоналу **<PS-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** враховує зобов'язання керівництва;
	PS-01a.01(a)[06]	політика безпеки персоналу **<PS-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** передбачає координацію між підрозділами організації;
	PS-01a.01(a)[07]	політика безпеки персоналу **<PS-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** стосується системb контролю відповідності;
	PS-01a.01(b)	відповідає політика безпеки персоналу **<PS-01_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** чинному законодавству, виконавчим наказам, директивам, положенням, політикам, стандартам і настановам;
	PS-01b.	призначено **<PS-01_ODP[04] посадову особу >** для управління розробкою, документуванням та розповсюдженням політики та процедур кадрової безпеки;
	PS-01c.01[01]	переглядається та оновлюється поточна політика безпеки персоналу **<PS-01_ODP[05] частота>**;
	PS-01c.01[02]	переглядається та оновлюється поточна політика безпеки персоналу після подій **<PS-01_ODP[06]>**;
	PS-01c.02[01]	переглядаються та оновлюються поточні процедури безпеки персоналу **<PS-01_ODP[07] частота>**;
	PS-01c.02[02]	переглядаються та оновлюються поточні процедури безпеки персоналу після подій **<PS-01_ODP[08]>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: [ВИБІР: Політики та процедури кадрової безпеки; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал відповідальний за політику кадрової безпеки; персонал, відповідальний за інформаційну безпеку].	

PS-2	**ВИЗНАЧЕННЯ ПОСАДОВОГО РИЗИКУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PS-02_ODP	**визначено періодичність перегляду та оновлення ідентифікаторів посадових ризиків;**

	PS-02a.	всім посадам в організації присвоєно ідентифікатор ризику;
	PS-02b.	вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {рівень організації; рівень місії/бізнес-процесу; рівень системи};
	PS-02c.	встановлені критерії відбору для осіб, які обіймають посади в організації;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика безпеки персоналу; процедури, що стосуються категоризації посади; відповідні кодекси федеральних нормативних актів; перелік позначень ризиків для організаційних посад; план захисту інформації; записи оглядів та оновлення позначень ризиків позицій; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за забезпечення персоналу; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для призначення, перегляду та оновлення позначень ризиків позицій; організаційні процеси для встановлення критеріїв скринінгу].	

PS-3	**ПЕРЕВІРКА ПЕРСОНАЛУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PS-03_ODP[01]	**визначені умови, що вимагають повторної перевірки осіб;**
	PS-03_ODP[02]	**визначена частота повторної перевірки осіб, для яких це показано;**
	PS-03a.	проходять особи перевірку перед тим, як надати їм доступ до системи;
	PS-03b.[01]	проходять особи повторну перевірку відповідно до **<PS-03_ODP[01] умови, що вимагають повторної перевірки>**;
	PS-03b.[02]	проводиться повторна перевірка у випадках, коли це зазначено, **<PS-03_ODP[02] частота>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика безпеки персоналу; процедури, що стосуються категоризації посади; відповідні кодекси федеральних нормативних актів; перелік позначень ризиків для організаційних посад; план захисту інформації; записи оглядів та оновлення позначень ризиків позицій; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за забезпечення персоналу; персонал організації, який відповідає за інформаційну безпеку].	

	Перевірка: [ВИБІР: Процеси організації для призначення, перегляду та оновлення позначень ризиків позицій; організаційні процеси для встановлення критеріїв скринінгу].

PS-3(1)	**ПЕРЕВІРКА ПЕРСОНАЛУ - ІНФОРМАЦІЯ З ОБМЕЖЕНИМ ДОСТУПОМ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PS-03(01)[01]	особи мають допуск та доступ до систем, де обробляється, зберігається або передається інформація з обмеженим доступом;
	PS-03(01)[02]	особи, які мають доступ до системи, де обробляється, зберігається або передається інформація з обмеженим доступом, ознайомлені з найвищим ступенем секретності інформації, до якої вони мають доступ у системі.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика безпеки персоналу; процедури, що стосуються скринінгу персоналу; записи про перевірений персонал; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за безпеку персоналу; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для перевірки та навчання персоналу для доступу до секретної інформації].	

PS-3(2)	**ПЕРЕВІРКА ПЕРСОНАЛУ - ІНСТРУКТАЖ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PS-03(02)	особи, які мають 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.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика безпеки персоналу; процедури, що стосуються скринінгу персоналу; записи про перевірений персонал; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за безпеку персоналу; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для перевірки та навчання персоналу для доступу до секретної інформації].	

PS-3(3)	ПЕРЕВІРКА ПЕРСОНАЛУ - ІНФОРМАЦІЯ, ЩО ПОТРЕБУЄ ДОДАТКОВИХ ЗАХОДІВ ЗАХИСТУ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PS-03(03)_ODP	**визначені додаткові критерії перевірки персоналу, яким повинні відповідати особи, що мають чинний дозвіл на доступ до системи, яка обробляє, зберігає або передає інформацію, потребує додаткових заходів захисту;**
	PS-03(03)(a)	мають особи, які отримують доступ до системи, що обробляє, зберігає або передає інформацію, яка потребує додаткових заходів захисту, чинний дозвіл на доступ;
	PS-03(03)(b)	відповідають особи, які отримують доступ до системи, що обробляє, зберігає або передає інформацію, яка потребує додаткових заходів захисту, **<PS-03(03)_ODP додаткові критерії перевірки персоналу>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика безпеки персоналу; політика контролю доступу, процедури, що стосуються перевірки персоналу; записи про перевірений персонал; критерії скринінгу; записи дозволів на доступ; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за безпеку персоналу; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для забезпечення дійсних дозволів на доступ до інформації, що вимагає особливого захисту; організаційний процес для додаткового відбору персоналу для інформації, що вимагає особливого захисту].	

PS-3(4)	ПЕРЕВІРКА ПЕРСОНАЛУ - ВИМОГИ ДО ГРОМАДЯНСТВА	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PS-03(04)_ODP[01]	**доступ осіб до систем відповідає типу інформації, яка обробляється, зберігається або передається системою;**
	PS-03(04)_ODP[02]	**визначені вимоги щодо громадянства, яким повинні відповідати особи з доступои до системи, де обробляється, зберігається або передається інформація;**
	PS-03(04)	відповідають особи, які мають доступ до системи, що обробляє, зберігає або передає **<PS-03(04)_ODP[01] типи інформації>**, **<PS-03(04)_ODP[02] вимогам щодо громадянства>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика безпеки персоналу; політика контролю доступу, процедури, що стосуються перевірки персоналу; записи про перевірений персонал; критерії скринінгу; записи дозволів на доступ; інші відповідні документи або	

	записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за безпеку персоналу; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для забезпечення дійсних дозволів на доступ до інформації, що вимагає особливого захисту; організаційний процес для додаткового відбору персоналу для інформації, що вимагає особливого захисту].

PS-4	**ЗВІЛЬНЕННЯ ПЕРСОНАЛУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PS-04_ODP[01]	**визначено період часу, протягом якого забороняється доступ до системи;**
	PS-04_ODP[02]	**визначені теми інформаційної безпеки для обговорення під час проведення співбесід;**
	PS-04a.	при звільненні працівника доступ до системи вимикається протягом **<PS-04_ODP[01] часового періоду>**;
	PS-04b.	припиняють дію або анулюють будь-які автентифікатори та облікові дані після припинення трудових відносин з окремими особами;
	PS-04c.	проводяться при звільненні окремих працівників співбесіди, які включають обговорення **<PS-04_ODP[02] питань інформаційної безпеки>**;
	PS-04d.	отримується після звільнення особи все майно, пов'язане з безпекою організаційної системи;
	PS-04e.	зберігається доступ до організаційної інформації та систем, які раніше перебували під контролем особи, що звільняється, після припинення нею трудових відносин.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика безпеки персоналу; політика контролю доступу, процедури, що стосуються перевірки персоналу; записи про перевірений персонал; критерії скринінгу; записи дозволів на доступ; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за безпеку персоналу; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для забезпечення дійсних дозволів на доступ до інформації, що вимагає особливого захисту; організаційний процес для додаткового відбору персоналу для інформації, що вимагає особливого захисту].	

PS-4(1)	**ЗВІЛЬНЕННЯ ПЕРСОНАЛУ - ВИМОГИ ПІСЛЯ ЗАКІНЧЕННЯ ТРУДОВОЇ ДІЯЛЬНОСТІ**
	МЕТА ОЦІНКИ:

	Визначити, чи:	
	PS-04(01)(a)	зберігається доступ до інформації організації та в системі, під контролем особи, що звільняється, після припинення з нею трудових відносин;
	PS-04(01)(b)	потрібно звільненим особам підписувати підтвердження вимог щодо працевлаштування в рамках процесу припинення діяльності організації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика безпеки персоналу; процедури, що стосуються звільнення персоналу; записи про припинення роботи персоналу; перелік рахунків системи; записи припинених або анульованих автентифікаторів, посвідчень; записи виїзних співбесід; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за безпеку персоналу; персонал організації, відповідальний за управління рахунками; адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації припинення персоналу; автоматизовані механізми, що підтримують та, або впроваджують повідомлення про припинення роботи персоналу; автоматизовані механізми відключення доступу до системи, скасування автентифікаторів].	

PS-4(2)	**ЗВІЛЬНЕННЯ ПЕРСОНАЛУ - АВТОМАТИЗОВАНЕ СПОВІЩЕННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PS-04(02)_ODP[01]	**визначені автоматизовані механізми сповіщення персоналу або ролей про окремі дії з припинення роботи та/або заборони доступу до ресурсів системи;**
	PS-04(02)_ODP[02]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {повідомляти <PS-04(02)_ODP[03] персонал або ролі> про окремі дії завершення; взаборони доступу до системних ресурсів};**
	PS-04(02)_ODP[03]	**визначено персонал або ролі, про які необхідно повідомляти при звільненні особи (якщо визначено);**
	PS-04(02)	використовуються **<PS-04(02)_ODP[01] автоматизовані механізми>** для **<PS-04(02)_ODP[02] ВИБРАНОГО ЗНАЧЕННЯ ПАРАМЕТРА(ів)>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика безпеки персоналу; процедури, що стосуються звільнення персоналу; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи про припинення персоналу; автоматизовані повідомлення про звільнення працівників; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за забезпечення	

	персоналу; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації звільнення персоналу; автоматизовані механізми, що підтримують та, або впроваджують повідомлення про припинення персоналу].

PS-5	**ПЕРЕВЕДЕННЯ ПЕРСОНАЛУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PS-05_ODP[01]	**визначені дії, які мають бути ініційовані після переведення або перепризначення;**
	PS-05_ODP[02]	**визначено період часу, протягом якого мають бути здійснені дії з переведення або перепризначення після переведення або перепризначення;**
	PS-05_ODP[03]	**визначено персонал або ролі, про які необхідно повідомляти, коли осіб призначають на інші посади або переводять на інші посади в організації;**
	PS-05_ODP[04]	**визначено період часу, протягом якого необхідно повідомляти визначений організацією персонал або ролі, коли осіб перепризначають або переводять на інші посади в межах організації;**
	PS-05a.	переглядаються та підтверджуються поточні потреби в логічних та фізичних дозволах на доступ до систем та об'єктів при перепризначенні або переведенні осіб на інші посади в організації;
	PS-05b.	були ініційовані **<PS-05_ODP[01] дії з переведення або перепризначення>** протягом **<PS-05_ODP[02] періоду часу після формальної дії з переведення>**;
	PS-05c.	змінюється авторизація доступу за необхідності, щоб відповідати будь-яким змінам в оперативних потребах у зв'язку з перепризначенням або переведенням;
	PS-05d.	було повідомлено **<PS-05_ODP[03] персонал або ролі>** протягом **<PS-05_ODP[04] часового періоду>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика безпеки персоналу; процедури, що стосуються звільнення персоналу; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи про припинення персоналу; автоматизовані повідомлення про звільнення працівників; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за забезпечення персоналу; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації звільнення персоналу; автоматизовані механізми, що підтримують та, або впроваджують повідомлення про припинення	

	персоналу].

PS-6	**УГОДИ ПРО ДОСТУП**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PS-06_ODP[01]	**визначено періодичність перегляду та оновлення угод про доступ;**
	PS-06_ODP[02]	**визначена періодичність перепідписання угод про доступ для збереження доступу до інформації організації;**
	PS-06a.	розроблені та задокументовані угоди про доступ до систем організації;
	PS-06b.	переглядаються та оновлюються угоди про доступ **<PS-06_ODP[01] частота>**;
	PS-06c.01	підписують особи, яким потрібен доступ до інформації та систем організації, відповідні угоди про доступ до того, як їм буде надано доступ;
	PS-06c.02	перепідписують особи, яким потрібен доступ до інформації та систем організації, угоди про доступ для збереження доступу до систем організації, коли угоди про доступ були оновлені чи як **<PS-06_ODP[02] частота>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика безпеки персоналу; процедури, що стосуються угод про доступ до організаційної інформації та інформаційних систем; план захисту інформації; угоди про доступ; записи оглядів та оновлень угоди про доступ; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за безпеку персоналу; персонал організації, який підписав, відмовившийся від угоди про доступ; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для угод про доступ; автоматизовані механізми, що підтримують договори про доступ].	

PS-6(1)	**УГОДИ ПРО ДОСТУП - ІНФОРМАЦІЯ, ЩО ВИМАГАЄ СПЕЦІАЛЬНОГО ЗАХИСТУ**
	[Вилучено: включено до PS-3]

PS-6(2)	**УГОДИ ПРО ДОСТУП - ІНФОРМАЦІЯ З ОБМЕЖЕНИМ ДОСТУПОМ, ЩО ВИМАГАЄ СПЕЦІАЛЬНОГО ЗАХИСТУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PS-06(02)(a)	надається доступ до інформації з обмеженим доступом, що потребує спеціального захисту, лише особам, які мають

		дійсний дозвіл на доступ, що підтверджується покладеними на них офіційними державними обов'язками;
	PS-06(02)(b)	надається доступ до інформації з обмеженим доступом, що потребує спеціального захисту, лише особам, які відповідають відповідним критеріям кадрової безпеки;
	PS-06(02)(c)	надається доступ до інформації з обмеженим доступом, що потребує спеціального захисту, лише особам, які прочитали, зрозуміли та підписали угоду про нерозголошення.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика безпеки персоналу; процедури, що стосуються угод про доступ до організаційної інформації та інформаційних систем; угоди про доступ; дозволи на доступ; критерії безпеки персоналу; підписані угоди про нерозголошення інформації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за безпеку персоналу; персонал організації, який підписав угоди про нерозголошення інформації; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації доступу до секретної інформації, що потребує особливого захисту].	

PS-6(3)	**УГОДИ ПРО ДОСТУП - ВИМОГИ ПІСЛЯ ЗАКІНЧЕННЯ ТРУДОВОЇ ДІЯЛЬНОСТІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PS-06(03)(a)	повідомляють людей про застосовні, юридично обов'язкові вимоги щодо захисту інформації організації після закінчення трудової діяльності;
	PS-06(03)(b)	повинні особи підписувати визнання застосовних, юридично обов'язкових вимог після звільнення як частину надання первинного доступу до інформації з обмеженим доступом.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика безпеки персоналу; процедури, що стосуються угод про доступ до організаційної інформації та інформаційних систем; підписані бланки підтвердження після працевлаштування; угоди про доступ; перелік чинних, юридично обов'язкових вимог після працевлаштування; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за безпеку персоналу; персонал організації, який підписав угоди про доступ, що включають вимоги після закінчення роботи; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації, що відповідають вимогам після працевлаштування; автоматизовані механізми, що підтримують повідомлення та індивідуальні підтвердження вимог після закінчення роботи].	

PS-7	БЕЗПЕКА ЗОВНІШНЬОГО ПЕРСОНАЛУ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PS-07_ODP[01]	**визначено персонал або ролі, які мають бути повідомлені про будь-які кадрові переведення або звільнення зовнішнього персоналу, який володіє організаційними повноваженнями та/або бейджами, або має системні привілеї;**
	PS-07_ODP[02]	**визначено період часу, протягом якого сторонні провайдери повинні повідомляти визначений організацією персонал або ролі про будь-які кадрові переведення або звільнення зовнішнього персоналу, який володіє організаційними повноваженнями та/або бейджами або має системні привілеї;**
	PS-07a.	встановлені вимоги до безпеки персоналу, включаючи ролі та обов'язки зовнішніх постачальників послуг у сфері безпеки;
	PS-07b.	зобов'язані зовнішні провайдери дотримуватися політики та процедур кадрової безпеки, встановлених організацією;
	PS-07c.	задокументовані вимоги до безпеки персоналу;
	PS-07d.	зобов'язані зовнішні провайдери повідомляти **<PS-07_ODP[01] персонал або ролі>** про будь-які кадрові переведення або звільнення зовнішнього персоналу, який володіє організаційними повноваженнями та/або бейджами або має системні привілеї протягом **<PS-07_ODP[02] часового періоду>**;
	PS-07e.	контролюється дотримання провайдером вимог щодо безпеки персоналу.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика безпеки персоналу; процедури, що стосуються угод про доступ до організаційної інформації та інформаційних систем; підписані бланки підтвердження після працевлаштування; угоди про доступ; перелік чинних, юридично обов'язкових вимог після працевлаштування; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за безпеку персоналу; персонал організації, який підписав угоди про доступ, що включають вимоги після закінчення роботи; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації, що відповідають вимогам після працевлаштування; автоматизовані механізми, що підтримують повідомлення та індивідуальні підтвердження вимог після закінчення роботи].	

PS-8	КАДРОВІ САНКЦІЇ

	МЕТА ОЦІНКИ: Визначити, чи:	
	PS-08_ODP[01]	**визначено персонал або ролі, про які необхідно повідомляти, коли ініціюється офіційний процес санкцій щодо працівників;**
	PS-07_ODP[02]	**визначено період часу, протягом якого визначений організацією персонал або ролі повинні бути повідомлені про початок офіційного процесу застосування санкцій до працівника;**
	PS-08a.	застосовується офіційний процес санкцій до осіб, які не дотримуються встановлених політик і процедур інформаційної безпеки та конфіденційності;
	PS-08b.	було повідомлено **<PS-08_ODP[01] персонал або ролі>** протягом **<PS-08_ODP[02] періоду часу>**, коли розпочато офіційний процес застосування санкцій до працівників, із зазначенням особи, до якої застосовано санкції, та причини санкцій.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика безпеки персоналу; процедури, що стосуються кадрових санкцій; правила поведінки; записи формальних санкцій; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за безпеку персоналу; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для управління кадровими санкціями; автоматизовані механізми підтримки та, або реалізації повідомлень].	

PS-9	**ОПИС ПОЗИЦІЙ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PS-09[01]	включені функції та обов'язки з безпеки в описи посадових осіб в організації;
	PS-09[02]	включені ролі та обов'язки щодо конфіденційності в описи посадових осіб в організації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика безпеки персоналу; процедури безпеки персоналу; процедури, що стосуються посадових інструкцій; посадові інструкції з питань безпеки та конфіденційності; план захисту інформації системи; план забезпечення конфіденційності; план програми забезпечення конфіденційності; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за безпеку персоналу; персонал організації, відповідальний за інформаційну безпеку та конфіденційність; персонал організації, відповідальний за управління людським капіталом].	

	Перевірка: [ВИБІР: Процеси організації управління посадовими інструкціями].

XV. КЛАС ЗАХОДІВ ЗАХИСТУ PT — ПОВНОВАЖЕННЯ НА ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ

PT-1	**ПОЛІТИКА ТА ПРОЦЕДУРИ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PT-01_ODP[01]	**визначено персонал або ролі, на які поширюється політика обробки персональних даних та забезпечення прозорості;**
	PT-01_ODP[02]	**визначено персонал або ролі, на які поширюються процедури обробки персональних даних та політики прозорості;**
	PT-01_ODP[03]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {рівень організації; рівень місії/бізнес-процесу; рівень системи};**
	PT-01_ODP[04]	**визначено посадову особу, яка керуватиме політикою та процедурами обробки персональних даних, а також політикою та процедурами прозорості;**
	PT-01_ODP[05]	**визначена періодичність перегляду та оновлення поточної політики обробки та прозорості інформації, що ідентифікує особу;**
	PT-01_ODP[06]	**є події, які вимагають перегляду та оновлення поточної політики обробки персональних даних та прозорості;**
	PT-01_ODP[07]	**визначена частота, з якою переглядаються та оновлюються поточні процедури обробки персональних даних та забезпечення прозорості;**
	PT-01_ODP[08]	**визначені події, які вимагають перегляду та оновлення процедур обробки персональних даних та забезпечення прозорості;**
	PT-01a.[01]	розроблена та задокументована політика обробки персональних даних та прозорості;
	PT-01a.[02]	поширюється політика обробки персональних даних та прозорості на **<PT-01_ODP[01] персонал або ролі>**;
	PT-01a.[03]	розроблені та задокументовані процедури обробки персональних даних та забезпечення прозорості, що сприяють впровадженню політики обробки персональних даних та забезпечення прозорості, а також пов'язані з ними засоби контролю обробки персональних даних та забезпечення прозорості;
	PT-01a.[04]	поширюються процедури обробки персональних даних та забезпечення прозорості на **<PT-01_ODP[02] персонал або ролі>**;
	PT-01a.01(a)[01]	відповідає **<PT-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ**

		ПАРАМЕТРА(ів)> політика обробки та прозорості інформації, що ідентифікує особу, поставленій меті;
	PT-01a.01(a)[02]	політика обробки та прозорості персональних даних **<PT-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** регулює сферу застосування;
	PT-01a.01(a)[03]	політика обробки та прозорості персональних даних **<PT-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** стосується ролей;
	PT-01a.01(a)[04]	стосується політика обробки персональних даних та прозорості **<PT-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** обов'язків щодо обробки персональних даних;
	PT-01a.01(a)[05]	відповідає політика обробки персональних даних та прозорості **<PT-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** зобов'язанням керівництва щодо обробки персональних даних та прозорості;
	PT-01a.01(a)[06]	передбачає політика обробки персональних даних та прозорості **<PT-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** координацію між структурними підрозділами організації;
	PT-01a.01(a)[07]	стосується політика обробки персональних даних та прозорості **<PT-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** дотримання вимог щодо обробки персональних даних та прозорості;
	PT-01a.01(b)	відповідає **<PT-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** політика обробки та прозорості персональних даних чинному законодавству, виконавчим наказам, директивам, нормативним актам, політикам, стандартам та настановам;
	PT-01b.	призначено **<Посадову особу <PT-01_ODP[04]>** для управління розробкою, документуванням та розповсюдженням політики та процедур обробки персональних даних та забезпечення прозорості;
	PT-01c.01[01]	переглядається та оновлюється поточна політика обробки та прозорості персональних даних **<PT-01_ODP[05] періодичність>**;
	PT-01c.01[02]	переглядається та оновлюється поточна політика обробки персональних даних та прозорості після подій **<PT-01_ODP[06]>**;
	PT-01c.02[01]	переглядаються та оновлюються поточні процедури обробки персональних даних та забезпечення прозорості **<PT-01_ODP[07] частота>**;
	PT-01c.02[02]	переглядаються та оновлюються поточні процедури обробки персональних даних та забезпечення прозорості після **<PT-01_ODP[08] подія >**.

	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика та процедури обробки персональних даних та забезпечення прозорості; план забезпечення конфіденційності; план програми забезпечення конфіденційності; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за обробку персональних даних та забезпечення прозорості; персонал організації, відповідальний за інформаційну безпеку та конфіденційність].

PT-2	**ПОВНОВАЖЕННЯ НА ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PT-02_ODP[01]	**визначені повноваження щодо надання дозволу на обробку (визначені в PT-02_ODP[02]) персональних даних;**
	PT-02_ODP[02]	**визначено тип обробки персональних даних;**
	PT-02_ODP[03]	**визначено тип обробки персональних даних, що підлягають обмеженню;**
	PT-02a.	визначено та задокументовано **<PT-02_ODP[01] орган>**, який дозволяє **<PT-02_ODP[02] обробку> персональних даних**;
	PT-02b.	**<PT-02_ODP[03] обробка>** персональних даних, обмежується лише таким чином, яким дозволено.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика та процедури обробки персональних даних та забезпечення прозорості; план забезпечення конфіденційності; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за обробку персональних даних та забезпечення прозорості; персонал організації, відповідальний за інформаційну безпеку та конфіденційність]. **Перевірка**: [ВИБІР: Процеси організації надання дозволів на обробку персональних даних; механізми, що підтримують та/або реалізують обмеження обробки персональних даних].	

PT-2(1)	**ПОВНОВАЖЕННЯ НА ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ - ТЕГУВАННЯ ДАНИХ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PT-	**включені функції та обов'язки з безпеки в описи посадових осіб в організації;**

	02(01)_ODP[01]	
	PT-02(01)_ODP[02]	**включені ролі та обов'язки щодо конфіденційності в описи посад в організації.**
	PT-02(01)	теги даних, що містять **<PT-02(01) _ODP[01] санкціонована обробка>**, прикріплені до **<PT-02(01) _ODP[02] елементів інформації, що іденти0фікує особу>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика та процедури обробки інформації, що дозволяє ідентифікувати особу, та забезпечення прозорості, включаючи процедури, що стосуються тегування даних; визначення тегів даних; задокументовані вимоги щодо використання та моніторингу тегування даних; витяги даних з відповідними тегами даних; план забезпечення конфіденційності; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за обробку персональних даних та забезпечення прозорості; персонал організації, відповідальний за інформаційну безпеку та конфіденційність]. **Перевірка**: [ВИБІР: Процеси організації надання дозволів на обробку персональних даних; організаційні процеси маркування даних; механізми застосування та моніторингу маркування даних; механізми підтримки та/або реалізації обмежень на обробку персональних даних].	

PT-2(2)	**ПОВНОВАЖЕННЯ НА ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ - АВТОМАТИЗАЦІЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PT-02(02)_ODP	**визначені автоматизовані механізми, які використовуються для управління дотриманням санкціонованої обробки інформації, що ідентифікує особу;**
	PT-02(02)	управління дотриманням санкціонованої обробки персональних даних здійснюється за допомогою **<PT-02(02)_ODP автоматизовані механізми обробки персональних даних>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика та процедури обробки персональних даних та забезпечення прозорості; план забезпечення конфіденційності; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за обробку персональних даних та забезпечення прозорості; персонал організації, відповідальний за інформаційну безпеку та конфіденційність]. **Перевірка**: [ВИБІР: Процеси організації санкціонування обробки персональних даних; автоматизовані механізми, що підтримують та/або реалізують управління	

	санкціонованою обробкою персональних даних].

PT-3	**ЦІЛІ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PT-03_ODP[01]	**визначено мету (цілі) обробки персональних даних;**
	PT-03_ODP[02]	**визначена обробка персональних даних, яка підлягає обмеженню;**
	PT-03_ODP[03]	**визначені механізми, які мають бути впроваджені для забезпечення того, щоб будь-які зміни в персональних данних, вносилися відповідно до вимог;**
	PT-03_ODP[04]	**визначені вимоги до зміни обробкиперсональних даних;**
	PT-03a.	визначено та задокументовано **<PT-03_ODP[01] мету (цілі) >** обробки персональних даних;
	PT-03b.[01]	описана мета (цілі) в публічних повідомленнях про конфіденційність організації;
	PT-03b.[02]	описана мета (цілі) в політиці організації;
	PT-03c	**<PT-03_ODP[02] обробка>** персональних даних, обмежується лише тим, що є сумісним з визначеною метою (цілями);
	PT-03d.[01]	здійснюється моніторинг змін в обробці персональних даних;
	PT-03d.[02]	впроваджено **<PT-03_ODP[03] механізми** > для забезпечення того, щоб будь-які зміни вносилися відповідно до **<PT-03_ODP[04] вимог>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика та процедури обробки персональних даних і забезпечення прозорості; план управління конфігурацією; організаційні повідомлення про конфіденційність; організаційні політики; заяви про Закон про конфіденційність; повідомлення про комп'ютерні збіги; відповідні повідомлення Федерального реєстру; задокументовані вимоги щодо забезпечення дотримання та моніторингу обробки персональних даних; план забезпечення конфіденційності; інші відповідні документи чи записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за обробку персональних даних та забезпечення прозорості; персонал організації, відповідальний за інформаційну безпеку та конфіденційність]. **Перевірка**: [ВИБІР: Процеси організації санкціонування обробки персональних	

	даних; механізми підтримки та/або реалізації управління санкціонованою обробкою персональних даних; організаційні процеси моніторингу змін в обробці персональних даних].

PT-3(1)	**ЦІЛІ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ - ТЕГУВАННЯ ДАНИХ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PT-03(01)_ODP[01]	**визначені цілі обробки, які повинні міститися в тегах даних;**
	PT-03(01)_ODP[02]	**визначені елементи персональних даних, які підлягають тегуванню;**
	PT-03(01)	теги даних, що містять **<PT-03(01) _ODP[01] цілі обробки>**, приєднані до **<PT-03(01) _ODP[02] елементів інформації, що ідентифікує особу>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика та процедури обробки та прозорості інформації, що дозволяє ідентифікувати особу; задокументований опис того, як теги даних використовуються для ідентифікації елементів даних, що дозволяють ідентифікувати особу, та їх санкціоноване використання; схема тегів даних; витяги даних з відповідними тегами даних; план забезпечення конфіденційності; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за обробку персональних даних та забезпечення прозорості; персонал організації, відповідальний за маркування даних; персонал організації, відповідальний за інформаційну безпеку та конфіденційність]. **Перевірка**: [ВИБІР: Процеси організації для надання дозволу на обробку інформації, що ідентифікує особу; механізми, що підтримують та/або впроваджують тегування даних].	

PT-3(2)	**ЦІЛІ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ - АВТОМАТИЗАЦІЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PT-03(02)_ODP	**визначені автоматизовані механізми відстеження цілей обробки персональних даних;**
	PT-03(02)	відстежуються цілі обробки персональних даних за допомогою **<PT-03(02)_ODP автоматизованих механізмів>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ:	

	Дослідження: [ВИБІР: Політика та процедури обробки персональних даних та забезпечення прозорості; витяги даних з відповідними тегами даних; план забезпечення конфіденційності; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за обробку персональних даних та забезпечення прозорості; персонал організації, відповідальний за інформаційну безпеку та конфіденційність]. **Перевірка**: [ВИБІР: Процеси організації управління дотриманням санкціонованої обробки персональних даних; автоматизовані механізми відстеження].

PT-4	**ЗГОДА НА ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PT-04_ODP	**визначені інструменти або механізми, які мають бути застосовані для надання особами згоди на обробку їхніх персональних даних;**
	PT-04	впроваджено **<PT-04_ODP інструменти або механізми>** для надання фізичними особами згоди на обробку їхніх персональних даних до її збору, які сприяють прийняттю фізичними особами поінформованих рішень.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика та процедури обробки та прозорості інформації, що ідентифікує особу; політика та процедури надання згоди; інструменти та механізми надання згоди; представлення або відображення згоди (користувацький інтерфейс); докази згоди осіб; план забезпечення конфіденційності; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за обробку персональних даних та забезпечення прозорості; персонал організації, відповідальний за інформаційну безпеку та конфіденційність]. **Перевірка**: [ВИБІР: Процеси організації збору інформації, що ідентифікує особу; інструменти згоди або механізми надання користувачами дозволу на обробку їхньої інформації, що ідентифікує особу; механізми імплементації згоди].	

PT-4(1)	**ЗГОДА НА ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ - ІНДИВІДУАЛЬНА ЗГОДА НА ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PT-04(01)_ODP	**визначені механізми адаптації для обробки окремих елементів дозволів персональних даних;**

	PT-04(01)	передбачені **<PT-04(01)_ODP механізми>**, які дозволяють особам пристосовувати дозволи на обробку до вибраних елементів персональних даних;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика та процедури обробки та прозорості інформації, що ідентифікує особу; політика та процедури надання згоди; інструменти та механізми надання згоди; презентація або відображення згоди (користувацький інтерфейс); план забезпечення конфіденційності; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за обробку персональних даних та прозорість; персонал організації, відповідальний за користувацький інтерфейс або взаємодію з користувачами; персонал організації, відповідальний за інформаційну безпеку та конфіденційність]. **Перевірка**: [ВИБІР: Процеси організації отримання згоди на обробку персональних даних; інструменти або механізми отримання згоди; механізми реалізації згоди].	

PT-4(2)	**ЗГОДА НА ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ - СВОЄЧАСНА ЗГОДА НА ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PT-04(02)_ODP[01]	**визначені механізми надання згоди, які мають бути надані особами;**
	PT-04(02)_ODP[02]	визначена частота, з якою необхідно представляти механізми надання згоди особам;
	PT-04(02)_ODP[03]	визначена обробка персональних даних, яка має бути представлена у поєднанні з визначеними організацією механізмами надання згоди;
	PT-04(02)	надаються **<PT-04(02)_ODP[01] механізми згоди>** особам **<PT-04(02)_ODP[02] частота>** та в поєднанні з **<PT-04(02)_ODP[03] обробкою персональних даних>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика та процедури обробки та прозорості інформації, що ідентифікує особу; політика та процедури надання згоди; план забезпечення конфіденційності; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за обробку персональних даних та прозорість; персонал організації, відповідальний за користувацький інтерфейс або взаємодію з користувачами; персонал організації, відповідальний за інформаційну безпеку та конфіденційність]. **Перевірка**: [ВИБІР: Процеси організації збору персональних даних; механізми	

	отримання своєчасної згоди користувачів на обробку їхніх персональних даних; механізми реалізації своєчасної згоди користувачів на обробку їхніх персональних даних].

PT-4(3)	**ЗГОДА НА ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ - ВІДКЛИКАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PT-04(03)_ODP	**визначені інструменти або механізми для відкликання згоди на обробку персональних даних;**
	PT-04(03)	впроваджено **<PT-04(03)_ODP інструменти або механізми>**, які дозволяють фізичним особам відкликати згоду на обробку їхніх персональних даних.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика та процедури обробки персональних даних і забезпечення прозорості; політика та процедури відкликання згоди; користувацький інтерфейс або досвід користувача щодо відкликання згоди; план забезпечення конфіденційності; інші відповідні документи або записи].**Співбесіда**: [ВИБІР: Персонал організації, відповідальний за обробку персональних даних та прозорість; персонал організації, відповідальний за користувацький інтерфейс або взаємодію з користувачами; персонал організації, відповідальний за інформаційну безпеку та конфіденційність]. **Перевірка**: [ВИБІР: Процеси організації надання згоди на обробку персональних даних; інструменти або механізми реалізації відкликання згоди].	

PT-5	**ПОВІДОМЛЕННЯ ПРО КОНФІДЕНЦІЙНІСТЬ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PT-05_ODP[01]	**визначена частота, з якою повідомлення надається особам на рівні первинної взаємодії з організацією;**
	PT-05_ODP[02]	**визначена інформація, яка повинна бути включена до повідомлення про обробку персональних даних;**
	PT-05a.[01]	направляється особам повідомлення про обробку персональних даних таким чином, щоб вони могли ознайомитися з ним при першій взаємодії з організацією;
	PT-05a.[02]	направляється повідомлення фізичним особам про обробку пермональних даних, таким чином, щоб це повідомлення було згодом доступне фізичним особам **<PT-05_ODP[01] частота>**;

	PT-05b.	направляється фізичним особам повідомлення про обробку персональних даних, яке є чітким, легким для розуміння та містить інформацію про обробку персональних даних простою мовою;
	PT-05c.	направляється фізичним особам повідомлення про обробку персональних даних, яке визначає орган, що надає дозвіл на обробку персональних даних;
	PT-05d.	направляється повідомлення фізичним особам про обробку персональних даних, в якому вказується мета, з якою буде оброблятися персональна інформація;
	PT-05e.	направляється повідомлення фізичним особам про обробку персональних даних, які включають **<PT-05_ODP[02] інформацію>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика та процедури обробки персональних даних і забезпечення прозорості; повідомлення про конфіденційність; заяви про Закон про конфіденційність; план забезпечення конфіденційності; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за обробку персональних даних та прозорість; персонал організації, відповідальний за користувацький інтерфейс або взаємодію з користувачами; персонал організації, відповідальний за інформаційну безпеку та конфіденційність]. **Перевірка**: [ВИБІР: Процеси організації надання згоди на обробку персональних даних; інструменти або механізми реалізації відкликання згоди].	

PT-5(1)	**ПОВІДОМЛЕННЯ ПРО КОНФІДЕНЦІЙНІСТЬ - СВОЄЧАСНЕ ПОВІДОМЛЕННЯ ПРО КОНФІДЕНЦІЙНІСТЬ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PT-05(01)_ODP	**визначена періодичність подання повідомлення про обробку персональних даних;**
	PT-05(01)	надається повідомлення про обробку персональних даних особам у той час і в тому місці, де особа надає персональні дані, у зв'язку з якою здійснюється дія з даними, або періодичність обробки даних **<PT-05(01)_ODP частота>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика та процедури обробки персональних даних і забезпечення прозорості; повідомлення про конфіденційність; план забезпечення конфіденційності; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за обробку	

	персональних даних та прозорість; персонал організації, відповідальний за користувацький інтерфейс або взаємодію з користувачами; персонал організації, відповідальний за інформаційну безпеку та конфіденційність]. **Перевірка**: [ВИБІР: Процеси організації та імплементаційна підтримка або механізми надання повідомлень особам про обробку їхніх персональних даних].

PT-5(2)	**ПОВІДОМЛЕННЯ ПРО КОНФІДЕНЦІЙНІСТЬ - ЗАЯВИ ПРО КОНФІДЕНЦІЙНІСТЬ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PT-05(02)	включаються повідомлення про конфіденційність у форми, які збирають інформацію, що буде зберігатися в системі записів Закону про конфіденційність, або ж заяви про конфіденційність надаються на окремих формах, які можуть зберігатися у приватних осіб.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика та процедури обробки персональних даних і забезпечення прозорості; повідомлення про конфіденційність; план забезпечення конфіденційності; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за обробку персональних даних та прозорість; персонал організації, відповідальний за користувацький інтерфейс або взаємодію з користувачами; персонал організації, відповідальний за інформаційну безпеку та конфіденційність]. **Перевірка**: [ВИБІР: Процеси організації та імплементаційна підтримка або механізми надання повідомлень особам про обробку їхніх персональних даних].	

PT-6	**СИСТЕМА ЗАПИСІВ ПОВІДОМЛЕНЬ ПРО КОНФІДЕНЦІЙНІСТЬ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PT-06a.[01]	повідомлення про систему записів складено відповідно до вказівок OMB для систем, які обробляють інформацію, що зберігатиметься в системі записів відповідно до законодавства;
	PT-06a.[02]	подаються повідомлення про нові та суттєво змінені системи записів до OMB та відповідних комітетів для попереднього розгляду для систем, які обробляють інформацію, що буде зберігатися в записах системи;
	PT-06b.	публікуються повідомлення про систему записів у Державному реєстрі систем, які обробляють інформацію, що зберігатиметься в системі записів відповідно до до

		законодавства;
	PT-06c.	зберігаються повідомлення в системі записів точними, актуальними та в повному обсязі відповідно до політики для систем, які обробляють інформацію, що буде зберігатися в системі записів згідно із законодавством.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика та процедури обробки персональних даних і забезпечення прозорості; повідомлення про конфіденційність; план забезпечення конфіденційності; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за обробку персональних даних та прозорість; персонал організації, відповідальний за користувацький інтерфейс або взаємодію з користувачами; персонал організації, відповідальний за інформаційну безпеку та конфіденційність]. **Перевірка**: [ВИБІР: Процеси організації та імплементаційна підтримка або механізми надання повідомлень особам про обробку їхніх персональних даних].	

PT-6(1)	**СИСТЕМА ЗАПИСІВ ПОВІДОМЛЕНЬ ПРО КОНФІДЕНЦІЙНІСТЬ - ЗВИЧАЙНЕ ВИКОРИСТАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PT-06(01)_ODP	**визначено періодичність перегляду всіх звичайних видів використання, опублікованих у системі обліку повідомлень;**
	PT-06(01)	переглядаються всі звичайні види використання, опубліковані в повідомленні системи записів **<PT-06(01)_ODP періодичність>**, для забезпечення постійної точності, а також для забезпечення того, щоб звичайні види використання і надалі були сумісними з метою, для якої була зібрана інформація.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика та процедури обробки персональних даних і забезпечення прозорості; повідомлення про конфіденційність; план забезпечення конфіденційності; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за обробку персональних даних та прозорість; персонал організації, відповідальний за користувацький інтерфейс або взаємодію з користувачами; персонал організації, відповідальний за інформаційну безпеку та конфіденційність]. **Перевірка**: [ВИБІР: Процеси організації та імплементаційна підтримка або механізми надання повідомлень особам про обробку їхніх персональних даних].	

PT-6(2)	**СИСТЕМА ЗАПИСІВ ПОВІДОМЛЕНЬ ПРО КОНФІДЕНЦІЙНІСТЬ -**

	ПРАВИЛА ЗВІЛЬНЕННЯ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PT-06(02)_ODP	**визначено періодичність перегляду всіх винятків із Закону про конфіденційність, заявлених для системи записів;**
	PT-06(02)[01]	всі винятки із Закону про конфіденційність, заявлені для системи записів, переглядаються **<PT-06(02)_ODP частота>**, щоб переконатися, що вони залишаються доречними та необхідними відповідно до закону;
	PT-06(02)[02]	всі винятки із Закону про конфіденційність, заявлені для системи записів, переглядаються **<PT-06(02)_ODP частота>**, щоб переконатися, що вони були оприлюднені як нормативні акти;
	PT-06(02)[03]	всі винятки із Закону про конфіденційність, заявлені для системи записів, переглядаються <**PT-06(02)_ODP частота>**, щоб переконатися, що вони точно описані в повідомленні про систему записів.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика та процедури обробки персональних даних і забезпечення прозорості; повідомлення про конфіденційність; план забезпечення конфіденційності; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за обробку персональних даних та прозорість; персонал організації, відповідальний за користувацький інтерфейс або взаємодію з користувачами; персонал організації, відповідальний за інформаційну безпеку та конфіденційність]. **Перевірка**: [ВИБІР: Процеси організації та імплементаційна підтримка або механізми надання повідомлень особам про обробку їхніх персональних даних].	

PT-7	**СПЕЦІАЛЬНІ КАТЕГОРІЇ ПЕРСОНАЛЬНИХ ДАНИХ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PT-07_ODP	**визначені умови обробки, що застосовуються до певних категорій персональних даних;**
	PT-07	застосовуються **<PT-07_ODP умови обробки>** до певних категорій персональних даних.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика та процедури обробки персональних даних і забезпечення прозорості; повідомлення про конфіденційність; план забезпечення конфіденційності; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за обробку	

	персональних даних та прозорість; персонал організації, відповідальний за користувацький інтерфейс або взаємодію з користувачами; персонал організації, відповідальний за інформаційну безпеку та конфіденційність]. **Перевірка**: [ВИБІР: Процеси організації та імплементаційна підтримка або механізми надання повідомлень особам про обробку їхніх персональних даних].

PT-7(1)	**СПЕЦІАЛЬНІ КАТЕГОРІЇ ПЕРСОНАЛЬНИХ ДАНИХ - НОМЕРИ СОЦІАЛЬНОГО СТРАХУВАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PT-07(01)(a)[01]	при обробці системою номерів соціального страхування усувається непотрібний збір, зберігання та використання номерів соціального страхування;
	PT-07(01)(a)[02]	вивчаються альтернативи використанню номерів соціального страхування в якості персонального ідентифікатора, коли система обробляє їх;
	PT-07(01)(b)	не відмовляється система при обробці номерів соціального страхування в індивідуальних правах, пільгах або привілеях, передбачених законом, через відмову особи розкрити свій номер соціального страхування;
	PT-07(01)(c)[01]	при обробці системою номерів соціального страхування кожну особу, яку просять розкрити свій номер соціального страхування, інформують про те, чи є таке розкриття обов'язковим чи добровільним, яким законодавчим чи іншим органом запитується такий номер, і як він буде використовуватися;
	PT-07(01)(c)[02]	при обробці системою номерів соціального страхування кожну особу, яку просять розкрити свій номер соціального страхування, інформують про те, яким законодавчим чи іншим органом запитується цей номер;
	PT-07(01)(c)[03]	при обробці системою номерів соціального страхування кожну особу, яку просять розкрити свій номер соціального страхування, інформують про те, як він буде використовуватися.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика та процедури обробки персональних даних і забезпечення прозорості; повідомлення про конфіденційність; система записів Закону про конфіденційність; окреме повідомлення про використання номерів соціального страхування; план забезпечення конфіденційності; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за обробку персональних даних та прозорість; персонал організації, відповідальний за користувацький інтерфейс або взаємодію з користувачами; персонал організації,	

	відповідальний за інформаційну безпеку та конфіденційність]. **Перевірка**: [ВИБІР: Процеси організації та імплементаційна підтримка або механізми надання повідомлень особам про обробку їхніх персональних даних].

PT-7(2)	**СПЕЦІАЛЬНІ КАТЕГОРІЇ ПЕРСОНАЛЬНИХ ДАНИХ - ІНФОРМАЦІЯ ПРО ПЕРШУ ПОПРАВКУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PT-07(02)	заборонена обробка 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.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика та процедури обробки персональних даних і забезпечення прозорості; повідомлення про конфіденційність; система записів Закону про конфіденційність; окреме повідомлення про використання номерів соціального страхування; план забезпечення конфіденційності; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за обробку персональних даних та прозорість; персонал організації, відповідальний за користувацький інтерфейс або взаємодію з користувачами; персонал організації, відповідальний за інформаційну безпеку та конфіденційність]. **Перевірка**: [ВИБІР: Процеси організації та імплементаційна підтримка або механізми надання повідомлень особам про обробку їхніх персональних даних].	

PT-8	**ВИМОГИ ДО ВІДПОВІДНОСТІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	PT-08a.	було отримано схвалення Ради з цілісності даних для проведення програми відповідності;
	PT-08b.[01]	розроблено та ухвалено договір комп'ютерної відповідності;
	PT-08b.[02]	ухвалено договір про комп'ютерну відповідність, коли система або організація обробляє інформацію з метою проведення програми відповідності;
	PT-08c.	публікується повідомлення про збіг у Державному реєстрі, коли система або організація обробляє інформацію з метою проведення програми збігу;

	PT-08d.	проводиться незалежна перевірка інформації, отриманої програмою співставлення, перед тим, як вжити несприятливих заходів проти особи, якщо це необхідно, коли система або організація обробляє інформацію з метою проведення програми відповідності;
	PT-08e.[01]	отримують особи повідомлення, коли система або організація обробляє інформацію з метою проведення програми відповідності;
	PT-08e.[02]	надається особам можливість оскаржити результати до того, як проти них будуть вжиті несприятливі дії, коли система або організація обробляє інформацію з метою проведення програми зіставлення.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика та процедури обробки персональних даних і забезпечення прозорості; повідомлення про конфіденційність; система записів Закону про конфіденційність; окреме повідомлення про використання номерів соціального страхування; план забезпечення конфіденційності; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за обробку персональних даних та прозорість; персонал організації, відповідальний за користувацький інтерфейс або взаємодію з користувачами; персонал організації, відповідальний за інформаційну безпеку та конфіденційність]. **Перевірка**: [ВИБІР: Процеси організації та імплементаційна підтримка або механізми надання повідомлень особам про обробку їхніх персональних даних].	

XVI. КЛАС ЗАХОДІВ ЗАХИСТУ RA – ОЦІНКА РИЗИКУ

RA-1	**ПОЛІТИКА ТА ПРОЦЕДУРИ ОЦІНЮВАННЯ РИЗИКУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	RA-01_ODP[01]	**визначено персонал або ролі, на які поширюється політика оцінювання ризику;**
	RA-01_ODP[02]	**визначено персонал або ролі, на які поширюються процедури, що сприяють здійсненню політики оцінювання ризику;**
	RA-01_ODP[03]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {рівень організації; рівень місії/бізнес-процесу; рівень системи};**
	RA-01_ODP[04]	**визначена посадова особа, відповідальна за управління політикою та процедурами оцінювання ризику;**
	RA-01_ODP[05]	**визначена періодичність перегляду та оновлення поточної політики оцінювання ризику;**
	RA-01_ODP[06]	**є події, які вимагають перегляду та оновлення поточної політики оцінювання ризику;**
	RA-01_ODP[07]	**визначено періодичність перегляду та оновлення поточних процедур оцінювання ризику;**
	RA-01_ODP[08]	**визначені події, які потребують перегляду та оновлення процедур оцінювання ризику;**
	RA-01a.[01]	розроблена та задокументована політика оцінювання ризику;
	RA-01a.[02]	поширюється політика оцінки ризиків на **<RA-01_ODP[01] персонал або ролі>**.
	RA-01a.[03]	розроблені та задокументовані процедури оцінки ризиків для сприяння впровадженню політики оцінки ризиків та пов'язаних з нею засобів контролю оцінювання ризику;
	RA-01a.[04]	поширюються процедури оцінювання ризику на **<RA-01_ODP[02] персонал або ролі>;**
	RA-01a.01(a)[01]	відповідає політика оцінювання ризику **<RA-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** поставленій меті;
	RA-01a.01(a)[02]	політика оцінювання ризику **<RA-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** враховує сферу застосування;
	RA-01a.01(a)[03]	політика оцінювання ризику **<RA-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** враховує ролі;
	RA-01a.01(a)[04]	стосується політика оцінювання ризику **<RA-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** обов'язків;

	RA-01a.01(a)[05]	враховує політика оцінювання ризику **<RA-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** зобов'язання керівництва;
	RA-01a.01(a)[06]	політика оцінювання ризику **<RA-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** передбачає координацію між структурними підрозділами організації;
	RA-01a.01(a)[07]	політика оцінювання ризику **<RA-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** враховує комплаєнс;
	RA-01a.01(b)	відповідає **<RA-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** політика оцінювання ризику чинному законодавству, виконавчим наказам, директивам, положенням, політикам, стандартам і настановам;
	RA-01b.	призначено посадову особу **<RA-01_ODP[04] посадову особу>** для управління розробкою, документуванням та розповсюдженням політики та процедур оцінювання ризику;
	RA-01c.01[01]	переглядається та оновлюється поточна політика оцінювання ризику **<RA-01_ODP[05] частота>**;
	RA-01c.01[02]	переглядається та оновлюється поточна політика оцінки ризиків після **<RA-01_ODP[06] події>**;
	RA-01c.02[01]	переглядаються та оновлюються поточні процедури оцінювання ризику **<RA-01_ODP[07] частота>**;
	RA-01c.02[02]	переглядаються та оновлюються поточні процедури оцінки ризиків після **<RA-01_ODP[08] події>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політики та процедури оцінювання ризику; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал відповідальний за політику оцінювання ризику; персонал, відповідальний за інформаційну безпеку].	

RA-2	**КАТЕГОРІЮВАННЯ БЕЗПЕКИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	RA-02a.	є категоризованою інформація, яку система обробляє, зберігає та передає;
	RA-02b.	результати категоризації безпеки, включно з обґрунтуванням, задокументовані в плані безпеки системи;
	RA-02c.	розглядає та затверджує рішення про категоризацію безпеки уповноважена посадова особа або призначений представник уповноваженої посадової особи.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика оцінювання ризику; політика та процедури	

	планування безпеки; процедури, що стосуються категоризації безпеки організаційної інформації та інформаційних систем; план захисту інформації; документація щодо категоризації безпеки; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за категоризацію безпеки та несе відповідальність за оцінку ризиків; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для категоріювання безпеки].

RA-2(1)	**КАТЕГОРІЮВАННЯ БЕЗПЕКИ - КАТЕГОРІЮВАННЯ ДРУГОГО РІВНЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	RA-02(01)	проводиться категоріювання другого рівня для інформаційних систем організації з метою отримання додаткової деталізації рівнів критичності системи.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика оцінювання ризику; політика та процедури планування безпеки; процедури, що стосуються категоризації безпеки організаційної інформації та інформаційних систем; план захисту інформації; документація щодо категоризації безпеки; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за категоризацію безпеки та несе відповідальність за оцінку ризиків; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для категоріювання безпеки].	

RA-3	**ОЦІНЮВАННЯ РИЗИКУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	RA-03_ODP[01]	**вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {плани безпеки та приватності; звіт про оцінювання ризику; <RA-03_ODP[02] документ>};**
	RA-03_ODP[02]	**визначено документ, в якому мають бути задокументовані результати оцінювання ризику (якщо вони не задокументовані в планах безпеки та приватності або в звіті про оцінювання ризику) (якщо вибрано);**
	RA-03_ODP[03]	**визначено періодичність перегляду результатів оцінювання ризику;**
	RA-03_ODP[04]	**визначено персонал або ролі, до яких мають бути доведені результати оцінювання ризику;**
	RA-03_ODP[05]	**визначена періодичність оновлення оцінювання ризику;**

	RA-03a.01	проводиться оцінювання ризику для виявлення загроз і вразливостей у системі;
	RA-03a.02	проводиться оцінювання ризику для визначення ймовірності та розміру шкоди від несанкціонованого доступу, використання, розкриття, порушення, модифікації або знищення системи; інформації, яку вона обробляє, зберігає або передає; а також будь-якої пов'язаної з нею інформації;
	RA-03a.03	проводиться оцінювання ризику для визначення ймовірності та впливу несприятливих наслідків для фізичних осіб, що виникають у зв'язку з обробкою інформації, яка ідентифікує особу;
	RA-03b.	інтегровані результати оцінювання ризику та рішення з управління ризиками з точки зору організації та місії або бізнес-процесів з оцінкою ризиків на системному рівні;
	RA-03c.	результати оцінювання ризику задокументовані в **<RA-03_ODP[01] ЗНАЧЕННЯ ВИБРАНОГО ПАРАМЕТРА>**;
	RA-03d.	переглядаються результати оцінювання ризику **<RA-03_ODP[03] частота>**;
	RA-03e.	поширюються результати оцінювання ризику серед **<RA-03_ODP[04] персоналу або ролей>**;
	RA-03f.	оновлюється оцінювання ризику **<RA-03_ODP[05] частота>** або коли відбуваються значні зміни в системі, середовищі її функціонування або інших умовах, які можуть вплинути на стан безпеки або приватності системи
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика оцінювання ризику; політика та процедури планування безпеки; процедури, що стосуються організаційних оцінок ризику; план захисту інформації; оцінка ризику; результати оцінки ризику; огляди оцінки ризику; оновлення оцінки ризику; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за оцінку ризиків; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для оцінювання ризику; автоматизовані механізми підтримки та, або для проведення, документування, перегляду, розповсюдження та оновлення оцінки ризику].	

RA-3(1)	**ОЦІНЮВАННЯ РИЗИКУ - ОЦІНЮВАННЯ РИЗИКУ ЛАНЦЮГА ПОСТАЧАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	RA-03(01)_ODP[01]	**визначені системи, компоненти системи та системні послуги для оцінювання ризику ланцюга постачання;**

	RA-03(01)_ODP[02]	**визначено періодичність оновлення оцінювання ризику ланцюга постачання;**
	RA-03(01)(a)	оцінювання ризику ланцюга постачання, пов'язані з **<RA-03(01)_ODP[01] системами, системними компонентами та системними послугами>**;
	RA-03(01)(b)	потрібно оновлювати оцінювання ризику ланцюга постачання, коли відбуваються значні зміни у відповідному ланцюгу постачання, або коли зміни в системі, середовищі функціонування чи інших умовах можуть вимагати змін у ланцюгу постачання.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика оцінювання ризику; політика та процедури планування безпеки; процедури, що стосуються організаційних оцінок ризику; план захисту інформації; оцінка ризику; результати оцінки ризику; огляди оцінки ризику; оновлення оцінки ризику; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за оцінювання ризику; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для оцінювання ризику; автоматизовані механізми підтримки та, або для проведення, документування, перегляду, розповсюдження та оновлення оцінки ризику].	

RA-3(2)	**ОЦІНЮВАННЯ РИЗИКУ - ВИКОРИСТАННЯ ІНФОРМАЦІЇ З УСІХ ДОСТУПНИХ ДЖЕРЕЛ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	RA-03(02)	використовується інформація з усіх доступних джерел для аналізу ризиків.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика оцінювання ризику; політика та процедури планування безпеки; процедури, що стосуються організаційних оцінок ризиків; оцінка ризиків; результати оцінки ризиків; огляди оцінки ризиків; оновлення оцінки ризиків; звіти з розвідки ризиків; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за оцінювання ризику; персонал організації, відповідальний за безпеку]. **Перевірка**: [ВИБІР: Процеси організації для оцінювання ризику; механізми підтримки та/або проведення, документування, аналізу, розповсюдження та оновлення оцінки ризиків].	

RA-3(3)	**ОЦІНЮВАННЯ РИЗИКУ - УСВІДОМЛЕННЯ ДИНАМІЧНИХ ЗАГРОЗ**
	МЕТА ОЦІНКИ:

	Визначити, чи:	
	RA-03(03)_ODP	**є засоби для постійного визначення поточного стану кіберзагроз;**
	RA-03(03)	визначається поточне середовище кіберзагроз на постійній основі за допомогою **<RA-03(03)_ODP засоби>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика оцінювання ризику; політика та процедури планування безпеки; процедури, що стосуються організаційних оцінок ризиків; оцінка ризиків; результати оцінки ризиків; огляди оцінки ризиків; оновлення оцінки ризиків; звіти з розвідки ризиків; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за оцінювання ризику; персонал організації, відповідальний за безпеку]. **Перевірка**: [ВИБІР: Процеси організації для оцінки ризиків; механізми підтримки та/або проведення, документування, аналізу, розповсюдження та оновлення оцінки ризиків].	

RA-3(4)	**ОЦІНЮВАННЯ РИЗИКУ - ПРОГНОСТИЧНА КІБЕРАНАЛІТИКА**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	RA-03(04)_ODP[01]	**визначені можливості розширеної автоматизації для прогнозування та виявлення ризику;**
	RA-03(04)_ODP[02]	**є системи або компоненти системи, в яких повинні бути застосовані розширені можливості автоматизації та аналітики;**
	RA-03(04)_ODP[03]	**визначені можливості розширеної аналітики для прогнозування та виявлення ризику;**
	RA-03(04)[01]	використовуються **<RA-03(04)_ODP[01] розширені можливості автоматизації>** для прогнозування та виявлення ризику для **<RA-03(04)_ODP[02] систем або компонентів системи>**;
	RA-03(04)[02]	застосовуються **<RA-03(04)_ODP[03] розширені аналітичні можливості>** для прогнозування та виявлення ризику для **<RA-03(04)_ODP[02] систем або компонентів системи>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика оцінювання ризику; політика та процедури планування безпеки; процедури, що стосуються організаційних оцінок ризиків; оцінка ризиків; результати оцінки ризиків; огляди оцінки ризиків; оновлення оцінки ризиків; звіти з розвідки ризиків; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за оцінювання ризику;	

	персонал організації, відповідальний за безпеку]. **Перевірка**: [ВИБІР: Процеси організації для оцінювання ризику; механізми підтримки та/або проведення, документування, аналізу, розповсюдження та оновлення оцінки ризиків].

RA-4	**ОНОВЛЕННЯ ОЦІНЮВАННЯ РИЗИКУ**
	[Вилучено: включено до RA-3]

RA-5	**СКАНУВАННЯ ВРАЗЛИВОСТЕЙ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	RA-05_ODP[01]	**визначена необхідність моніторингу систем та розміщених застосунків на наявність вразливостей;**
	RA-05_ODP[02]	**визначена періодичність перевірки систем та розміщених на них застосунків на наявність вразливостей;**
	RA-05_ODP[03]	**визначено час реагування на усунення законних вразливостей відповідно до організаційної оцінення ризику;**
	RA-05_ODP[04]	**потрібно ділитися інформацією, отриманою в процесі сканування вразливостей та оцінок контролю, з персоналом або ролями, з якими потрібно ділитися;**
	RA-05a.[01]	здійснюється моніторинг систем та розміщених застосунків на наявність вразливостей **<RA-05_ODP[01] частота та/або випадковість відповідно до визначеного організацією процесу>**, а також коли виявляються та повідомляються нові вразливості, що потенційно можуть вплинути на систему;
	RA-05a.[02]	перевіряються системи та розміщені застосунки на наявність вразливостей **<RA-05_ODP[02] частота та/або випадковим чином відповідно до визначеного організацією процесу>**, а також коли виявляються та повідомляються нові вразливості, що потенційно можуть вплинути на систему;
	RA-05b.	застосовуються інструменти та методи моніторингу вразливостей для забезпечення сумісності між інструментами;
	RA-05b.01	застосовуються інструменти та методи моніторингу вразливостей для автоматизації частини процесу управління вразливостями, використовуючи стандарти для переліку платформ, недоліків програмного забезпечення та неправильних конфігурацій;
	RA-05b.02	застосовуються інструменти та методи моніторингу вразливостей для полегшення взаємодії між інструментами та автоматизації частини процесу управління вразливостями шляхом використання стандартів для формування контрольних списків та процедур тестування;

	RA-05b.03	застосовуються інструменти та методи моніторингу вразливостей для полегшення взаємодії між інструментами та автоматизації частин процесу управління вразливостями шляхом використання стандартів для вимірювання впливу вразливостей;
	RA-05c.	аналізуються звіти про сканування вразливостей та результати моніторингу вразливостей;
	RA-05d.	усуваються легітимні вразливості **<RA-05_ODP[03] час реагування>** відповідно до організаційної оцінки ризиків;
	RA-05e.	надається інформація, отримана в процесі моніторингу вразливостей та оцінки контролю, **<RA-05_ODP[04] персонал або ролі>**, щоб допомогти усунути подібні вразливості в інших системах;
	RA-05f.	використовуються інструменти моніторингу вразливостей, які передбачають можливість швидкого оновлення вразливостей, що підлягають скануванню.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика оцінювання ризику; процедури, що стосуються сканування вразливості; оцінка ризику; план захисту інформації; звіт про оцінку безпеки; засоби сканування вразливості та відповідна документація щодо конфігурації; результати сканування вразливості; записи про виправлення та вразливість; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за оцінку ризиків, оцінку контролю безпеки та сканування вразливості; персонал організації, відповідальний за аналіз вразливості персонал організації, відповідальний за усунення вразливостей; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи, мережі]. **Перевірка:** [ВИБІР: Процеси організації для сканування, аналізу, виправлення та обміну інформацією щодо вразливостей; автоматизовані механізми, що підтримують та, або впроваджують сканування, аналіз, виправлення та обмін інформацією про вразливість].	

RA-5(1)	**СКАНУВАННЯ ВРАЗЛИВОСТЕЙ - МОЖЛИВІСТЬ ОНОВЛЕННЯ ІНСТРУМЕНТІВ**
	[Вилучено: включено до RA-5]

RA-5(2)	**СКАНУВАННЯ ВРАЗЛИВОСТЕЙ - ОНОВЛЕННЯ ЗА ЧАСТОТОЮ, ПЕРЕД НОВИМ СКАНУВАННЯМ АБО ПРИ ІДЕНТИФІКАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	RA-05(02)_ODP[01]	**визначена необхідність моніторингу систем та розміщених застосунків на наявність вразливостей;**
	RA-	**визначена періодичність перевірки систем та розміщених**

	05(02)_ODP[02]	**на них застосунків на наявність вразливостей;**
	RA-05(02)	визначено час реагування на усунення законних вразливостей відповідно до організаційної оцінення ризику;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Процедури, що стосуються сканування вразливості; план захисту інформації; звіт про оцінку безпеки; засоби сканування вразливості та відповідна документація щодо конфігурації; результати сканування вразливості; записи про виправлення та вразливість; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який несе відповідальність за сканування вразливостей; персонал організації, відповідальний за аналіз вразливості персонал організації, який відповідає за інформаційну безпеку; адміністратори системи, мережі]. **Перевірка:** [ВИБІР: Процеси організації для сканування вразливості; автоматизовані механізми, інструменти, що підтримують та, або впроваджують сканування вразливостей].	

RA-5(3)	**СКАНУВАННЯ ВРАЗЛИВОСТЕЙ - ШИРОТА ТА ГЛИБИНА ПОКРИТТЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	RA-05(03)	визначено ширину та глибину охоплення сканування вразливостей.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Процедури, що стосуються сканування вразливості; план захисту інформації; звіт про оцінку безпеки; засоби сканування вразливості та відповідна документація щодо конфігурації; результати сканування вразливості; записи про виправлення та вразливість; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який несе відповідальність за сканування вразливостей; персонал організації, відповідальний за аналіз вразливості персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для сканування вразливості; автоматизовані механізми, інструменти, що підтримують та, або впроваджують сканування вразливостей].	

RA-5(4)	**СКАНУВАННЯ ВРАЗЛИВОСТЕЙ - ВИЯВНА ІНФОРМАЦІЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	RA-05(04)_ODP	**визначені коригувальні дії, які необхідно вжити, якщо інформація про систему буде виявлена;**
	RA-05(04)[01]	є інформація про систему відкритою;

	RA-05(04)[02]	вживаються **<RA-05(04)_ODP коригувальні дії>**, коли інформація про систему підтверджується як така, що може бути виявлена.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Процедури, що стосуються сканування вразливості; звіт про оцінку безпеки; результати тесту на проникнення; результати сканування вразливості; звіт про оцінку ризику; записи про вжиті коригувальні дії; записи реагування на події; записи аудиту; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який несе відповідальність за сканування та, або тестування на проникнення; персонал організації, відповідальний за аналіз вразливості; персонал організації, відповідальний за реагування на ризик; персонал організації, відповідальний за управління інцидентами та реагування на них; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для сканування вразливості; організаційні процеси реагування на ризик; організаційні процеси для управління інцидентами та реагування на них; автоматизовані механізми, інструменти, що підтримують та, або впроваджують сканування вразливості; автоматизовані механізми підтримки та, або реалізації реагування на ризик; автоматизовані механізми підтримки та, або реалізації управління та реагування на інциденти].	

RA-5(5)	**СКАНУВАННЯ ВРАЗЛИВОСТЕЙ - ПРИВІЛЕЙОВАНИЙ ДОСТУП**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	RA-05(05)_ODP[01]	**визначено компоненти системи, до яких дозволено привілейований доступ для вибраних дій зі сканування вразливостей;**
	RA-05(05)_ODP[02]	**визначені дії сканування вразливостей, обрані для авторизації привілейованого доступу до компонентів системи;**
	RA-05(05)	реалізовано авторизацію привілейованого доступу до **<RA-05(05)_ODP[01] компоненти системи>** для **<RA-05(05)_ODP[02] діяльність зі сканування вразливостей>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика оцінення ризику; процедури, що стосуються сканування вразливості; план захисту інформації; проєктна документація системи; налаштування конфігурації системи та відповідна документація; перелік компонентів системи для сканування вразливості; список дозволів на доступ персоналу; авторизаційні дані; отримати доступ до записів авторизації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який несе відповідальність за сканування вразливостей; адміністратори системи, мережі; персонал організації, відповідальний за контроль доступу до системи; персонал організації, відповідальний за управління конфігурацією системи; розробники системи;	

	персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для сканування вразливості; організаційні процеси контролю доступу; автоматизовані механізми, що підтримують та, або впроваджують контроль доступу; автоматизовані механізми, інструменти, що підтримують та, або впроваджують сканування вразливостей].

RA-5(6)	**СКАНУВАННЯ ВРАЗЛИВОСТЕЙ - АВТОМАТИЗОВАНИЙ АНАЛІЗ ТЕНДЕНЦІЙ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	RA-05(06)_ODP	**визначені автоматизовані механізми для порівняння результатів багаторазового сканування вразливостей;**
	RA-05(06)	порівнюються результати багаторазового сканування вразливостей за допомогою **<RA-05(06)_ODP автоматизовані механізми>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика оцінки ризику; процедури, що стосуються сканування вразливості; проєктна документація системи; документація щодо засобів та методів сканування вразливостей; результати сканування вразливості; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який несе відповідальність за сканування вразливостей; персонал організації, відповідальний за аналіз вразливості персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для сканування вразливості; автоматизовані механізми, інструменти, що підтримують та, або впроваджують сканування вразливості; автоматизовані механізми, що підтримують та, або впроваджують аналіз тенденцій результатів сканування вразливості].	

RA-5(7)	**СКАНУВАННЯ ВРАЗЛИВОСТЕЙ - АВТОМАТИЗОВАНЕ ВИЯВЛЕННЯ ТА СПОВІЩЕННЯ ПРО НЕАВТОРИЗОВАНІ КОМПОНЕНТИ**
	[Вилучено: включено до CM-8]

RA-5(8)	**СКАНУВАННЯ ВРАЗЛИВОСТЕЙ - ОГЛЯД ЖУРНАЛІВ АУДИТУ ЗА МИНУЛІ ПЕРІОДИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	RA-05(08)_ODP[01]	**визначена система, чиї журнали аудиту за минулі періоди потрібно переглядати;**
	RA-05(08)_ODP[02]	**визначено часовий проміжок для потенційного попереднього використання системи;**

	RA-05(08)	переглядаються журнали аудиту за минулі періоди, щоб визначити, чи була вразливість, яка виявлена в **<RA-05(08)_ODP[01] системі>**, була раніше використана протягом **<RA-05(08)_ODP[02] часовий період>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика оцінки ризику; процедури, що стосуються сканування вразливості; журнали аудиту; записи оглядів журналу аудиту; результати сканування вразливості; записи про виправлення та вразливість; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який несе відповідальність за сканування вразливостей; персонал організації, відповідальний за аналіз вразливості ; персонал організації, відповідальний за перевірку аудиторських записів; адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для сканування вразливості; організаційний процес для перевірки та відповіді на записи аудиту; автоматизовані механізми, інструменти, що підтримують та, або впроваджують сканування вразливості; автоматизовані механізми, що підтримують та, або впроваджують перевірку записів аудиту].	

RA-5(9)	**СКАНУВАННЯ ВРАЗЛИВОСТЕЙ - ТЕСТУВАННЯ ТА АНАЛІЗ ПРОНИКНЕННЯ**
	[Вилучено: включено до CA-8]

RA-5(10)	**СКАНУВАННЯ ВРАЗЛИВОСТЕЙ - ЗІСТАВЛЕННЯ ІНФОРМАЦІЇ ПРО СКАНУВАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	RA-05(10)	порівнюють результати сканування вразливостей для визначення наявності численних вразливостей на множинних векторів атак.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика оцінки ризиків; процедури, що стосуються сканування вразливості; оцінка ризику; план захисту інформації; документація щодо засобів та методів сканування вразливостей; результати сканування вразливості; записи управління вразливістю; записи аудиту; журнали кореляції подій, уразливостей; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який несе відповідальність за сканування вразливостей; персонал організації, відповідальний за аналіз вразливості персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для сканування вразливості; автоматизовані механізми, інструменти, що підтримують та, або впроваджують сканування вразливості; автоматизовані механізми, що реалізують кореляцію результатів сканування вразливості].	

RA-5(11)	СКАНУВАННЯ ВРАЗЛИВОСТЕЙ - ПРОГРАМА ПУБЛІЧНОГО ОПРИЛЮДНЕННЯ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	RA-05(11)	створено публічний канал для отримання повідомлень про вразливості в системах організації і компонентах системи.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика оцінки ризиків; політика та процедури планування безпеки; процедури, що стосуються організаційних оцінок ризиків; оцінка ризиків; результати оцінки ризиків; огляди оцінки ризиків; оновлення оцінки ризиків; звіти з розвідки ризиків; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за сканування вразливостей; персонал організації, відповідальний за аналіз результатів сканування вразливостей; персонал організації, відповідальний за безпеку]. **Перевірка**: [ВИБІР: Процеси організації сканування вразливостей; механізми/інструменти, що підтримують та/або реалізують сканування вразливостей; механізми, що реалізують публічне інформування про вразливості].	

RA-6	ЗАХОДИ ПРОТИДІЇ ТЕХНІЧНІЙ РОЗВІДЦІ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	RA-06_ODP[01]	**визначені місця для використання заходів ПДТР;**
	RA-06_ODP[02]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {<RA-06_ODP[03] частота>; коли <RA-06_ODP[04] події або показники>};**
	RA-06_ODP[03]	**визначено частоту, з якою слід проводити заходи ПДТР (якщо обрано);**
	RA-06_ODP[04]	**визначені події або показники, які, у разі їх виникнення, спричиняють проведення заходів ПДТР (якщо вони були обрані);**
	RA-06	застосовується опитування щодо заходів технічного спостереження в **<RA-06_ODP[01] місцезнаходження> <RA-06_ODP[02] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика оцінки ризику; процедури, що стосуються обстеження контрзаходів технічного нагляду; план захисту інформації; записи	

	аудиту, журнали подій; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за обстеження контрзаходів технічного нагляду; адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для обстеження контрзаходів технічного нагляду; автоматизовані механізми, інструменти, що підтримують та, або впроваджують обстеження контрзаходів технічного нагляду].

RA-7	**РЕАГУВАННЯ НА РИЗИК**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	RA-07[01]	вживаються заходи реагування на результати оцінок безпеки відповідно до організаційної толерантності до ризиків;
	RA-07[02]	вживаються заходи реагування на результати оцінювання приватності відповідно до організаційної толерантності до ризиків;
	RA-07[03]	вживаються заходи реагування на результати моніторингу відповідно до організаційної толерантності до ризиків;
	RA-07[04]	вживаються заходи реагування на висновки аудиту відповідно до організаційної толерантності до ризиків.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика оцінки ризику; процедури, що стосуються реагування на ризик; план захисту інформації; записи аудиту, журнали подій; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за реагування на інциденти; адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для реагування на ризик ; автоматизовані механізми, інструменти, що підтримують та, або впроваджують реагування на ризик].	

RA-8	**ОЦІНКА ВПЛИВУ НА ПРИВАТНІСТЬ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	RA-08a.	проводиться оцінка впливу на приватність для систем, програм або інших видів діяльності перед розробкою або придбанням інформаційних технологій, які які становлять ризик приватності;

	RA-08b.[01]	проводиться оцінка впливу на приватність для систем, програм або інших видів діяльності перед початком збору інформації, що містить персональні дані, яка буде оброблятися за допомогою інформаційних технологій;
	RA-08b.[02]	проводиться оцінка впливу на приватність для систем, програм або інших видів діяльності перед початком збору персональної інформації, яка включає персональну інформацію, що дозволяє встановити фізичний або віртуальний (онлайн) контакт з конкретною особою, якщо ідентичні запитання були поставлені десятьом або більше особам, окрім агентств, інструментів або працівників федерального уряду, або якщо до них були висунуті ідентичні вимоги щодо звітності.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика оцінки ризику; процедури, що стосуються реагування на ризик; план захисту інформації; записи аудиту, журнали подій; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за реагування на інциденти; адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для реагування на ризик ; автоматизовані механізми, інструменти, що підтримують та, або впроваджують реагування на ризик].	

RA-9	**АНАЛІЗ КРИТИЧНОСТІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	RA-09_ODP[01]	**визначені системи, компоненти системи або системні сервіси, що підлягають аналізу на предмет критичності;**
	RA-09_ODP[02]	**визначені точки прийняття рішень в життєвому циклі розробки системи, коли необхідно проводити аналіз критичності;**
	RA-09	визначені критичні компоненти та функції системи шляхом проведення аналізу критичності для **<RA-09_ODP[01] систем, системних компонентів або системних служб>** в **<RA-09_ODP[02] точках прийняття рішень в життєвому циклі розробки системи>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика оцінки ризику; процедури, що стосуються аналізу критичності; план захисту інформації; записи аудиту, журнали подій; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за аналізу критичності; адміністратори системи, мережі; персонал організації, який	

	відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для аналізу критичності; автоматизовані механізми, інструменти, що підтримують та, або впроваджують аналіз критичності].

RA-10	**АКТИВНИЙ ПОШУК ЗАГРОЗ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	RA-10_ODP	**визначена частота, з якою слід використовувати можливість виявлення загроз;**
	RA-10a.01	створена та підтримується спроможність протидії кіберзагрозам для пошуку індикаторів компрометації в організаційних системах;
	RA-10a.02	створена та підтримується спроможність виявляти, відслідковувати та знешкоджувати кіберзагрози, які не піддаються існуючому контролю;
	RA-10b.	використовується функція відстеження загроз **<RA-10_ODP частота>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика оцінки ризиків; звіти про оцінку; записи аудиту/журнали подій; можливість відстеження загроз; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за пошук загроз; системні/мережеві адміністратори; персонал організації, відповідальний за безпеку]. **Перевірка**: [ВИБІР: Процеси організації оцінювання та аудиту; механізми/інструменти, що підтримують та/або впроваджують можливості виявлення загроз].	

XVII. КЛАС ЗАХОДІВ ЗАХИСТУ SA – ПРИДБАННЯ СИСТЕМИ ТА ПОСЛУГ

SA-1	**ПОЛІТИКИ ТА ПРОЦЕДУРИ ПРИДБАННЯ СИСТЕМ ТА ПОСЛУГ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-01_ODP[01]	**визначено персонал або ролі, на які поширюватиметься політика придбання систем і послуг;**
	SA-01_ODP[02]	**визначено персонал або ролі, на які поширюються процедури придбання систем і послуг;**
	SA-01_ODP[03]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {рівень організації; рівень місії/бізнес-процесу; рівень системи};**
	SA-01_ODP[04]	**визначено посадову особу, яка керуватиме політикою та процедурами придбання систем і послуг;**
	SA-01_ODP[05]	**визначено періодичність перегляду та оновлення поточної політики придбання систем і послуг;**
	SA-01_ODP[06]	**є події, які вимагають перегляду та оновлення поточної політики придбання систем і послуг;**
	SA-01_ODP[07]	**визначено частоту, з якою переглядаються та оновлюються поточні процедури придбання систем і послуг;**
	SA-01_ODP[08]	**є події, які вимагають перегляду та оновлення процедур придбання систем і послуг;**
	SA-01a.[01]	розроблена та задокументована політика придбання систем і послуг;
	SA-01a.[02]	поширюється політика придбання систем і послуг на **<SA-01_ODP[01] персонал або ролі>**;
	SA-01a.[03]	розроблені та задокументовані процедури придбання систем і послуг, що сприяють впровадженню політики придбання систем та послуг, а також відповідні засоби контролю за придбанням систем та послуг;
	SA-01a.[04]	поширюються процедури придбання системи і послуг на **<SA-01_ODP[02] персонал або ролі>**;
	SA-01a.01(a)[01]	відповідає політика придбання системи і послуг **<SA-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** поставленій меті;
	SA-01a.01(a)[02]	політика придбання систем і послуг **<SA-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(S)>** враховує сферу застосування;
	SA-01a.01(a)[03]	політика придбання системи і послуг **<SA-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(S)>** стосується ролей;

	SA-01a.01(a)[04]	політика придбання систем і послуг **<SA-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** враховує відповідальність;
	SA-01a.01(a)[05]	враховує політика придбання систем і послуг **<SA-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** зобов'язання керівництва;
	SA-01a.01(a)[06]	політика придбання систем і послуг **<SA-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** передбачає координацію між організаціями;
	SA-01a.01(a)[07]	політика придбання систем і послуг **<SA-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** враховує відповідність вимогам;
	SA-01a.01(b)	відповідає **<SA-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** політика придбання системи і послуг чинному законодавству, виконавчим наказам, директивам, положенням, політикам, стандартам та настановам;
	SA-01b.	призначена **<SA-01_ODP[04] посадова особа>** для управління розробкою, документуванням та розповсюдженням політики та процедур придбання системи і послуг;
	SA-01c.01[01]	переглядається та оновлюється політика придбання систем і послуг **<SA-01_ODP[05] частота>**;
	SA-01c.01[02]	переглядається та оновлюється поточна політика придбання систем та послуг після **<SA-01_ODP[06] подій>**;
	SA-01c.02[01]	переглядаються та оновлюються поточні процедури придбання систем і послуг **<SA-01_ODP[07] частота>**;
	SA-01c.02[02]	переглядаються та оновлюються поточні процедури закупівлі систем та послуг після **<SA-01_ODP[08] подій>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політики та процедури придбання систем і послуг; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал відповідальний за політику придбання систем і послуг; персонал, відповідальний за інформаційну безпеку].	

SA-2	**РОЗПОДІЛ РЕСУРСІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-02a.[01]	визначені вимоги до інформаційної безпеки високого рівня для систем або послуг для системи при плануванні місії та бізнес-процесів;
	SA-02a.[02]	визначені вимоги до приватності високого рівня для систем або послуг для системи при плануванні місії та бізнес-

		процесів;
	SA-02b.[01]	визначені та задокументовані ресурси, необхідні для захисту систем або послуг для системи, як частина процесу планування організаційного капіталу та контролю за інвестиціями;
	SA-02b.[02]	виділені ресурси, необхідні для захисту систем або послуг для системи, в рамках процесу планування організаційного капіталу та контролю інвестицій;
	SA-02c.[01]	передбачено окрему статтю витрат на інформаційну безпеку в програмній та бюджетній документації організації;
	SA-02c.[02]	передбачена окрема стаття для захисту приватності в програмній та бюджетній документації організації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються розподілу ресурсів відповідно до вимог інформаційної безпеки; процедури, що стосуються планування капіталу та контролю інвестицій; документація щодо організаційного програмування та бюджетування; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за планування капіталу, контроль інвестицій, організаційне програмування та бюджетування; персонал організації, відповідальний за визначення вимог інформаційної безпеки до інформаційних систем, послуг; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для визначення вимог до інформаційної безпеки; організаційні процеси для капітального планування, програмування та бюджетування; автоматизовані механізми підтримки та, або реалізації планування, програмування та бюджетування організаційного капіталу].	

SA-3	**ЖИТТЄВИЙ ЦИКЛ РОЗРОБКИ СИСТЕМИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-03_ODP	**визначено життєвий цикл розробки системи;**
	SA-03a.[01]	система придбана, розроблена та керується з використанням життєвого циклу **<SA-03_ODP життєвий цикл розробки системи >**, який охоплює інформаційну безпеку;
	SA-03a.[02]	система придбана, розроблена та керується з використанням **<SA-03_ODP життєвий цикл розробки системи >**, який охоплює приватність;
	SA-03b.[01]	визначені та задокументовані ролі та обов'язки з інформаційної безпеки протягом усього життєвого циклу розробки системи;
	SA-03b.[02]	визначені та задокументовані ролі та обов'язки щодо

		приватності протягом усього життєвого циклу розробки системи;
	SA-03c.[01]	визначені особи, які виконують функції та обов'язки з інформаційної безпеки;
	SA-03c.[02]	визначені особи з функціями та обов'язками, пов'язаними з приватністю;
	SA-03d.[01]	інтегровані процеси управління інформаційною безпекою організації в діяльність життєвого циклу розробки системи;
	SA-03d.[02]	інтегровані процеси управління приватністю в життєвого циклу розробки системи.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються інтеграції інформаційної безпеки в процес життєвого циклу розробки системи; документація життєвого циклу розробки системи; стратегія управління ризиками інформаційної безпеки, програмна документація; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за інформаційну безпеку та життєвий цикл системи; персонал організації, відповідальний за управління ризиками інформаційної безпеки; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для визначення та документування життєвого циклу розробки системи (ЖЦРС); організаційні процеси для визначення ролей та відповідальності ЖЦРС; організаційний процес для інтеграції управління ризиками інформаційної безпеки в ЖЦРС; автоматизовані механізми підтримки та, або реалізації ЖЦРС].	

SA-3(1)	**ЖИТТЄВИЙ ЦИКЛ РОЗРОБКИ СИСТЕМИ - УПРАВЛІННЯ СЕРЕДОВИЩЕМ РОЗРОБКИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-03(01)	захищене середовище розробки системи, відповідно до ризиків протягом усього життєвого циклу розробки системи для системи, компонентів системи або служб..
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються інтеграції інформаційної безпеки в процес життєвого циклу розробки системи; документація життєвого циклу розробки системи; стратегія управління ризиками інформаційної безпеки, програмна документація; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за інформаційну безпеку та життєвий цикл системи; персонал організації, відповідальний за управління ризиками інформаційної безпеки; персонал організації, який відповідає за інформаційну безпеку].	

	Перевірка: [ВИБІР: Процеси організації для визначення та документування ЖЦРС; організаційні процеси для визначення ролей та відповідальності ЖЦРС; організаційний процес для інтеграції управління ризиками інформаційної безпеки в ЖЦРС; автоматизовані механізми підтримки та, або реалізації ЖЦРС].

SA-3(2)	**ЖИТТЄВИЙ ЦИКЛ РОЗРОБКИ СИСТЕМИ - ВИКОРИСТАННЯ РЕАЛЬНИХ ДАНИХ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-03(02)a.[01]	дозволено використання реальних даних у середовищах розробки, тестування та інтеграції системи, компонента системи або послуг для системи;
	SA-03(02)a.[02]	задокументовано використання реальних даних у середовищах розробки, тестування та інтеграції системи, компонента системи або послуг для системи;
	SA-03(02)a.[03]	контролюється використання реальних даних у середовищах розробки, тестування та інтеграції системи, компонента системи або послуг для системи;
	SA-03(02)b.	захищені 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..
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються інтеграції інформаційної безпеки в процес життєвого циклу розробки системи; документація життєвого циклу розробки системи; стратегія управління ризиками інформаційної безпеки, програмна документація; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за інформаційну безпеку та життєвий цикл системи; персонал організації, відповідальний за управління ризиками інформаційної безпеки; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для визначення та документування ЖЦРС; організаційні процеси для визначення ролей та відповідальності ЖЦРС; організаційний процес для інтеграції управління ризиками інформаційної безпеки в ЖЦРС; автоматизовані механізми підтримки та, або реалізації ЖЦРС].	

SA-3(3)	**ЖИТТЄВИЙ ЦИКЛ РОЗРОБКИ СИСТЕМИ - ОНОВЛЕННЯ ТЕХНОЛОГІЙ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-03(03)[01]	планується оновлення технологій для підтримки системи

		протягом усього життєвого циклу розробки системи;
	SA-03(03)[02]	впроваджено графік оновлення технологій для підтримки системи протягом усього життєвого циклу розробки системи.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються інтеграції інформаційної безпеки в процес життєвого циклу розробки системи; документація життєвого циклу розробки системи; стратегія управління ризиками інформаційної безпеки, програмна документація; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за інформаційну безпеку та життєвий цикл системи; персонал організації, відповідальний за управління ризиками інформаційної безпеки; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для визначення та документування ЖЦРС; організаційні процеси для визначення ролей та відповідальності ЖЦРС; організаційний процес для інтеграції управління ризиками інформаційної безпеки в ЖЦРС; автоматизовані механізми підтримки та, або реалізації ЖЦРС].	

SA-4	**ПРОЦЕС ЗАКУПІВЕЛЬ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-04_ODP[01]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРА: { стандартні пункти контракту; <SA-04_ODP[02] пункт контракту>};**
	SA-04_ODP[02]	**визначено пункт контракту (якщо вибрано);**
	SA-04a.[01]	включені функціональні вимоги, описи та критерії безпеки в явному вигляді або шляхом посилання за допомогою **<SA-04_ODP[01] ЗНАЧЕННЯ(Я) ВИБОРКОВОГО ПАРАМЕТРА(ів)>** до договору про закупівлю системи, системного компонента або системної послуги;
	SA-04a.[02]	включені функціональні вимоги, описи та критерії щодо приватності явно або шляхом посилання за допомогою **<SA-04_ODP[01] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** до договору про закупівлю системи, системного компонента або системної послуги;
	SA-04b.	включені вимоги, описи та критерії надійності механізму в явному вигляді або за допомогою посилань у контракт на закупівлю системи, системного компонента або системної послуги;
	SA-04c.[01]	включені вимоги, описи та критерії забезпечення безпеки в явному вигляді або шляхом посилання за допомогою **<SA-04_ODP[01] ЗНАЧЕННЯ(Я) ВИБОРКОВОГО ПАРАМЕТРА(ів)>** до договору про закупівлю системи,

		системного компонента або системної послуги;
	SA-04c.[02]	включені вимоги, описи та критерії забезпечення приватності у явному вигляді або шляхом посилання за допомогою **<SA-04_ODP[01] ЗНАЧЕННЯ ВИБОРКОВОГО ПАРАМЕТРА(ів)>** до контракту на придбання системи, системного компонента або системної послуги;
	SA-04d.[01]	засоби контролю, необхідні для задоволення вимог, описів та критеріїв безпеки, включені явно або шляхом посилання за допомогою **<SA-04_ODP[01] ЗНАЧЕННЯ(Я) ВИБОРКОВОГО ПАРАМЕТРА(ів)>** до контракту на придбання системи, системного компонента або системної послуги;
	SA-04d.[02]	включені засоби контролю, необхідні для задоволення вимог, описів та критеріїв конфіденційності, явно або шляхом посилання за допомогою **<SA-04_ODP[01] ВИБІРКОВЕ ЗНАЧЕННЯ(Я) ПАРАМЕТРА(ів)>** у контракт на придбання системи, системного компонента або системної послуги;
	SA-04e.[01]	включені вимоги, описи та критерії документації з безпеки в явному вигляді або шляхом посилання за допомогою **<SA-04_ODP[01] ЗНАЧЕННЯ(Я) ВИБРАНОГО ПАРАМЕТРА(ів)>** до договору про закупівлю системи, системного компонента або системної послуги;
	SA-04e.[02]	включені вимоги, описи та критерії щодо документації про конфіденційність у явному вигляді або шляхом посилання за допомогою **<SA-04_ODP[01] ЗНАЧЕННЯ ВИБІРКОВОГО ПАРАМЕТРА(ів)>** до договору про закупівлю системи, системного компонента або системної послуги;
	SA-04f.[01]	включені вимоги щодо захисту документації, описів та критеріїв безпеки в явному вигляді або шляхом посилання за допомогою **<SA-04_ODP[01] ВИБІРКОВЕ ЗНАЧЕННЯ(Я) ПАРАМЕТРА(ів)>** до контракту на придбання системи, системного компонента або системної послуги;
	SA-04f.[02]	включені вимоги щодо захисту приватності документації, описів та критеріїв явно або шляхом посилання за допомогою **<SA-04_ODP[01] ВИБІРКОВЕ ЗНАЧЕННЯ(Я) ПАРАМЕТРА(ів)>** до договору про закупівлю системи, системного компонента або системної послуги;
	SA-04g	включено опис середовища розробки системи та середовища, в якому система має функціонувати, вимоги та критерії явно або шляхом посилання з використанням **<SA-04_ODP[01] ЗНАЧЕННЯ(Я) ВИБОРКОВОГО ПАРАМЕТРА(ів)>** до договору про закупівлю системи, системного компонента або системної послуги;
	SA-04h.[01]	включено розподіл відповідальності або визначення сторін, відповідальних за вимоги, описи та критерії інформаційної безпеки, явно або шляхом посилання за допомогою **<SA-04_ODP[01] ЗНАЧЕННЯ(Я) ВИБРАНОГО**

		ПАРАМЕТРА(ів)> до договору про закупівлю системи, системного компонента або системної послуги;
	SA-04h.[02]	включено розподіл відповідальності або ідентифікацію сторін, відповідальних за вимоги щодо приватності, описи та критерії явно або за допомогою посилання за допомогою **<SA-04_ODP[01] ЗНАЧЕННЯ(Я) ВИБРАНОГО ПАРАМЕТРА(ів)>**;
	SA-04h.[03]	розподіл відповідальності або визначення сторін, відповідальних за вимоги, описи та критерії управління ризиками ланцюга поставок, включено явно або шляхом посилання за допомогою **<SA-04_ODP[01] ЗНАЧЕННЯ(Я) ВИБРАНОГО ПАРАМЕТРА(ів)>**;
	SA-04i.	включені вимоги та описи критеріїв прийнятності в явному вигляді або шляхом посилання з використанням **<SA-04_ODP[01] ЗНАЧЕННЯ(Я) ВИБОРКОВОГО ПАРАМЕТРА(ів)>** до договору про закупівлю системи, системного компонента або системної послуги.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються інтеграції вимог, описів та критеріїв інформаційної безпеки в процесі придбання; договори придбання системи, компонента системи або послуги системи; проєктна документація системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання, підряд; персонал організації, відповідальний за визначення вимог до функціональних можливостей, міцності та впевненості в безпеці системи; адміністратори системи, мережі; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для визначення вимог до функціональних можливостей безпеки, міцності та впевненості в системі; організаційні процеси для розробки контрактів на придбання; автоматизовані механізми підтримки та, або реалізації придбань та включення вимог безпеки до контрактів].	

SA-4(1)	**ПРОЦЕС ЗАКУПІВЕЛЬ - ФУНКЦІОНАЛЬНІ ВЛАСТИВОСТІ ЗАХОДІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-04(01)	планується оновлення технологій для системи протягом життєвого циклу розробки системи;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються інтеграції вимог, описів та критеріїв інформаційної безпеки в процесі придбання; договори придбання системи, компонента системи або послуги системи; проєктна документація системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання, підряд; персонал організації, відповідальний за визначення вимог до функціональних	

	можливостей, міцності та впевненості в безпеці системи; адміністратори системи, мережі; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для визначення вимог до функціональних можливостей безпеки, міцності та впевненості в системі; організаційні процеси для розробки контрактів на придбання; автоматизовані механізми підтримки та, або реалізації придбань та включення вимог безпеки до контрактів].

SA-4(2)	**ПРОЦЕС ЗАКУПІВЕЛЬ - РОЗРОБКА ТА ВПРОВАДЖЕННЯ ІНФОРМАЦІЇ ДЛЯ ЗАХОДІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-04(02)_ODP[01]	**вибрано одне або більше з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: { пов'язані з безпекою зовнішні системні інтерфейси; архітектуру (проєкт) високого рівня; архітектури (проєкт) низького рівня; вихідний код або апаратні схеми; <SA-04(02)_ODP[02] інформація про розробку та реалізацію>};**
	SA-04(02)_ODP[02]	**визначена інформація про розробку та впровадження (якщо вибрано);**
	SA-04(02)_ODP[03]	**визначено рівень деталізації;**
	SA-04(02)	повинен розробник системи, системного компонента або системної послуги надавати інформацію про проектування та реалізацію засобів управління, яка включає використання **<SA-04(02)_ODP[01] ВИБІРКОВОГО ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** на **<SA-04(02)_ODP[03] рівні деталізації>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються інтеграції вимог, описів та критеріїв інформаційної безпеки в процес придбання; тендерні документи; документація про придбання; договори придбання системи, компонентів системи або послуг системи; інформація про розробку та впровадження засобів контролю безпеки, що використовуються в системі, компоненти системи або служби системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання, підряд; персонал організації, відповідальний за визначення вимог безпеки системи; розробник системи або постачальник послуг; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для визначення рівня деталізації для проєктування системи та контролю безпеки; організаційні процеси для розробки контрактів на придбання; автоматизовані механізми, що підтримують та, або	

	впроваджують розробку деталей проєктування системи].

SA-4(3)	**ПРОЦЕС ЗАКУПІВЕЛЬ - МЕТОДИ, ТЕХНІКИ ТА ПРАКТИКИ РОЗРОБКИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-04(03)_ODP[01]	**визначені методи проєктування (інженерії) систем;**
	SA-04(03)_ODP[02]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {<SA-04(03)_ODP[03] методи інженерії безпеки системи>; <SA-04(03)_ODP[04] методи інженерії приватності>};**
	SA-04(03)_ODP[03]	**визначені методи інженерії безпеки системи (якщо вибрано);**
	SA-04(03)_ODP[04]	**визначені методи інженерії приватності (якщо вибрано);**
	SA-04(03)_ODP[05]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {<SA-04(03)_ODP[06] методи розробки програмного забезпечення>; <SA-04(03)_ODP[07] методи тестування, оцінки, аналізу, верифікації та валідації>; <SA-04(03)_ODP[08] процеси контролю якості>};**
	SA-04(03)_ODP[06]	**визначено методи розробки програмного забезпечення (якщо вибрано);**
	SA-04(03)_ODP[07]	**визначені методи тестування, оцінки, аналізу, верифікації та валідації (якщо вони були обрані);**
	SA-04(03)_ODP[08]	**визначені процеси контролю якості (якщо вибрано);**
	SA-04(03)(a)	повинен розробник системи, системного компонента або системної послуги демонструвати використання процесу життєвого циклу розробки системи, який включає **<SA-04(03)_ODP[01] методи системної інженерії>**;
	SA-04(03)(b)	повинен розробник системи, системного компонента або системної послуги демонструвати використання процесу життєвого циклу розробки системи, який включає **<SA-04(03)_ODP[02] ВИБІРКОВЕ ЗНАЧЕННЯ(Я) ПАРАМЕТРА(ів)>**;
	SA-04(03)(c)	повинен розробник системи, системного компонента або системної послуги демонструвати використання процесу життєвого циклу розробки системи, який включає **<SA-04(03)_ODP[05] ВИБІРКОВЕ ЗНАЧЕННЯ(Я) ПАРАМЕТРА(ів)>**.

	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються інтеграції вимог, описів та критеріїв інформаційної безпеки в процес придбання; тендерні документи; документація про придбання; договори придбання системи, компонентів системи або послуг системи; інформація про розробку та впровадження засобів контролю безпеки, що використовуються в системі, компоненти системи або служби системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання, підряд; персонал організації, відповідальний за визначення вимог безпеки системи; розробник системи або постачальник послуг; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для визначення рівня деталізації для проєктування системи та контролю безпеки; організаційні процеси для розробки контрактів на придбання; автоматизовані механізми, що підтримують та, або впроваджують розробку деталей проєктування системи].

SA-4(4)	**ПРОЦЕС ЗАКУПІВЕЛЬ - ВІДНЕСЕННЯ КОМПОНЕНТІВ ДО СИСТЕМ**
	[Вилучено: включено до CM-8(9)]

SA-4(5)	**ПРОЦЕС ЗАКУПІВЕЛЬ - КОНФІГУРАЦІЇ СИСТЕМИ, КОМПОНЕНТА ТА СИСТЕМНОЇ СЛУЖБИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-04(05)_ODP	**визначено конфігурації безпеки для системи, компонента або служби;**
	SA-04(05)(a)	повинен розробник системи, компонента системи або системної служби постачати систему, компонент або службу із впровадженими **<SA-04(05)_ODP конфігураціями безпеки>**;
	SA-04(05)(b)	будуть конфігурації використовуватися за замовчуванням для будь-якої наступної переінсталяції або оновлення системи, компонента чи служби.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються інтеграції вимог, описів та критеріїв інформаційної безпеки в процес придбання; тендерні документи; документація про придбання; договори придбання системи, компонента системи або послуги системи; конфігурації безпеки, які повинні бути реалізовані розробником системи, системного компонента або служби системи; угоди про рівень обслуговування; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання, підряд; персонал організації, відповідальний за визначення вимог безпеки системи; розробник системи або постачальник послуг; персонал організації, який	

	відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що використовуються для перевірки того, що конфігурація системи, компонента чи послуги, як надається, відповідає зазначеному].

SA-4(6)	**ПРОЦЕС ЗАКУПІВЕЛЬ - ВИКОРИСТАННЯ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-04(06)(a)	використовуються лише засоби захисту інформації, які пройшли державну експертизу або сертифікацію, створені для технічного та криптографічного захисту інформації;
	SA-04(06)(b)	були ці засоби захисту мають позитивний експертний висновок або сертифікат відповідності, а також відповідні дозволи для використання для захисту критичної інформації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються інтеграції вимог, описів та критеріїв інформаційної безпеки в процес придбання; тендерні документи; документація про придбання; договори придбання системи, компонента системи або послуги системи; конфігурації безпеки, які повинні бути реалізовані розробником системи, системного компонента або служби системи; угоди про рівень обслуговування; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання, підряд; персонал організації, відповідальний за визначення вимог безпеки системи; персонал організації, **Перевірка:** [ВИБІР: Процеси організації для вибору та використання оцінених та, або підтверджених продуктів та послуг із забезпечення безпеки інформації].	

SA-4(7)	**ПРОЦЕС ЗАКУПІВЕЛЬ - ЗАТВЕРДЖЕНІ ПРОФІЛІ ЗАХИЩЕНОСТІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-04(07)(a)	обмежується 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;
	SA-04(07)(b)	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.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються інтеграції вимог, описів та критеріїв інформаційної безпеки в процес придбання; тендерні документи; документація про придбання; договори придбання системи, компонента системи або послуги системи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання, підряд; персонал організації, відповідальний за визначення вимог безпеки системи; персонал організації, відповідальний за забезпечення продуктів забезпечення безпеки інформації]. **Перевірка:** [ВИБІР: Процеси організації вибору та використання продуктів, послуг, що оцінені].	

SA-4(8)	**ПРОЦЕС ЗАКУПІВЕЛЬ - ПЛАН БЕЗПЕРЕРВНОГО МОНІТОРИНГУ ЗАХОДІВ БЕЗПЕКИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-04(08)	розробник системи, системного компонента або системної служби створив план безперервного моніторингу ефективності заходів безпеки та приватності, який узгоджується з відповідним планом постійного моніторингу організації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються планів постійного моніторингу розробників; процедури, що стосуються інтеграції вимог, описів та критеріїв інформаційної безпеки в процес придбання; плани постійного моніторингу розробника; плани оцінки безпеки; договори придбання системи, компонента системи або послуги системи; документація про придбання; тендерна документація; угоди про рівень обслуговування; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання, підряд; персонал організації, відповідальний за визначення вимог безпеки системи; розробники інформаційних систем; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси постачальника для постійного моніторингу; автоматизовані механізми, що підтримують та, або впроваджують постійний моніторинг розробника].	

SA-4(9)	**ПРОЦЕС ЗАКУПІВЕЛЬ - ФУНКЦІЇ, ПОРТИ, ПРОТОКОЛИ ТА ПОСЛУГИ, ЩО ВИКОРИСТОВУЮТЬСЯ**

	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-04(09)[01]	зобов'язаний розробник системи, системного компонента або системного сервісу визначити функції, призначені для використання в організації;
	SA-04(09)[02]	зобов'язаний розробник системи, системного компонента або системної служби визначити порти, призначені для використання в організації;
	SA-04(09)[03]	зобов'язаний розробник системи, системного компонента або системної служби визначити протоколи, призначені для використання в організації;
	SA-04(09)[04]	зобов'язаний розробник системи, системного компонента або системної послуги визначити послуги, призначені для використання в організації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються інтеграції вимог, описів та критеріїв інформаційної безпеки в процес придбання; проєктна документація системи; документація системи, включаючи функції, порти, протоколи та послуги, призначені для організаційного використання; договори придбання інформаційних систем або послуг; документація про придбання; тендерна документація; угоди про рівень обслуговування; організаційні вимоги до безпеки, описи та критерії для розробників інформаційних систем, компонентів системи та служб системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання, підряд; персонал організації, відповідальний за визначення вимог безпеки системи; адміністратори системи, мережі; персонал організації, який працює, використовує та, або підтримує інформаційну систему; розробники інформаційних систем; персонал організації, відповідальний за інформаційну безпеку].	

SA-4(10)	**ПРОЦЕС ЗАКУПІВЕЛЬ - ФУНКЦІЇ, ПОРТИ, ПРОТОКОЛИ ТА ПОСЛУГИ, ЩО ВИКОРИСТОВУЮТЬСЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-04(10)	використовується лише та інформаційно-технічна продукція, що перебуває в списку продуктів схвалених FIPS 201, затверджених уповноваженим органом, для можливостей підтвердження особистості (PIV), реалізованих в системах організації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються інтеграції вимог, описів та критеріїв інформаційної безпеки в процес	

	придбання; тендерна документація; документація про придбання; договори придбання системи, компонента системи або послуги системи; угоди про рівень обслуговування; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання, підряд; персонал організації, відповідальний за визначення вимог безпеки системи; персонал організації, відповідальний за забезпечення впровадження лише продуктів, затверджених уповноваженим органом; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації вибору та використання продуктів, схвалених уповноваженим органом].

SA-4(11)	**ПРОЦЕС ЗАКУПІВЕЛЬ – СИСТЕМА ЗАПИСІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-04(11)_ODP	**визначені вимоги Закону про конфіденційність до функціонування записів системи;**
	SA-04(11)	визначені в договорі про закупівлю **<SA-04(11)_ODP вимоги Закону про конфіденційність>** для експлуатації системи записів від імені організації з метою виконання організаційної місії або функції.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання систем та послуг; процедури придбання систем та послуг; процедури, що стосуються інтеграції вимог Закону про конфіденційність у системи записів, що експлуатуються зовнішніми організаціями; тендерна документація; документація про придбання; контракти на придбання системи, системного компонента або системної послуги; угоди про рівень обслуговування; план захисту інформації системи; план забезпечення конфіденційності; політика обробки інформації, що дозволяє ідентифікувати особу; план програми забезпечення конфіденційності; оцінка впливу на конфіденційність; документація з оцінки ризиків для конфіденційності; інші відповідні документи чи записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за збір інформації; персонал організації, відповідальний за інформаційну безпеку та конфіденційність]. **Перевірка**: [ВИБІР: Процеси управління контрактами для перевірки вимог Закону про конфіденційність визначені для функціонування системи записів; процеси постачальника для демонстрації включення вимог Закону про конфіденційність в роботу системи записів].	

SA-4(12)	**ПРОЦЕС ЗАКУПІВЕЛЬ – ПРАВО ВЛАСНОСТІ НА ДАНІ**
	МЕТА ОЦІНКИ: Визначити, чи:

	SA-04(12)_ODP	**визначені часові рамки для видалення даних із системи підрядника та повернення їх до організації;**
	SA-04(12)(a)	включені вимоги щодо права власності на дані організації до договору про придбання;
	SA-04(12)(b)	потрібно видаляти всі дані з системи підрядника та повертати їх до організації протягом **<SA-04(12)_ODP період часу>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання систем та послуг; процедури придбання систем та послуг; процедури, що стосуються інтеграції вимог Закону про конфіденційність у системи записів, що експлуатуються зовнішніми організаціями; тендерна документація; документація про придбання; контракти на придбання системи, системного компонента або системної послуги; угоди про рівень обслуговування; план захисту інформації системи; план забезпечення конфіденційності; політика обробки інформації, що дозволяє ідентифікувати особу; план програми забезпечення конфіденційності; оцінка впливу на конфіденційність; документація з оцінки ризиків для конфіденційності; інші відповідні документи чи записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за закупівлю/ укладання контрактів; персонал організації, відповідальний за управління даними та вимоги до обробки даних; персонал організації, відповідальний за інформаційну безпеку та конфіденційність]. **Перевірка**: [ВИБІР: Процеси управління контрактами для перевірки того, що дані видаляються відповідно до вимог; процеси постачальника для видалення даних у встановлені терміни; механізми перевірки видалення та повернення даних].	

SA-5	**СИСТЕМНА ДОКУМЕНТАЦІЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-05_ODP[01]	**визначені дії, яких слід вжити, коли документація на систему, системний компонент або системне обслуговування недоступна або відсутня;**
	SA-05_ODP[02]	**визначено персонал або ролі для розповсюдження системної документації;**
	SA-05a.01[01]	отримана або розроблена документація для адміністратора системи, системного компонента або системної служби, яка описує безпечну конфігурацію системи, компонента або служби;
	SA-05a.01[02]	була отримана або розроблена документація для адміністратора системи, системного компонента або системної служби, яка описує безпечне встановлення системи, компонента або служби;
	SA-05a.01[03]	отримана або розроблена документація адміністратора

		системи, системного компонента або системної служби, яка описує безпечну роботу системи, компонента або служби;
	SA-05a.02[01]	отримана або розроблена адміністраторська документація системи, системного компонента або системної служби, яка описує ефективне використання функцій та механізмів безпеки;
	SA-05a.02[02]	була отримана або розроблена документація адміністратора системи, системного компонента або системної служби, яка описує безпечне встановлення системи, компонента або служби;
	SA-05a.02[03]	отримана або розроблена документація для адміністратора системи, системного компонента або системної служби, яка описує ефективне використання функцій і механізмів забезпечення конфіденційності;
	SA-05a.02[04]	отримана або розроблена документація для адміністратора системи, системного компонента або системної служби, яка описує ефективну підтримку функцій і механізмів забезпечення конфіденційності;
	SA-05a.03[01]	була отримана або розроблена документація адміністратора системи, системного компонента або системної служби, яка описує відомі вразливості, що стосуються конфігурації адміністративних або привілейованих функцій;
	SA-05a.03[02]	була отримана або розроблена документація адміністратора системи, системного компонента або системної служби, яка описує відомі вразливості, пов'язані з використанням адміністративних або привілейованих функцій;
	SA-05b.01[01]	отримана або розроблена користувацька документація системи, системного компонента або системної служби, яка описує доступні користувачеві функції та механізми безпеки;
	SA-05b.01[02]	отримана або розроблена користувацька документація системи, системного компоненту або системної служби, яка описує, як ефективно використовувати ці (доступні користувачеві) функції та механізми безпеки;
	SA-05b.01[03]	отримана або розроблена користувацька документація системи, системного компонента або системної служби, яка описує доступні користувачеві функції та механізми забезпечення конфіденційності;
	SA-05b.01[04]	отримана або розроблена користувацька документація системи, системного компонента або системної служби, яка описує, як ефективно використовувати ці (доступні користувачеві) функції та механізми захисту приватності;
	SA-05b.02[01]	отримана або розроблена користувацька документація системи, системного компонента або системної послуги, яка описує методи взаємодії з користувачем, що дозволяють особам використовувати систему, компонент або послугу в більш безпечний спосіб;

	SA-05b.02[02]	отримана або розроблена користувацька документація системи, системного компонента або системної служби, яка описує методи взаємодії з користувачем, що дозволяють особам використовувати систему, компонент або службу для захисту особистої приватності;
	SA-05b.03[01]	отримана або розроблена користувацька документація системи, системного компоненту або системного сервісу, яка описує обов'язки користувача щодо підтримання безпеки системи, компоненту або сервісу;
	SA-05b.03[02]	отримана або розроблена користувацька документація системи, системного компонента або системної служби, яка описує обов'язки користувачів щодо збереження приватності приватних осіб;
	SA-05c.[01]	були задокументовані спроби отримати документацію на систему, системний компонент або системне обслуговування, коли така документація або недоступна, або взагалі не існує;
	SA-05c.[02]	після спроб отримати документацію системи, системного компонента або системної служби, коли така документація недоступна або не існує, у відповідь виконуються **<SA-05_ODP[01] дії>**;
	SA-05d.	розповсюджується документація серед <**SA-05_ODP[02] персоналу або ролей>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання систем та послуг; процедури придбання систем та послуг; процедури, що стосуються інтеграції вимог Закону про конфіденційність у системи записів, що експлуатуються зовнішніми організаціями; тендерна документація; документація про придбання; контракти на придбання системи, системного компонента або системної послуги; угоди про рівень обслуговування; план захисту інформації системи; план забезпечення конфіденційності; політика обробки інформації, що дозволяє ідентифікувати особу; план програми забезпечення конфіденційності; оцінка впливу на конфіденційність; документація з оцінки ризиків для конфіденційності; інші відповідні документи чи записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за збір інформації; персонал організації, відповідальний за інформаційну безпеку та конфіденційність]. **Перевірка**: [ВИБІР: Процеси управління контрактами для перевірки вимог Закону про конфіденційність визначені для функціонування системи записів; процеси постачальника для демонстрації включення вимог Закону про конфіденційність в роботу системи записів].	

SA-5(1)	**СИСТЕМНА ДОКУМЕНТАЦІЯ - ФУНКЦІОНАЛЬНІ ВЛАСТИВОСТІ ЗАХОДІВ БЕЗПЕКИ**
	[Вилучено: включено до SA-4(1)].

SA-5(2)	**СИСТЕМНА ДОКУМЕНТАЦІЯ - ЗОВНІШНІ СИСТЕМНІ ІНТЕРФЕЙСИ,**

	ЩО СТОСУЮТЬСЯ БЕЗПЕКИ
	[Вилучено: включено до SA-4(2)].

SA-5(3)	**СИСТЕМНА ДОКУМЕНТАЦІЯ - АРХІТЕКТУРА (ПРОЄКТ) ВИСОКОГО РІВНЯ**
	[Вилучено: включено до SA-4(2)].

SA-5(4)	**СИСТЕМНА ДОКУМЕНТАЦІЯ - АРХІТЕКТУРА (ПРОЄКТ) НИЗЬКОГО РІВНЯ**
	[Вилучено: включено до SA-4(2)].

SA-5(5)	**СИСТЕМНА ДОКУМЕНТАЦІЯ - ВИХІДНИЙ КОД**
	[Вилучено: включено до SA-4(2)].

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**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-08_ODP[01]	**визначені принципи інжинірингу безпеки систем;**
	SA-08_ODP[02]	**визначені принципи інжинірингу конфіденційності системи;**
	SA-08[01]	застосовуються **<SA-08_ODP[01] принципи інжинірингу безпеки систем>** у специфікації системи та компонентів системи;
	SA-08[02]	застосовуються **<SA-08_ODP[01] принципи інжинірингу безпеки систем>** при розробці системи та її компонентів;
	SA-08[03]	були застосовані **<SA-08_ODP[01] принципи інжинірингу безпеки систем>** при розробці системи та компонентів систем;
	SA-08[04]	застосовуються **<SA-08_ODP[01] принципи інжинірингу безпеки систем>** при реалізації системи та компонентів систем;
	SA-08[05]	застосовуються **<SA-08_ODP[01] принципи інжинірингу безпеки систем>** при модифікації системи та компонентів систем;
	SA-08[06]	застосовуються **<SA-08_ODP[02] принципи інжинірингу конфіденційності>** у специфікації системи та компонентів систем;

	SA-08[07]	застосовуються **<SA-08_ODP[02] принципи інжинірингу конфіденційності>** при розробці системи та компонентів систем;
	SA-08[08]	застосовуються **<SA-08_ODP[02] принципи інжинірингу конфіденційності>** при розробці системи та компонентів систем;
	SA-08[09]	застосовуються **<SA-08_ODP[02] принципи інжинірингу конфіденційності>** при реалізації системи та компонентів систем;
	SA-08[10]	застосовуються **<SA-08_ODP[02] принципи інжинірингу конфіденційності>** при модифікації системи та компонентів систем.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання систем та послуг; процедури придбання систем та послуг; процедури, що стосуються інтеграції вимог Закону про конфіденційність у системи записів, що експлуатуються зовнішніми організаціями; тендерна документація; документація про придбання; контракти на придбання системи, системного компонента або системної послуги; угоди про рівень обслуговування; план захисту інформації системи; план забезпечення конфіденційності; політика обробки інформації, що дозволяє ідентифікувати особу; план програми забезпечення конфіденційності; оцінка впливу на конфіденційність; документація з оцінки ризиків для конфіденційності; інші відповідні документи чи записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за закупівлю/ укладання контрактів; персонал організації, відповідальний за управління даними та вимоги до обробки даних; персонал організації, відповідальний за інформаційну безпеку та конфіденційність]. **Перевірка**: [ВИБІР: Процеси управління контрактами для перевірки того, що дані видаляються відповідно до вимог; процеси постачальника для видалення даних у встановлені терміни; механізми перевірки видалення та повернення даних].	

SA-8(1)	**БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - ЧІТКА АБСТРАКЦІЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-08(01)	реалізовано принцип проектування безпеки чітких абстракцій.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються принципу проектування безпеки чітких абстракцій, які використовуються при специфікації, проектуванні, розробці, впровадженні та модифікації системи; проектна документація системи; вимоги та специфікації безпеки та конфіденційності для системи; архітектура безпеки та	

	конфіденційності системи; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за визначення вимог до безпеки та конфіденційності системи; персонал організації, відповідальний за специфікацію, проектування, розробку, впровадження та модифікацію системи; розробники системи; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка**: [ВИБІР: Процеси організації застосування принципу проектування безпеки на основі чітких абстракцій до специфікації, проектування, розробки, впровадження та модифікації систем; механізми, що підтримують застосування принципу проектування безпеки на основі чітких абстракцій до специфікації, проектування, розробки, впровадження та модифікації систем].

SA-8(2)	**БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - НАЙМЕНШ ПОШИРЕНИЙ МЕХАНІЗМ**
	МЕТА ОЦІНКИ: Визначити, чи:

SA-08(02)_ODP	**реалізовано принцип проектування безпеки чітких абстракцій.**
SA-08(02)	реалізують **<SA-08(02)_ODP системи або компоненти системи>** принцип побудови безпеки за принципом найменш поширеного механізму.

ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ:

Дослідження: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються принципу проектування безпеки чітких абстракцій, які використовуються при специфікації, проектуванні, розробці, впровадженні та модифікації системи; проектна документація системи; вимоги та специфікації безпеки та конфіденційності для системи; архітектура безпеки та конфіденційності системи; план захисту інформації системи; інші відповідні документи або записи].

Співбесіда: [ВИБІР: Персонал організації, відповідальний за визначення вимог до безпеки та конфіденційності системи; персонал організації, відповідальний за специфікацію, проектування, розробку, впровадження та модифікацію системи; розробники системи; персонал організації, відповідальний за інформаційну безпеку].

Перевірка: [ВИБІР: Процеси організації застосування принципу проектування безпеки на основі чітких абстракцій до специфікації, проектування, розробки, впровадження та модифікації систем; механізми, що підтримують застосування принципу проектування безпеки на основі чітких абстракцій до специфікації, проектування, розробки, впровадження та модифікації систем].

SA-8(3)	**БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - МОДУЛЬНІСТЬ І БАГАТОРІВНЕВІСТЬ**

	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-08(03)_ODP[01]	**визначені системи або компоненти системи, які реалізують принцип модульності дизайну безпеки;**
	SA-08(03)_ODP[02]	**визначені системи або компоненти системи, які реалізують принцип багаторівневого проектування безпеки;**
	SA-08(03)[01]	**<SA-08(03)_ODP[01] системи або компоненти системи>** реалізують принцип модульності проектування безпеки;
	SA-08(03)[02]	**<SA-08(03)_ODP[02] системи або компоненти системи>** реалізують принцип багаторівневого проектування безпеки.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються принципу проектування безпеки чітких абстракцій, які використовуються при специфікації, проектуванні, розробці, впровадженні та модифікації системи; проектна документація системи; вимоги та специфікації безпеки та конфіденційності для системи; архітектура безпеки та конфіденційності системи; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за визначення вимог до безпеки та конфіденційності системи; персонал організації, відповідальний за специфікацію, проектування, розробку, впровадження та модифікацію системи; розробники системи; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка**: [ВИБІР: Процеси організації застосування принципу проектування безпеки на основі чітких абстракцій до специфікації, проектування, розробки, впровадження та модифікації систем; механізми, що підтримують застосування принципу проектування безпеки на основі чітких абстракцій до специфікації, проектування, розробки, впровадження та модифікації систем].	

SA-8(4)	**БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ – ЧАСТКОВО ВПОРЯДКОВАНІ ЗАЛЕЖНОСТІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-08(04)_ODP	**визначені системи або компоненти системи, які реалізують принцип проектування безпеки частково впорядкованих залежностей;**
	SA-08(04)	**<SA-08(04)_ODP системи або компоненти системи>** реалізують принцип проектування безпеки частково впорядкованих залежностей.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ:	

	Дослідження: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються принципу проектування безпеки чітких абстракцій, які використовуються при специфікації, проектуванні, розробці, впровадженні та модифікації системи; проектна документація системи; вимоги та специфікації безпеки та конфіденційності для системи; архітектура безпеки та конфіденційності системи; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за визначення вимог до безпеки та конфіденційності системи; персонал організації, відповідальний за специфікацію, проектування, розробку, впровадження та модифікацію системи; розробники системи; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка**: [ВИБІР: Процеси організації застосування принципу проектування безпеки на основі чітких абстракцій до специфікації, проектування, розробки, впровадження та модифікації систем; механізми, що підтримують застосування принципу проектування безпеки на основі чітких абстракцій до специфікації, проектування, розробки, впровадження та модифікації систем].

SA-8(5)	**БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - ЕФЕКТИВНИЙ ОПОСЕРЕДКОВАНИЙ ДОСТУП**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-08(05)_ODP	**визначені системи або її компоненти, які реалізують принцип проектування безпеки ефективного опосередкованого доступу;**
	SA-08(05)	**<SA-08(05)_ODP системи або компоненти системи>** реалізують принцип проектування безпеки ефективного опосередкованого доступу.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються принципу проектування безпеки чітких абстракцій, які використовуються при специфікації, проектуванні, розробці, впровадженні та модифікації системи; проектна документація системи; вимоги та специфікації безпеки та конфіденційності для системи; архітектура безпеки та конфіденційності системи; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за визначення вимог до безпеки та конфіденційності системи; персонал організації, відповідальний за специфікацію, проектування, розробку, впровадження та модифікацію системи; розробники системи; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка**: [ВИБІР: Процеси організації застосування принципу проектування безпеки на основі чітких абстракцій до специфікації, проектування, розробки, впровадження та модифікації систем; механізми, що підтримують застосування принципу проектування безпеки на основі чітких абстракцій до специфікації,	

	проектування, розробки, впровадження та модифікації систем].

SA-8(6)	**БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - МІНІМІЗОВАНИЙ ОБМІН**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-08(06)_ODP	**визначені системи або компоненти системи, які реалізують принцип проектування безпеки, що полягає в мінімізації спільного використання;**
	SA-08(06)	**<SA-08(06)_ODP системи або компоненти системи>** реалізують принцип побудови безпеки за принципом мінімізації спільного використання.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються принципу проектування безпеки чітких абстракцій, які використовуються при специфікації, проектуванні, розробці, впровадженні та модифікації системи; проектна документація системи; вимоги та специфікації безпеки та конфіденційності для системи; архітектура безпеки та конфіденційності системи; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за визначення вимог до безпеки та конфіденційності системи; персонал організації, відповідальний за специфікацію, проектування, розробку, впровадження та модифікацію системи; розробники системи; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка**: [ВИБІР: Процеси організації застосування принципу проектування безпеки на основі чітких абстракцій до специфікації, проектування, розробки, впровадження та модифікації систем; механізми, що підтримують застосування принципу проектування безпеки на основі чітких абстракцій до специфікації, проектування, розробки, впровадження та модифікації систем].	

SA-8(7)	**БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - ЗНИЖЕНА СКЛАДНІСТЬ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-08(07)_ODP	**визначені системи або компоненти системи, які реалізують принцип проектування безпеки за принципом зниженої складності;**
	SA-08(07)	**<SA-08(07)_ODP системи або компоненти системи>** реалізують принцип проектування безпеки за принципом зниженої складності.

	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються принципу проектування безпеки чітких абстракцій, які використовуються при специфікації, проектуванні, розробці, впровадженні та модифікації системи; проектна документація системи; вимоги та специфікації безпеки та конфіденційності для системи; архітектура безпеки та конфіденційності системи; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за визначення вимог до безпеки та конфіденційності системи; персонал організації, відповідальний за специфікацію, проектування, розробку, впровадження та модифікацію системи; розробники системи; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка**: [ВИБІР: Процеси організації застосування принципу проектування безпеки на основі чітких абстракцій до специфікації, проектування, розробки, впровадження та модифікації систем; механізми, що підтримують застосування принципу проектування безпеки на основі чітких абстракцій до специфікації, проектування, розробки, впровадження та модифікації систем].

SA-8(8)	**БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - ЕВОЛЮЦІЯ БЕЗПЕКИ В СИСТЕМІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-08(08)_ODP	**визначені системи або компоненти системи, які реалізують принцип безпечного проектування безпечної еволюційності;**
	SA-08(08)	**<SA-08(08)_ODP системи або компоненти системи>** реалізують принцип безпечного проектування безпечної еволюційності.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються принципу проектування безпеки чітких абстракцій, які використовуються при специфікації, проектуванні, розробці, впровадженні та модифікації системи; проектна документація системи; вимоги та специфікації безпеки та конфіденційності для системи; архітектура безпеки та конфіденційності системи; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за визначення вимог до безпеки та конфіденційності системи; персонал організації, відповідальний за специфікацію, проектування, розробку, впровадження та модифікацію системи; розробники системи; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка**: [ВИБІР: Процеси організації застосування принципу проектування безпеки на основі чітких абстракцій до специфікації, проектування, розробки,	

	впровадження та модифікації систем; механізми, що підтримують застосування принципу проектування безпеки на основі чітких абстракцій до специфікації, проектування, розробки, впровадження та модифікації систем].

SA-8(9)	**БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - ДОВІРЕНІ КОМПОНЕНТИ СИСТЕМИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-08(09)_ODP	**визначені системи або компоненти системи, які реалізують принцип побудови безпеки довірених компонентів;**
	SA-08(09)	**<SA-08(09)_ODP системи або компоненти системи>** реалізують принцип побудови безпеки довірених компонентів.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються принципу проектування безпеки чітких абстракцій, які використовуються при специфікації, проектуванні, розробці, впровадженні та модифікації системи; проектна документація системи; вимоги та специфікації безпеки та конфіденційності для системи; архітектура безпеки та конфіденційності системи; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за визначення вимог до безпеки та конфіденційності системи; персонал організації, відповідальний за специфікацію, проектування, розробку, впровадження та модифікацію системи; розробники системи; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка**: [ВИБІР: Процеси організації застосування принципу проектування безпеки на основі чітких абстракцій до специфікації, проектування, розробки, впровадження та модифікації систем; механізми, що підтримують застосування принципу проектування безпеки на основі чітких абстракцій до специфікації, проектування, розробки, впровадження та модифікації систем].	

SA-8(10)	**БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - ІЄРАРХІЧНА ДОВІРА**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-08(10)_ODP	**визначені системи або компоненти системи, які реалізують принцип ієрархічної довіри при проектуванні безпеки;**
	SA-08(10)	**<SA-08(09)_ODP системи або компоненти системи>** реалізують принцип ієрархічної довіри в дизайні безпеки.

	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються принципу проектування безпеки чітких абстракцій, які використовуються при специфікації, проектуванні, розробці, впровадженні та модифікації системи; проектна документація системи; вимоги та специфікації безпеки та конфіденційності для системи; архітектура безпеки та конфіденційності системи; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за визначення вимог до безпеки та конфіденційності системи; персонал організації, відповідальний за специфікацію, проектування, розробку, впровадження та модифікацію системи; розробники системи; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка**: [ВИБІР: Процеси організації застосування принципу проектування безпеки на основі чітких абстракцій до специфікації, проектування, розробки, впровадження та модифікації систем; механізми, що підтримують застосування принципу проектування безпеки на основі чітких абстракцій до специфікації, проектування, розробки, впровадження та модифікації систем].

SA-8(11)	**ЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - ЗВОРОТНІЙ ПОРІГ МОДИФІКАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-08(11)_ODP	**визначені системи або компоненти системи, які реалізують принцип ієрархічної довіри при проектуванні безпеки;**
	SA-08(11)	**<SA-08(11)_ODP системи або компоненти системи>** реалізують принцип проектування безпеки зворотного порогу модифікації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються принципу проектування безпеки чітких абстракцій, які використовуються при специфікації, проектуванні, розробці, впровадженні та модифікації системи; проектна документація системи; вимоги та специфікації безпеки та конфіденційності для системи; архітектура безпеки та конфіденційності системи; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за визначення вимог до безпеки та конфіденційності системи; персонал організації, відповідальний за специфікацію, проектування, розробку, впровадження та модифікацію системи; розробники системи; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка**: [ВИБІР: Процеси організації застосування принципу проектування безпеки на основі чітких абстракцій до специфікації, проектування, розробки,	

	впровадження та модифікації систем; механізми, що підтримують застосування принципу проектування безпеки на основі чітких абстракцій до специфікації, проектування, розробки, впровадження та модифікації систем].

SA-8(12)	**БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - ІЄРАРХІЧНИЙ ЗАХИСТ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-08(12)_ODP	**визначені системи або компоненти системи, які реалізують принцип ієрархічного дизайну безпеки;**
	SA-08(12)	**<SA-08(12)_ODP системи або компоненти системи>** реалізують принцип побудови ієрархічного захисту.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються принципу проектування безпеки чітких абстракцій, які використовуються при специфікації, проектуванні, розробці, впровадженні та модифікації системи; проектна документація системи; вимоги та специфікації безпеки та конфіденційності для системи; архітектура безпеки та конфіденційності системи; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за визначення вимог до безпеки та конфіденційності системи; персонал організації, відповідальний за специфікацію, проектування, розробку, впровадження та модифікацію системи; розробники системи; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка**: [ВИБІР: Процеси організації застосування принципу проектування безпеки на основі чітких абстракцій до специфікації, проектування, розробки, впровадження та модифікації систем; механізми, що підтримують застосування принципу проектування безпеки на основі чітких абстракцій до специфікації, проектування, розробки, впровадження та модифікації систем].	

SA - 8(13)	**БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - МІНІМІЗОВАНІ ЕЛЕМЕНТИ БЕЗПЕКИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-08(13)_ODP	**визначено системи або компоненти системи, які реалізують принцип проектування безпеки за принципом мінімізації елементів безпеки;**
	SA-08(13)	**<SA-08(13)_ODP системи або компоненти системи>** реалізують принцип проектування безпеки з мінімізацією елементів безпеки.

	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються принципу мінімізації елементів безпеки, які використовуються в специфікації, проектуванні, розробці, впровадженні та модифікації системи; проектна документація системи; вимоги та специфікації безпеки та конфіденційності для системи; архітектура безпеки та конфіденційності системи; план захисту інформації системи; інші відповідні документи або записи].**Співбесіда**: [ВИБІР: Персонал організації, відповідальний за визначення вимог до безпеки та конфіденційності системи; персонал організації, відповідальний за специфікацію, проектування, розробку, впровадження та модифікацію системи; розробники системи; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка**: [ВИБІР: Процеси організації застосування принципу проектування безпеки з мінімізацією елементів безпеки при специфікації, проектуванні, розробці, впровадженні та модифікації системи; механізми, що підтримують застосування принципу проектування безпеки з мінімізацією елементів безпеки при специфікації, проектуванні, розробці, впровадженні та модифікації системи].

SA-8(14)	**БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - НАЙМЕНШІ ПРИВІЛЕЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-08(14)_ODP	**визначено системи або компоненти системи, які реалізують принцип побудови безпеки за принципом найменших привілеїв;**
	SA-08(14)	**<SA-08(14)_ODP системи або компоненти системи>** реалізують принцип побудови безпеки за принципом найменших привілеїв.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються принципу найменших привілеїв, які використовуються при специфікації, проектуванні, розробці, впровадженні та модифікації системи; проектна документація системи; вимоги та специфікації безпеки та конфіденційності для системи; архітектура безпеки та конфіденційності системи; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за визначення вимог до безпеки та конфіденційності системи; персонал організації, відповідальний за специфікацію, проектування, розробку, впровадження та модифікацію системи; розробники системи; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка**: [ВИБІР: Процеси організації для застосування принципу найменших привілеїв у специфікації, проектуванні, розробці, впровадженні та модифікації систем; механізми, що підтримують застосування принципу найменших привілеїв у специфікації, проектуванні, розробці, впровадженні та модифікації	

	систем].

SA-8(15)	**БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - ПРЕДИКАТНИЙ ДОЗВІЛ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-08(15)_ODP	**визначено системи або компоненти системи, які реалізують принцип проектування безпеки попереднього дозволу;**
	SA-08(15)	**<SA-08(15)_ODP системи або компоненти системи>** реалізують принцип проектування безпеки попереднього дозволу.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються принципу проектування безпеки попереднього дозволу, який використовується в специфікації, проектуванні, розробці, впровадженні та модифікації системи; проектна документація системи; вимоги та специфікації безпеки та конфіденційності для системи; архітектура безпеки та конфіденційності системи; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за визначення вимог до безпеки та конфіденційності системи; персонал організації, відповідальний за специфікацію, проектування, розробку, впровадження та модифікацію системи; розробники системи; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка**: [ВИБІР: Процеси організації застосування принципу проектування безпеки попереднього дозволу при специфікації, проектуванні, розробці, впровадженні та модифікації систем; механізми, що підтримують застосування принципу проектування безпеки попереднього дозволу при специфікації, проектуванні, розробці, впровадженні та модифікації систем].	

SA-8(16)	**БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - САМОСТІЙНА НАДІЙНІСТЬ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-08(16)_ODP	**визначено системи або компоненти системи, які реалізують принцип проектування безпеки, що ґрунтується на самодостатній надійності;**
	SA-08(16)	**<SA-08(16)_ODP системи або компоненти системи>** реалізують принцип проектування безпеки самодостатньої надійності.

	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються принципу проектування безпеки попереднього дозволу, який використовується в специфікації, проектуванні, розробці, впровадженні та модифікації системи; проектна документація системи; вимоги та специфікації безпеки та конфіденційності для системи; архітектура безпеки та конфіденційності системи; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за визначення вимог до безпеки та конфіденційності системи; персонал організації, відповідальний за специфікацію, проектування, розробку, впровадження та модифікацію системи; розробники системи; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка**: [ВИБІР: Процеси організації застосування принципу проектування безпеки попереднього дозволу при специфікації, проектуванні, розробці, впровадженні та модифікації систем; механізми, що підтримують застосування принципу проектування безпеки попереднього дозволу при специфікації, проектуванні, розробці, впровадженні та модифікації систем].

SA-8(17)	**БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - БЕЗПЕЧНО РОЗПОДІЛЕНА КОМПОЗИЦІЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-08(17)_ODP	**визначено системи або компоненти системи, які реалізують принцип безпечного проектування захищеного розподіленого вмісту;**
	SA-08(17)	**<SA-08(17)_ODP системи або компоненти системи>** реалізують принцип проектування безпеки захищеного розподіленого вмісту.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються принципу проектування безпеки попереднього дозволу, який використовується в специфікації, проектуванні, розробці, впровадженні та модифікації системи; проектна документація системи; вимоги та специфікації безпеки та конфіденційності для системи; архітектура безпеки та конфіденційності системи; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за визначення вимог до безпеки та конфіденційності системи; персонал організації, відповідальний за специфікацію, проектування, розробку, впровадження та модифікацію системи; розробники системи; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка**: [ВИБІР: Процеси організації застосування принципу проектування безпеки попереднього дозволу при специфікації, проектуванні, розробці,	

	впровадженні та модифікації систем; механізми, що підтримують застосування принципу проектування безпеки попереднього дозволу при специфікації, проектуванні, розробці, впровадженні та модифікації систем].

SA-8(18)	**БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - ДОВІРЕНІ КАНАЛИ КОМУНІКАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-08(18)_ODP	**визначено системи або компоненти системи, які реалізують принцип побудови безпеки довірених каналів зв'язку;**
	SA-08(18)	**<SA-08(18)_ODP системи або компоненти системи>** реалізують принцип побудови безпеки довірених каналів зв'язку.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються принципу проектування безпеки попереднього дозволу, який використовується в специфікації, проектуванні, розробці, впровадженні та модифікації системи; проектна документація системи; вимоги та специфікації безпеки та конфіденційності для системи; архітектура безпеки та конфіденційності системи; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за визначення вимог до безпеки та конфіденційності системи; персонал організації, відповідальний за специфікацію, проектування, розробку, впровадження та модифікацію системи; розробники системи; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка**: [ВИБІР: Процеси організації застосування принципу проектування безпеки попереднього дозволу при специфікації, проектуванні, розробці, впровадженні та модифікації систем; механізми, що підтримують застосування принципу проектування безпеки попереднього дозволу при специфікації, проектуванні, розробці, впровадженні та модифікації систем].	

SA-8(19)	**БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - ПОСТІЙНИЙ ЗАХИСТ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-08(19)_ODP	**визначено системи або компоненти системи, які втілюють принцип проектування безпеки довготривалого захисту.**
	SA-08(19)	**<SA-08(19)_ODP системи або компоненти системи>** реалізують принцип проектування безпеки довготривалого

		захисту.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються принципу проектування безпеки попереднього дозволу, який використовується в специфікації, проектуванні, розробці, впровадженні та модифікації системи; проектна документація системи; вимоги та специфікації безпеки та конфіденційності для системи; архітектура безпеки та конфіденційності системи; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за визначення вимог до безпеки та конфіденційності системи; персонал організації, відповідальний за специфікацію, проектування, розробку, впровадження та модифікацію системи; розробники системи; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка**: [ВИБІР: Процеси організації застосування принципу проектування безпеки попереднього дозволу при специфікації, проектуванні, розробці, впровадженні та модифікації систем; механізми, що підтримують застосування принципу проектування безпеки попереднього дозволу при специфікації, проектуванні, розробці, впровадженні та модифікації систем].	

SA-8(20)	**БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - БЕЗПЕЧНЕ КЕРУВАННЯ МЕТАДАНИМИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-08(20)_ODP	**визначено системи або компоненти системи, які реалізують принцип безпечного управління метаданими.**
	SA-08(20)	**<SA-08(20)_ODP системи або компоненти системи>** реалізують принцип безпечного управління метаданими.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються принципу проектування безпеки попереднього дозволу, який використовується в специфікації, проектуванні, розробці, впровадженні та модифікації системи; проектна документація системи; вимоги та специфікації безпеки та конфіденційності для системи; архітектура безпеки та конфіденційності системи; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за визначення вимог до безпеки та конфіденційності системи; персонал організації, відповідальний за специфікацію, проектування, розробку, впровадження та модифікацію системи; розробники системи; персонал організації, відповідальний за інформаційну	

	безпеку]. **Перевірка**: [ВИБІР: Процеси організації застосування принципу проектування безпеки попереднього дозволу при специфікації, проектуванні, розробці, впровадженні та модифікації систем; механізми, що підтримують застосування принципу проектування безпеки попереднього дозволу при специфікації, проектуванні, розробці, впровадженні та модифікації систем].

SA-8(21)	**БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - САМОАНАЛІЗ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-08(21)_ODP	**визначено системи або компоненти системи, які реалізують принцип самоаналізу при проектуванні безпеки;**
	SA-08(21)	**<SA-08(21)_ODP системи або компоненти системи>** реалізують принцип проектування безпеки на основі самоаналізу.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються принципу проектування безпеки попереднього дозволу, який використовується в специфікації, проектуванні, розробці, впровадженні та модифікації системи; проектна документація системи; вимоги та специфікації безпеки та конфіденційності для системи; архітектура безпеки та конфіденційності системи; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за визначення вимог до безпеки та конфіденційності системи; персонал організації, відповідальний за специфікацію, проектування, розробку, впровадження та модифікацію системи; розробники системи; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка**: [ВИБІР: Процеси організації застосування принципу проектування безпеки попереднього дозволу при специфікації, проектуванні, розробці, впровадженні та модифікації систем; механізми, що підтримують застосування принципу проектування безпеки попереднього дозволу при специфікації, проектуванні, розробці, впровадженні та модифікації систем].	

SA-8(22)	**БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - ЗВІТНІСТЬ І ВІДСТЕЖУВАНІСТЬ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-08(22)_ODP[1]	**визначено системи або компоненти системи, які реалізують принцип самоаналізу при проектуванні**

		безпеки;
	SA-08(22)_ODP[2]	**визначено системи або компоненти системи, які реалізують принцип відстежуваності при проектуванні безпеки;**
	SA-08(22)[1]	**<SA-08(22)_ODP[01] системи або компоненти системи>** реалізують принцип звітності при проектуванні безпеки;
	SA-08(22)[2]	**<SA-08(22)_ODP[02] системи або компоненти системи >** реалізують принцип відстежуваності при проектуванні безпеки.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання системи та послуг; політика аудиту та звітності; політика контролю доступу; процедури, що стосуються найменших привілеїв; процедури, що стосуються подій, які підлягають аудиту; політика ідентифікації та автентифікації; процедури, що стосуються ідентифікації та автентифікації користувачів; процедури, що стосуються принципу звітності та відстежуваності, який використовується під час специфікації, проектування, розробки, впровадження та модифікації системи; документація з проектування системи; записи аудиту системи; події, що підлягають аудиту системи; налаштування конфігурації системи та пов'язана з ними документація; вимоги та специфікації щодо безпеки та конфіденційності для системи; архітектура безпеки та конфіденційності системи; план забезпечення безпеки системи; інші відповідні документи чи записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за визначення вимог до безпеки та конфіденційності системи; персонал організації, відповідальний за аудит та звітність; персонал організації, відповідальний за специфікацію, проектування, розробку, впровадження та модифікацію системи; розробники системи; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка**: [ВИБІР: Процеси організації застосування принципу звітності та відстежуваності при проектуванні, розробці, впровадженні та модифікації систем; механізми підтримки застосування принципу звітності та відстежуваності при проектуванні, розробці, впровадженні та модифікації систем; механізми реалізації аудиту інформаційних систем; механізми реалізації функцій з найменшими привілеями].	

SA-8(23)	**БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - БЕЗПЕЧНІ ПАРАМЕТРИ ЗА ЗАМОВЧУВАННЯМ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-08(23)_ODP	**визначено системи або компоненти системи, які реалізують принцип безпечних налаштувань за замовчуванням;**

	SA-08(23)	**<SA-08(23)_ODP системи або компоненти системи>** реалізують принцип проектування безпечних налаштувань за замовчуванням.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання системи та послуг; політика аудиту та звітності; політика контролю доступу; процедури, що стосуються найменших привілеїв; процедури, що стосуються подій, які підлягають аудиту; політика ідентифікації та автентифікації; процедури, що стосуються ідентифікації та автентифікації користувачів; процедури, що стосуються принципу звітності та відстежуваності, який використовується під час специфікації, проектування, розробки, впровадження та модифікації системи; документація з проектування системи; записи аудиту системи; події, що підлягають аудиту системи; налаштування конфігурації системи та пов'язана з ними документація; вимоги та специфікації щодо безпеки та конфіденційності для системи; архітектура безпеки та конфіденційності системи; план забезпечення безпеки системи; інші відповідні документи чи записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за визначення вимог до безпеки та конфіденційності системи; персонал організації, відповідальний за аудит та звітність; персонал організації, відповідальний за специфікацію, проектування, розробку, впровадження та модифікацію системи; розробники системи; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка**: [ВИБІР: Процеси організації застосування принципу звітності та відстежуваності при проектуванні, розробці, впровадженні та модифікації систем; механізми підтримки застосування принципу звітності та відстежуваності при проектуванні, розробці, впровадженні та модифікації систем; механізми реалізації аудиту інформаційних систем; механізми реалізації функцій з найменшими привілеями].	

SA-8(24)	**БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - ЗБОЇ БЕЗПЕКИ І ВІДНОВЛЕННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-08(24)_ODP[1]	**визначено системи або компоненти системи, які реалізують принцип безпечних збоїв;**
	SA-08(24)_ODP[2]	**визначено системи або компоненти системи, які реалізують принцип безпечного відновлення;**
	SA-08(24)[1]	**<SA-08(24)_ODP[01] системи або компоненти системи>** реалізують принцип безпечних збоїв;
	SA-08(24)[2]	**<SA-08(24)_ODP[02] системи або компоненти системи>** реалізують принцип безпечного відновлення.

	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання системи та послуг; політика аудиту та звітності; політика контролю доступу; процедури, що стосуються найменших привілеїв; процедури, що стосуються подій, які підлягають аудиту; політика ідентифікації та автентифікації; процедури, що стосуються ідентифікації та автентифікації користувачів; процедури, що стосуються принципу звітності та відстежуваності, який використовується під час специфікації, проектування, розробки, впровадження та модифікації системи; документація з проектування системи; записи аудиту системи; події, що підлягають аудиту системи; налаштування конфігурації системи та пов'язана з ними документація; вимоги та специфікації щодо безпеки та конфіденційності для системи; архітектура безпеки та конфіденційності системи; план забезпечення безпеки системи; інші відповідні документи чи записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за визначення вимог до безпеки та конфіденційності системи; персонал організації, відповідальний за аудит та звітність; персонал організації, відповідальний за специфікацію, проектування, розробку, впровадження та модифікацію системи; розробники системи; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка**: [ВИБІР: Процеси організації застосування принципу звітності та відстежуваності при проектуванні, розробці, впровадженні та модифікації систем; механізми підтримки застосування принципу звітності та відстежуваності при проектуванні, розробці, впровадженні та модифікації систем; механізми реалізації аудиту інформаційних систем; механізми реалізації функцій з найменшими привілеями].

SA-8(25)	**БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - ЕКОНОМІЧНА БЕЗПЕКА**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-08(25)_ODP	**визначено системи або компоненти системи, які реалізують принцип безпеки економіки;**
	SA-08(25)	**<SA-08(25)_ODP системи або компоненти системи>** реалізують принцип безпеки економіки.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються принципів безпеки економіки, які використовуються в специфікації, проектуванні, розробці, впровадженні та модифікації системи; проектна документація системи; вимоги та специфікації безпеки та конфіденційності для системи; архітектура безпеки та конфіденційності системи; аналіз компромісів між продуктивністю та безпекою; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за визначення вимог до безпеки та конфіденційності системи; персонал організації, відповідальний за специфікацію, проектування, розробку, впровадження та модифікацію системи;	

	розробники системи; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка**: [ВИБІР: Процеси організації застосування принципу безпеки економіки при специфікації, проектуванні, розробці, впровадженні та модифікації систем; механізми, що підтримують застосування принципу безпеки економіки при специфікації, проектуванні, розробці, впровадженні та модифікації систем].

SA-8(26)	**БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - БЕЗПЕКА ПРОДУКТИВНОСТІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-08(26)_ODP	**визначено системи або компоненти системи, які реалізують принцип безпеки продуктивності;**
	SA-08(26)	**<SA-08(26)_ODP системи або компоненти системи>** реалізують принцип безпеки продуктивності.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються принципів безпеки економіки, які використовуються в специфікації, проектуванні, розробці, впровадженні та модифікації системи; проектна документація системи; вимоги та специфікації безпеки та конфіденційності для системи; архітектура безпеки та конфіденційності системи; аналіз компромісів між продуктивністю та безпекою; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за визначення вимог до безпеки та конфіденційності системи; персонал організації, відповідальний за специфікацію, проектування, розробку, впровадження та модифікацію системи; розробники системи; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка**: [ВИБІР: Процеси організації застосування принципу безпеки економіки при специфікації, проектуванні, розробці, впровадженні та модифікації систем; механізми, що підтримують застосування принципу безпеки економіки при специфікації, проектуванні, розробці, впровадженні та модифікації систем].	

SA-8(27)	**БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - ЛЮДСЬКИЙ ФАКТОР БЕЗПЕКИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-08(27)_ODP	**визначено системи або компоненти системи, які реалізують принцип безпеки з урахуванням людського**

		фактору;
	SA-08(27)	**<SA-08(27)_ODP системи або компоненти системи>** реалізують принцип безпеки з урахуванням людського фактору.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються принципів безпеки економіки, які використовуються в специфікації, проектуванні, розробці, впровадженні та модифікації системи; проектна документація системи; вимоги та специфікації безпеки та конфіденційності для системи; архітектура безпеки та конфіденційності системи; аналіз компромісів між продуктивністю та безпекою; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за визначення вимог до безпеки та конфіденційності системи; персонал організації, відповідальний за специфікацію, проектування, розробку, впровадження та модифікацію системи; розробники системи; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка**: [ВИБІР: Процеси організації застосування принципу безпеки економіки при специфікації, проектуванні, розробці, впровадженні та модифікації систем; механізми, що підтримують застосування принципу безпеки економіки при специфікації, проектуванні, розробці, впровадженні та модифікації систем].	

SA-8(28)	**БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - ПРИЙНЯТНА БЕЗПЕКА**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-08(28)_ODP	**визначено системи або компоненти системи, які реалізують принцип прийнятного рівня безпеки;**
	SA-08(28)	**<SA-08(28)_ODP системи або компоненти системи>** реалізують принцип прийнятного рівня безпеки.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються принципів безпеки економіки, які використовуються в специфікації, проектуванні, розробці, впровадженні та модифікації системи; проектна документація системи; вимоги та специфікації безпеки та конфіденційності для системи; архітектура безпеки та конфіденційності системи; аналіз компромісів між продуктивністю та безпекою; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за визначення вимог до безпеки та конфіденційності системи; персонал організації, відповідальний за специфікацію, проектування, розробку, впровадження та модифікацію системи; розробники системи; персонал організації, відповідальний за інформаційну	

	безпеку]. **Перевірка**: [ВИБІР: Процеси організації застосування принципу безпеки економіки при специфікації, проектуванні, розробці, впровадженні та модифікації систем; механізми, що підтримують застосування принципу безпеки економіки при специфікації, проектуванні, розробці, впровадженні та модифікації систем].

SA-8(29)	**БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - ПОВТОРЮВАНІ І ДОКУМЕНТОВАНІ ПРОЦЕДУРИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-08(29)_ODP	**визначено системи або компоненти системи, які реалізують принцип повторюваних та задокументованих процедур;**
	SA-08(28)	**<SA-08(29)_ODP системи або компоненти системи>** реалізують принцип повторюваних та задокументованих процедур.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються принципів безпеки економіки, які використовуються в специфікації, проектуванні, розробці, впровадженні та модифікації системи; проектна документація системи; вимоги та специфікації безпеки та конфіденційності для системи; архітектура безпеки та конфіденційності системи; аналіз компромісів між продуктивністю та безпекою; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за визначення вимог до безпеки та конфіденційності системи; персонал організації, відповідальний за специфікацію, проектування, розробку, впровадження та модифікацію системи; розробники системи; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка**: [ВИБІР: Процеси організації застосування принципу безпеки економіки при специфікації, проектуванні, розробці, впровадженні та модифікації систем; механізми, що підтримують застосування принципу безпеки економіки при специфікації, проектуванні, розробці, впровадженні та модифікації систем].	

SA-8(30)	**БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - ПРОЦЕСУАЛЬНА СТРОГІСТЬ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-08(30)_ODP	**визначено системи або компоненти системи, які реалізують принцип проектування прийнятної безпеки;**

	SA-08(28)	**<SA-08(30)_ODP системи або компоненти системи>** реалізують принцип проектування прийнятної безпеки.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються принципів безпеки економіки, які використовуються в специфікації, проектуванні, розробці, впровадженні та модифікації системи; проектна документація системи; вимоги та специфікації безпеки та конфіденційності для системи; архітектура безпеки та конфіденційності системи; аналіз компромісів між продуктивністю та безпекою; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за визначення вимог до безпеки та конфіденційності системи; персонал організації, відповідальний за специфікацію, проектування, розробку, впровадження та модифікацію системи; розробники системи; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка**: [ВИБІР: Процеси організації застосування принципу безпеки економіки при специфікації, проектуванні, розробці, впровадженні та модифікації систем; механізми, що підтримують застосування принципу безпеки економіки при специфікації, проектуванні, розробці, впровадженні та модифікації систем].	

SA-8(31)	**БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - БЕЗПЕЧНА МОДИФІКАЦІЯ СИСТЕМИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-08(31)_ODP	**визначено системи або компоненти системи, які реалізують принцип безпечної модифікації систем;**
	SA-08(31)	**<SA-08(31)_ODP системи або компоненти системи>** реалізують принцип безпечної модифікації систем.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються принципів безпеки економіки, які використовуються в специфікації, проектуванні, розробці, впровадженні та модифікації системи; проектна документація системи; вимоги та специфікації безпеки та конфіденційності для системи; архітектура безпеки та конфіденційності системи; аналіз компромісів між продуктивністю та безпекою; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за визначення вимог до безпеки та конфіденційності системи; персонал організації, відповідальний за специфікацію, проектування, розробку, впровадження та модифікацію системи; розробники системи; персонал організації, відповідальний за інформаційну безпеку].	

	Перевірка: [ВИБІР: Процеси організації застосування принципу безпеки економіки при специфікації, проектуванні, розробці, впровадженні та модифікації систем; механізми, що підтримують застосування принципу безпеки економіки при специфікації, проектуванні, розробці, впровадженні та модифікації систем].

SA-8(32)	**БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - ДОСТАТНЄ ДОКУМЕНТУВАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-08(32)_ODP	**визначено системи або компоненти системи, які реалізують принцип достатньої допускної документації;**
	SA-08(32)	**<SA-08(32)_ODP системи або компоненти системи>** реалізують принцип достатньої допускної документації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються принципів безпеки економіки, які використовуються в специфікації, проектуванні, розробці, впровадженні та модифікації системи; проектна документація системи; вимоги та специфікації безпеки та конфіденційності для системи; архітектура безпеки та конфіденційності системи; аналіз компромісів між продуктивністю та безпекою; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за визначення вимог до безпеки та конфіденційності системи; персонал організації, відповідальний за специфікацію, проектування, розробку, впровадження та модифікацію системи; розробники системи; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка**: [ВИБІР: Процеси організації застосування принципу безпеки економіки при специфікації, проектуванні, розробці, впровадженні та модифікації систем; механізми, що підтримують застосування принципу безпеки економіки при специфікації, проектуванні, розробці, впровадженні та модифікації систем].	

SA-8(33)	**БЕЗПЕКА ТА ПРИВАТНІСТЬ ПРИНЦИПІВ ІНЖИНІРИНГУ - МІНІМІЗАЦІЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-08(33)_ODP	**визначено системи або компоненти системи, які реалізують принцип мінімізації конфіденційності;**

	SA-08(33)	**<SA-08(33)_ODP системи або компоненти системи>** реалізують принцип мінімізації конфіденційності.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання системи та послуг; процедури, що стосуються принципів безпеки економіки, які використовуються в специфікації, проектуванні, розробці, впровадженні та модифікації системи; проектна документація системи; вимоги та специфікації безпеки та конфіденційності для системи; архітектура безпеки та конфіденційності системи; аналіз компромісів між продуктивністю та безпекою; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за визначення вимог до безпеки та конфіденційності системи; персонал організації, відповідальний за специфікацію, проектування, розробку, впровадження та модифікацію системи; розробники системи; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка**: [ВИБІР: Процеси організації застосування принципу безпеки економіки при специфікації, проектуванні, розробці, впровадженні та модифікації систем; механізми, що підтримують застосування принципу безпеки економіки при специфікації, проектуванні, розробці, впровадженні та модифікації систем].	

SA-9	**ЗОВНІШНІ ПОСЛУГИ ДЛЯ СИСТЕМИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-09_ODP[01]	**визначені засоби контролю, які будуть застосовуватися зовнішніми постачальниками системних послуг;**
	SA-09_ODP[02]	**визначені процеси, методи та техніки, що застосовуються для моніторингу дотримання вимог контролю зовнішніми постачальниками послуг;**
	SA-09a.[01]	дотримуються постачальники зовнішніх системних послуг вимог організаційної безпеки;
	SA-09a.[02]	дотримуються постачальники зовнішніх системних послуг вимог приватності організації;
	SA-09a.[03]	використовують постачальники зовнішніх системних послуг **<SA-09_ODP[01] елементи керування>**;
	SA-09b.[01]	визначено та задокументовано організаційний нагляд за зовнішніми системними послугами;
	SA-09b.[02]	визначені та задокументовані ролі та обов'язки користувачів щодо зовнішніх системних сервісів;

	SA-09c.	визначені та задокументовані ролі та обов'язки користувачів щодо зовнішніх системних послуг;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються послуг зовнішньої системи; процедури, що стосуються методів та прийомів моніторингу дотримання контролю безпеки зовнішніми провайдерами послуг інформаційних систем; договори придбання, угоди про рівень послуг; організаційні вимоги до безпеки та технічні вимоги до послуг зовнішніх постачальників; докази оцінки контролю безпеки від зовнішніх постачальників послуг системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання системи та послуг; зовнішні провайдери послуг системи; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для постійного моніторингу дотримання контролю безпеки зовнішніми постачальниками послуг; автоматизовані механізми для постійного моніторингу дотримання контролю безпеки зовнішніми постачальниками послуг].	

SA-9(1)	**ЗОВНІШНІ ПОСЛУГИ ДЛЯ СИСТЕМИ- ОЦІНЮВАННЯ РИЗИКІВ ТА ОРГАНІЗАЦІЙНІ ПОГОДЖЕННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-09(01)_ODP	**визначено персонал або ролі, які схвалюють придбання або передачу спеціальних послуг з інформаційної безпеки;**
	SA-09(01)(a)	проводиться організаційна оцінка ризиків перед придбанням або передачею послуг з інформаційної безпеки;
	SA-09(01)(b)	схвалюють **<SA-09(01)_ODP персонал або ролі>** придбання або передачу спеціальних послуг з інформаційної безпеки.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються послуг зовнішньої системи; документація про придбання; договори придбання системи, компонента системи або послуги системи; звіти про оцінку ризиків; записи про затвердження для придбання або передачі на замовлення спеціальних служб захисту інформації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання системи та послуг; персонал організації, який відповідає за безпеку системи; зовнішні провайдери послуг системи; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для проведення оцінки ризиків до придбання або передачі в спеціальну службу захисту інформації; організаційні процеси для затвердження аутсорсингу спеціальних служб захисту інформації; автоматизовані механізми підтримки та, або впровадження оцінки ризику;	

	автоматизовані механізми, що підтримують та, або впроваджують процеси затвердження].

SA-9(2)	**ЗОВНІШНІ ПОСЛУГИ ДЛЯ СИСТЕМИ- ВИЗНАЧЕННЯ ФУНКЦІЙ, ПОРТІВ, ПРОТОКОЛІВ ТА СЛУЖБ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-09(02)_ODP	**визначені зовнішні системні сервіси, які потребують ідентифікації функцій, портів, протоколів та інших сервісів;**
	SA-09(02)	необхідно постачальникам **<SA-09(02)_ODP зовнішніх системних послуг>** ідентифікувати функції, порти, протоколи та інші послуги, необхідні для використання таких послуг.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються послуг зовнішньої системи; документація про придбання; договори придбання системи, компонента системи або послуги системи; звіти про оцінку ризиків; записи про затвердження для придбання або передачі на замовлення спеціальних служб захисту інформації; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання системи та послуг; персонал організації, який відповідає за безпеку системи; зовнішні провайдери послуг системи; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для проведення оцінки ризиків до придбання або передачі в спеціальну службу захисту інформації; організаційні процеси для затвердження аутсорсингу спеціальних служб захисту інформації; автоматизовані механізми підтримки та, або впровадження оцінки ризику; автоматизовані механізми, що підтримують та, або впроваджують процеси затвердження].	

SA-9(3)	**ЗОВНІШНІ ПОСЛУГИ ДЛЯ СИСТЕМИ - СТВОРЕННЯ ТА ПІДТРИМКА ДОВІРЧИХ ВІДНОСИН З ПОСТАЧАЛЬНИКАМИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-09(03)_ODP[01]	**визначені вимоги безпеки, властивості, фактори або умови, що визначають прийнятні довірчі відносини, на яких підтримуються довірчі відносини;**
	SA-09(03)_ODP[02]	**визначені вимоги до конфіденційності, властивості, фактори або умови, що визначають прийнятні довірчі відносини, на основі яких підтримуються довірчі**

		відносини;
	SA-09(03)[01]	встановлені та задокументовані довірчі відносини з зовнішніми постачальниками послуг на основі **<SA-09(03)_ODP[01] вимог, властивостей, факторів або умов безпеки>**;
	SA-09(03)[02]	підтримуються довірчі відносини з зовнішніми постачальниками послуг на основі **<SA-09(03)_ODP[01] вимог, властивостей, факторів або умов безпеки>**;
	SA-09(03)[03]	встановлені та задокументовані довірчі відносини із зовнішніми постачальниками послуг на основі **<SA-09(03)_ODP[02] вимог, властивостей, факторів або умов конфіденційності>**;
	SA-09(03)[04]	підтримуються довірчі відносини із зовнішніми постачальниками послуг на основі **<SA-09(03)_ODP[02] вимог, властивостей, факторів або умов конфіденційності>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються послуг зовнішньої системи; договори придбання системи, компонента системи або послуги системи; документація про придбання; тендерна документація; угоди про рівень обслуговування; вимоги до безпеки організації, властивості, фактори або умови, що визначають прийнятні довірчі відносини; документація довірчих відносин із зовнішніми постачальниками послуг; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання системи та послуг; персонал організації, відповідальний за інформаційну безпеку; зовнішні провайдери послуг системи].	

SA-9(4)	**ЗОВНІШНІ СИСТЕМНІ СЛУЖБИ - УЗГОДЖЕННЯ ІНТЕРЕСІВ СПОЖИВАЧІВ І ПОСТАЧАЛЬНИКІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-09(04)_ODP[01]	**визначені зовнішні постачальники послуг;**
	SA-09(04)_ODP[02]	**визначені дії, які необхідно вжити для перевірки того, що інтереси зовнішніх постачальників послуг узгоджуються з інтересами організації та відображають їх;**
	SA-09(04)	вживаються **<SA-09(04)_ODP[02] дії>** для перевірки того, що інтереси **<SA-09(04)_ODP[01] зовнішніх постачальників послуг>** узгоджуються з інтересами організації та

		відображають їх.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються послуг зовнішньої системи; договори придбання системи, компонента системи або послуги системи; заявна документація; документація про придбання; угоди про рівень обслуговування; організаційні вимоги, гарантії безпеки для зовнішніх постачальників послуг; політика кадрової безпеки для зовнішніх постачальників послуг; оцінки, проведені зовнішніми постачальниками послуг; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання системи та послуг; персонал організації, який відповідає за інформаційну безпеку; зовнішні провайдери послуг системи]. **Перевірка:** [ВИБІР: Процеси організації для визначення та використання гарантій для забезпечення узгоджених інтересів із зовнішніми постачальниками послуг; автоматизовані механізми, що підтримують та, або впроваджують гарантії для забезпечення узгоджених інтересів із зовнішніми постачальниками послуг].	

SA-9(5)	**ЗОВНІШНІ ПОСЛУГИ ДЛЯ СИСТЕМИ- МІСЦЕ ОБРОБКИ, ЗБЕРІГАННЯ ТА ОБСЛУГОВУВАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-09(05)_ODP[01]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {обробка інформації; інформація або дані; системні послуги};**
	SA-09(05)_ODP[02]	**визначено місця, де <SA-09(05)_ODP[01] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(S)> є/мають бути обмежені;**
	SA-09(05)_ODP[03]	**визначено вимоги або умови для обмеження розташування <SA-09(05)_ODP[01] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>;**
	SA-09(05)	на основі вимог **<SA-09(05)_ODP[03]>, <SA-09(05)_ODP[01] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** обмежене(і) **<SA-09(05)_ODP[02] місцезнаходженнями>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються послуг зовнішньої системи; договори придбання системи, компонента системи або послуги системи; заявна документація; документація про придбання; угоди про рівень обслуговування; обмежені місця для обробки інформації; інформація, дані та, або послуги системи; обробка інформації, інформація, дані та, або послуги системи, які будуть підтримуватися в обмежених місцях; вимоги або умови організаційної безпеки для зовнішніх	

	постачальників; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання системи та послуг; персонал організації, який відповідає за інформаційну безпеку; зовнішні провайдери послуг системи]. **Перевірка:** [ВИБІР: Процеси організації для визначення вимог щодо обмеження місць обробки інформації, інформації, даних або інформаційних служб; організаційні процеси для забезпечення розташування обмежені відповідно до вимог чи умов].

SA-9(6)	**ЗОВНІШНІ ПОСЛУГИ ДЛЯ СИСТЕМИ- КРИПТОГРАФІЧНІ КЛЮЧІ, КЕРОВАНІ ОРГАНІЗАЦІЄЮ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-09(06)	зберігається ексклюзивний контроль над криптографічними ключами для зашифрованих матеріалів, що зберігаються або передаються через зовнішню систему.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються послуг зовнішньої системи; договори придбання системи, компонента системи або послуги системи; заявна документація; документація про придбання; угоди про рівень обслуговування; обмежені місця для обробки інформації; інформація, дані та, або послуги системи; обробка інформації, інформація, дані та, або послуги системи, які будуть підтримуватися в обмежених місцях; вимоги або умови організаційної безпеки для зовнішніх постачальників; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання системи та послуг; персонал організації, який відповідає за інформаційну безпеку; зовнішні провайдери послуг системи]. **Перевірка:** [ВИБІР: Процеси організації для визначення вимог щодо обмеження місць обробки інформації, інформації, даних або інформаційних служб; організаційні процеси для забезпечення розташування обмежені відповідно до вимог чи умов].	

SA-9(7)	**ЗОВНІШНІ ПОСЛУГИ ДЛЯ СИСТЕМИ- ПЕРЕВІРКА ЦІЛІСНОСТІ, ЩО КОНТРОЛЮЄТЬСЯ ОРГАНІЗАЦІЄЮ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-09(07)	передбачена можливість перевірки цілісності інформації під час її перебування у зовнішній системі.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика придбання систем та послуг; процедури, що	

	стосуються послуг зовнішньої системи; договори придбання системи, компонента системи або послуги системи; заявна документація; документація про придбання; угоди про рівень обслуговування; обмежені місця для обробки інформації; інформація, дані та, або послуги системи; обробка інформації, інформація, дані та, або послуги системи, які будуть підтримуватися в обмежених місцях; вимоги або умови організаційної безпеки для зовнішніх постачальників; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання системи та послуг; персонал організації, який відповідає за інформаційну безпеку; зовнішні провайдери послуг системи]. **Перевірка:** [ВИБІР: Процеси організації для визначення вимог щодо обмеження місць обробки інформації, інформації, даних або інформаційних служб; організаційні процеси для забезпечення розташування обмежені відповідно до вимог чи умов].

SA-9(8)	**ЗОВНІШНІ ПОСЛУГИ ДЛЯ СИСТЕМИ- МІСЦЕ ОБРОБКИ ТА ЗБЕРІГАННЯ – ЮРИСДИКЦІЯ УКРАЇНИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-09(08)	обмежується географічне розміщення обробки інформації та зберігання даних об'єктами, розташованими в межах юридичної юрисдикції України
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання систем та послуг; процедури придбання систем та послуг; процедури, що стосуються зовнішніх системних послуг; контракти на придбання системи, системного компонента або системної послуги; документація щодо подання пропозицій; документація щодо придбання; угоди про рівень обслуговування; процедури, що стосуються визначення обмежень юрисдикції для обробки та місця зберігання; інформація/дані та/або системні послуги; вимоги або умови організаційної безпеки для зовнішніх постачальників; план захисту інформації системи; план управління ризиками ланцюга постачання; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за придбання систем та послуг; персонал організації, відповідальний за інформаційну безпеку; персонал організації, відповідальний за управління ризиками ланцюга постачання; зовнішні постачальники системних послуг]. **Перевірка**: [ВИБІР: Процеси організації, що обмежують зовнішніх постачальників системних послуг обробляти та зберігати інформацію в межах юридичної юрисдикції України].	

SA-10	**УПРАВЛІННЯ КОНФІГУРАЦІЄЮ РОЗРОБНИКА**
	МЕТА ОЦІНКИ: Визначити, чи:

	SA-10_ODP[01]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {дизайн; розробка; впровадження; експлуатація; утилізація};**
	SA-10_ODP[02]	**визначено елементи конфігурації під керуванням;**
	SA-10_ODP[03]	**визначено персонал, якому повідомляється про недоліки безпеки та способи їх усунення в системі, компонента або служби;**
	SA-10a.	повинен розробник системи, системного компонента або системної служби виконувати керування конфігурацією під час роботи системи, компонента або служби **<SA-10_ODP[01] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>**;
	SA-10b.[01]	повинен розробник системи, системного компонента або системної служби документувати цілісність змін до **<SA-10_ODP[02] елементів конфігурації>**;
	SA-10b.[02]	повинен розробник системи, системного компонента або системної служби керувати цілісністю змін до **<SA-10_ODP[02] елементів конфігурації>**;
	SA-10b.[03]	повинен розробник системи, системного компонента або системної служби контролювати цілісність змін до **<SA-10_ODP[02] елементів конфігурації>**;
	SA-10c.	зобов'язаний розробник системи, компонента системи або системної послуги впроваджувати лише затверджені організацією зміни до системи, компонента або послуги;
	SA-10d.[01]	зобов'язаний розробник системи, компонента системи або системної послуги документувати затверджені зміни до системи, компонента або послуги;
	SA-10d.[02]	зобов'язаний розробник системи, системного компонента або системної служби документувати потенційний вплив затверджених змін на безпеку;
	SA-10d.[03]	зобов'язаний розробник системи, системного компонента або системної служби документувати потенційний вплив затверджених змін на конфіденційність;
	SA-10e.[01]	зобов'язаний розробник системи, системного компонента або системного сервісу відстежувати недоліки безпеки в системі, компоненті або сервісі;
	SA-10e.[02]	зобов'язаний розробник системи, системного компонента або системної служби відстежувати усунення вразливостей безпеки в системі, компоненті або службі;
	SA-10e.[03]	повинен розробник системи, системного компонента або системної служби повідомляти про результати перевірки **<SA-10_ODP[03] персоналу>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження: [**ВИБІР: Політика придбання систем та послуг; процедури, що стосуються управління конфігурацією розробника системи; тендерна	

	документація; документація про придбання; угоди про рівень обслуговування; договори придбання системи; системний компонент, або послуга системи; план управління конфігурацією розробника системи; змінити записи контролю; записи управління конфігурацією; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання системи та послуг; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який відповідає за управління конфігурацією; розробники системи]. **Перевірка:** [ВИБІР: Процеси організації для моніторингу управління конфігурацією розробника; автоматизовані механізми, що підтримують та, або впроваджують моніторинг управління конфігурацією розробника].

SA-10(1)	**УПРАВЛІННЯ КОНФІГУРАЦІЄЮ РОЗРОБНИКА - ПЕРЕВІРКА ЦІЛІСНОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА МІКРОПРОГРАМ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-10(01)	зобов'язаний розробник системи, системного компонента або системного служби забезпечити перевірку цілісності програмного забезпечення та компонентів програмного забезпечення.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження: [**ВИБІР: Політика придбання систем та послуг; процедури, що стосуються управління конфігурацією розробника системи; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання системи; системний компонент, або послуга системи; план управління конфігурацією розробника системи; змінити записи контролю; записи управління конфігурацією; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання системи та послуг; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який відповідає за управління конфігурацією; розробники системи]. **Перевірка:** [ВИБІР: Процеси організації для моніторингу управління конфігурацією розробника; автоматизовані механізми, що підтримують та, або впроваджують моніторинг управління конфігурацією розробника].	

SA-10(2)	**УПРАВЛІННЯ КОНФІГУРАЦІЄЮ РОЗРОБНИКА - АЛЬТЕРНАТИВНІ ПРОЦЕСИ КЕРУВАННЯ КОНФІГУРАЦІЄЮ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-10(02)	було передбачено альтернативний процес керування конфігурацією за допомогою організаційного персоналу за відсутності спеціалізованої команди керування конфігурацією

		розробників..
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження: [**ВИБІР: Політика придбання систем та послуг; процедури, що стосуються управління конфігурацією розробника системи; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання системи; системний компонент, або послуга системи; план управління конфігурацією розробника системи; змінити записи контролю; записи управління конфігурацією; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання системи та послуг; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який відповідає за управління конфігурацією; розробники системи]. **Перевірка:** [ВИБІР: Процеси організації для моніторингу управління конфігурацією розробника; автоматизовані механізми, що підтримують та, або впроваджують моніторинг управління конфігурацією розробника].	

SA-10(3)	**УПРАВЛІННЯ КОНФІГУРАЦІЄЮ РОЗРОБНИКА - ПЕРЕВІРКА ЦІЛІСНОСТІ АПАРАТНИХ ЗАСОБІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-10(03)	зобов'язаний розробник системи, системного компонента або системної служби уможливити перевірку цілісності апаратних компонентів.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються управління конфігурацією розробника системи; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання системи; системний компонент, або послуга системи; план управління конфігурацією розробника системи; змінити записи контролю; записи управління конфігурацією; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання системи та послуг; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який відповідає за управління конфігурацією; розробники системи]. **Перевірка:** [ВИБІР: Процеси організації для моніторингу управління конфігурацією розробника; автоматизовані механізми, що підтримують та, або впроваджують моніторинг управління конфігурацією розробника].	

SA-10(4)	**УПРАВЛІННЯ КОНФІГУРАЦІЄЮ РОЗРОБНИКА - ДОВІРЧЕ ГЕНЕРУВАННЯ**
	МЕТА ОЦІНКИ: Визначити, чи:

	SA-10(04)	зобов'язаний розробник системи, системного компонента або системної служби уможливити перевірку цілісності апаратних компонентів.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються управління конфігурацією розробника системи; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання системи; системний компонент, або послуга системи; план управління конфігурацією розробника системи; змінити записи контролю; записи управління конфігурацією; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання системи та послуг; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який відповідає за управління конфігурацією; розробники системи]. **Перевірка:** [ВИБІР: Процеси організації для моніторингу управління конфігурацією розробника; автоматизовані механізми, що підтримують та, або впроваджують моніторинг управління конфігурацією розробника].	

SA-10(4)	**УПРАВЛІННЯ КОНФІГУРАЦІЄЮ РОЗРОБНИКА - ДОВІРЧЕ ГЕНЕРУВАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-10(04)[01]	повинен розробник системи, системного компонента або системної служби використовувати інструменти для порівняння новостворених версій описів апаратного забезпечення, що мають відношення до безпеки, з попередніми версіями;
	SA-10(04)[02]	зобов'язаний розробник системи, системного компонента або системної служби використовувати інструменти для порівняння новостворених версій вихідного коду з попередніми версіями;
	SA-10(04)[03]	зобов'язаний розробник системи, системного компонента або системного сервісу використовувати інструменти для порівняння новостворених версій об'єктного коду з попередніми версіями.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються управління конфігурацією розробника системи; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання системи; системний компонент, або послуга системи; план управління конфігурацією розробника системи; змінити записи контролю; записи управління конфігурацією; інші відповідні документи або записи]. **Перевірка:** [ВИБІР: Процеси організації для моніторингу управління конфігурацією розробника; автоматизовані механізми, що підтримують та, або	

	впроваджують моніторинг управління конфігурацією розробника].

SA-10(5)	**УПРАВЛІННЯ КОНФІГУРАЦІЄЮ РОЗРОБНИКА - ВІДОБРАЖЕННЯ ЦІЛІСНОСТІ ДЛЯ КЕРУВАННЯ ВЕРСІЯМИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-10(05)	повинен 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.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження: [**ВИБІР: Політика придбання систем та послуг; процедури, що стосуються управління конфігурацією розробника системи; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання системи; системний компонент, або послуга системи; план управління конфігурацією розробника системи; змінити записи контролю; записи управління конфігурацією; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання системи та послуг; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який відповідає за управління конфігурацією; розробники системи]. **Перевірка:** [ВИБІР: Процеси організації для моніторингу управління конфігурацією розробника; автоматизовані механізми, що підтримують та, або впроваджують моніторинг управління конфігурацією розробника].	

SA-10(6)	**УПРАВЛІННЯ КОНФІГУРАЦІЄЮ РОЗРОБНИКА - ДОВІРЕНЕ ПОСТАЧАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-10(06)	повинен розробник 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.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження: [**ВИБІР: Політика придбання систем та послуг; процедури, що стосуються управління конфігурацією розробника системи; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання системи; системний компонент, або послуга системи; план управління конфігурацією розробника системи; змінити записи контролю; записи	

	управління конфігурацією; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання системи та послуг; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який відповідає за управління конфігурацією; розробники системи]. **Перевірка:** [ВИБІР: Процеси організації для моніторингу управління конфігурацією розробника; автоматизовані механізми, що підтримують та, або впроваджують моніторинг управління конфігурацією розробника].

SA-10(7)	**УПРАВЛІННЯ КОНФІГУРАЦІЄЮ РОЗРОБНИКА - ПРЕДСТАВНИКИ БЕЗПЕКИ ТА ПРИВАТНОСТІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-10(07)_ODP[01]	**визначаються представники безпеки, які повинні бути включені в процес управління змінами конфігурації та контролю;**
	SA-10(07)_ODP[02]	**визначено представників приватності, які будуть включені в процес управління змінами конфігурації та контролю;**
	SA-10(07)_ODP[03]	**визначено процеси управління змінами конфігурації та контролю, до яких обов'язково мають бути включені представники служби безпеки;**
	SA-10(07)_ODP[04]	**визначено процеси управління змінами конфігурації та контролю, до яких обов'язково мають бути включені представники з питань приватності;**
	SA-10(07)[01]	визначити **<SA-10(07)_ODP[01] представників безпеки>**, які мають бути включені до **<SA-10(07)_ODP[03] процесів управління та контролю змін конфігурації>**;
	SA-10(07)[02]	визначити **<SA-10(07)_ODP[02] представників приватності>**, які мають бути включені до **<SA-10(07)_ODP[04] процесів управління та контролю змін конфігурації>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються управління конфігурацією розробника системи; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання системи; системний компонент, або послуга системи; план управління конфігурацією розробника системи; змінити записи контролю; записи управління конфігурацією; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, який відповідає за придбання системи та послуг; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який відповідає за управління конфігурацією; розробники системи].	

	Перевірка: [ВИБІР: Процеси організації для моніторингу управління конфігурацією розробника; автоматизовані механізми, що підтримують та, або впроваджують моніторинг управління конфігурацією розробника].

SA-11	**УПРАВЛІННЯ КОНФІГУРАЦІЄЮ РОЗРОБНИКА - ПРЕДСТАВНИКИ БЕЗПЕКИ ТА ПРИВАТНОСТІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-11_ODP[01]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {одиниця; інтеграція; система; регресія};**
	SA-11_ODP[02]	**визначено частоту, з якою слід проводити <SA-11_ODP[01] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(S)> тестування/оцінювання;**
	SA-11_ODP[03]	**визначено глибину та охоплення <SA-11_ODP[01] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(S)> тестування/оцінювання;**
	SA-11a.[01]	зобов'язаний розробник системи, системного компонента або системної служби на всіх етапах життєвого циклу розробки системи після проектування розробляти план постійних оцінок безпеки;
	SA-11a.[02]	зобов'язаний розробник системи, системного компонента або системної служби на всіх етапах життєвого циклу розробки системи після проектування впроваджувати план постійних оцінок безпеки;
	SA-11a.[03]	зобов'язаний розробник системи, системного компонента або системної служби на всіх післяпроектних етапах життєвого циклу розробки системи розробляти план оцінки приватності;
	SA-11a.[04]	зобов'язаний розробник системи, системного компонента або системної служби на всіх етапах життєвого циклу розробки системи після проектування впроваджувати план постійних оцінок конфіденційності;
	SA-11b.	повинен розробник системи, системного компонента або системної служби на всіх післяпроектних етапах життєвого циклу розробки системи виконувати **<SA-11_ODP[01] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** тестування/оцінювання **<SA-11_ODP[02] частота проведення>** з **<SA-11_ODP[03] глибиною та охопленням>**;
	SA-11c.[01]	повинен розробник системи, системного компонента або системної служби на всіх післяпроектних етапах життєвого циклу розробки системи надавати докази виконання плану оцінювання;
	SA-11c.[02]	потрібен розробник системи, системного компонента або системної служби на всіх післяпроектних етапах життєвого циклу розробки системи для надання результатів тестування

		та оцінки;
	SA-11d.	зобов'язаний розробник системи, системного компонента або системної служби на всіх етапах життєвого циклу розробки системи після проектування впроваджувати процес усунення дефектів, що піддається перевірці;
	SA-11e.	потрібен розробник системи, системного компонента або системної служби на всіх післяпроектних етапах життєвого циклу розробки системи для виправлення недоліків, виявлених під час тестування та оцінки.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються тестування безпеки розробника системи; процедури, що стосуються усунення недоліків; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання системи, компонента системи або послуги системи; плани тестування безпеки розробника системи; записи результатів тестування безпеки розробника для системи, компонента системи або служби системи; записи про виявлення недоліків безпеки та усунення несправностей; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання системи та послуг; персонал організації, який відповідає за інформаційну безпеку; персонал організації, відповідальний за тестування безпеки розробника; розробники системи]. **Перевірка:** [ВИБІР: Процеси організації для моніторингу тестування та оцінки безпеки розробника; автоматизовані механізми, що підтримують та, або впроваджують моніторинг тестування та оцінки безпеки розробника].		

SA-11(1)	**ТЕСТУВАННЯ ТА ОЦІНЮВАННЯ РОЗРОБНИКА - АНАЛІЗ СТАТИЧНОГО КОДУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-11(01)[01]	повинен розробник системи, системного компонента або системного служби використовувати інструменти статичного аналізу коду для виявлення поширених помилок;
	SA-11(01)[02]	зобов'язаний розробник системи, системного компонента або системного служби використовувати інструменти статичного аналізу коду для документування результатів аналізу.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються тестування безпеки розробника системи; процедури, що стосуються усунення недоліків; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання системи, компонента системи або послуги системи; плани тестування безпеки розробника системи; результати тестування безпеки розробника системи; записи про виявлення недоліків безпеки	

	та усунення несправностей; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання систем та послуг; персонал організації, який відповідає за інформаційну безпеку; персонал організації, відповідальний за тестування безпеки розробника; персонал організації, який відповідає за управління конфігурацією; розробники системи]. **Перевірка:** [ВИБІР: Процеси організації для моніторингу тестування та оцінки безпеки розробника; автоматизовані механізми, що підтримують та, або впроваджують моніторинг тестування та оцінки безпеки розробника; засоби аналізу статичного коду].

SA-11(2)	**ТЕСТУВАННЯ ТА ОЦІНЮВАННЯ РОЗРОБНИКА - МОДЕЛЮВАННЯ ЗАГРОЗ ТА АНАЛІЗ ВРАЗЛИВОСТЕЙ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-11(02)_ODP[01]	**визначена інформація про вплив вразливостей, середовище проведення операцій, відомі або передбачувані загрози та прийнятні рівні ризику, яку слід використовувати як контекстну інформацію для моделювання загроз та аналізу вразливостей;**
	SA-11(02)_ODP[02]	**визначені інструменти та методи, які будуть використовуватися для моделювання загроз та аналізу вразливостей;**
	SA-11(02)_ODP[03]	**визначено широту та глибину моделювання загроз, яке буде проводитися;**
	SA-11(02)_ODP[04]	**визначено широту та глибину аналізу вразливостей, який необхідно провести;**
	SA-11(02)_ODP[05]	**визначені критерії прийнятності, яким мають відповідати отримані докази для моделювання загроз;**
	SA-11(02)_ODP[06]	**визначені критерії прийнятності, яким мають відповідати надані докази для аналізу вразливості;**
	SA-11(02)(a)[01]	повинен розробник системи, компонента системи або системного сервісу виконувати моделювання загроз під час розробки системи, компонента або сервісу, що використовує **<SA-11(02)_ODP[01]_інформацію>**;
	SA-11(02)(a)[02]	повинен розробник системи, системного компонента або системної служби виконувати аналіз вразливостей під час розробки системи, компонента або служби, які використовують **<SA-11(02)_ODP[01]_інформацію>**;
	SA-11(02)(a)[03]	повинен розробник системи, компонента системи або системного сервісу виконувати моделювання загроз під час подальшого тестування та оцінювання системи, компонента або сервісу, що використовує **<SA-**

		11(02)_ODP[01]_інформацію>;
	SA-11(02)(a)[04]	повинен розробник системи, системного компонента або системного сервісу виконувати аналіз вразливостей під час подальшого тестування та оцінювання системи, компонента або сервісу, що використовує **<SA-11(02)_ODP[01]_інформацію>**;
	SA-11(02)(b)[01]	повинен розробник системи, компонента системи або системного сервісу виконувати моделювання загроз під час розробки системи, компонента або сервісу, що використовує **<SA-11(02)_ODP[02] засоби та методи>**;
	SA-11(02)(b)[02]	повинен розробник системи, компонента системи або системного сервісу виконувати моделювання загроз під час подальшого тестування та оцінювання системи, компонента або сервісу, що використовує **<SA-11(02)_ODP[02] інструменти та методи>**;
	SA-11(02)(b)[03]	повинен розробник системи, компонента системи або системної служби виконувати аналіз вразливостей під час розробки системи, компонента або служби, яка використовує **<SA-11(02)_ODP[02] інструменти та методи>**;
	SA-11(02)(b)[04]	повинен розробник системи, системного компонента або системного сервісу виконувати аналіз вразливостей під час подальшого тестування та оцінювання системи, компонента або сервісу, що використовує **<SA-11(02)_ODP[02] інструменти та методи>**;
	SA-11(02)(c)[01]	повинен розробник системи, системного компонента або системної служби виконувати моделювання загроз на **<SA-11(02)_ODP[03] широті та глибині>** під час розробки системи, компонента або сервісу;
	SA-11(02)(c)[02]	зобов'язаний розробник системи, компонента системи або системної служби виконувати аналіз вразливостей під час подальшого тестування та оцінювання системи, компонента або сервісу, який проводить моделювання та аналіз на **<SA-11(02)_ODP[04] ширину та глибину>**;
	SA-11(02)(d)[01]	повинен розробник системи, компонента системи або системної служби виконувати моделювання загроз під час розробки системи, компонента або сервісу, що дає змогу отримати докази, які відповідають **<SA-11(02)_ODP[05] критеріям прийнятності>**;
	SA-11(02)(d)[02]	повинен розробник системи, компонента системи або системної служби виконувати моделювання загроз під час подальшого тестування та оцінювання системи, компонента або сервісу, що дає змогу отримати докази, які відповідають критеріям прийнятності **<SA-11(02)_ODP[05]>**;
	SA-11(02)(d)[03]	повинен розробник системи, системного компонента або системної служби виконувати аналіз вразливостей під час розробки системи, компонента або служби, який надає докази,

		що відповідають **<SA-11(02)_ODP[06] критеріям прийнятності>**;
	SA-11(02)(d)[04]	повинен розробник системи, системного компонента або системної служби виконувати аналіз вразливостей під час подальшого тестування та оцінювання системи, компонента або сервісу, який надає докази, що відповідають **<SA-11(02)_ODP[06] критеріям прийнятності>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються тестування безпеки розробника системи; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання системи, компонента системи або послуги системи; звіти про незалежну перевірку та валідацію; плани тестування та оцінки безпеки; результати перевірки та оцінки безпеки системи, компонента системи або служби системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання системи та послуг; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який відповідає за тестування безпеки розробника; розробники системи; незалежний агент верифікації]. **Перевірка:** [ВИБІР: Процеси організації для моніторингу тестування та оцінки безпеки розробника; автоматизовані механізми, що підтримують та, або впроваджують моніторинг тестування та оцінки безпеки розробника].	

SA-11(3)	**ТЕСТУВАННЯ ТА ОЦІНЮВАННЯ РОЗРОБНИКА - НЕЗАЛЕЖНА ПЕРЕВІРКА ПЛАНІВ ОЦІНЮВАННЯ ТА ДОКАЗІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-11(03)_ODP	**визначені критерії незалежності, яким повинен відповідати незалежний агент;**
	SA-11(03)(a)[01]	потрібен незалежний агент, який відповідатиме **<SA-11(03)_ODP критеріям незалежності>** для перевірки правильності виконання плану оцінки безпеки розробника та доказів, отриманих під час тестування та оцінки;
	SA-11(03)(a)[02]	потрібен незалежний агент, який відповідатиме **<SA-11(03)_ODP критеріям незалежності>** для перевірки правильності виконання плану оцінювання конфіденційності розробника та доказів, отриманих під час тестування та оцінювання;
	SA-11(03)(b)	надано незалежному агенту достатньо інформації для завершення процесу перевірки, чи надано йому повноваження для отримання такої інформації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються тестування безпеки розробника системи; тендерна документація;	

	документація про придбання; угоди про рівень обслуговування; договори придбання системи, компонента системи або послуги системи; звіти про незалежну перевірку та валідацію; плани тестування та оцінки безпеки; результати перевірки та оцінки безпеки системи, компонента системи або служби системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання системи та послуг; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який відповідає за тестування безпеки розробника; розробники системи; незалежний агент верифікації]. **Перевірка:** [ВИБІР: Процеси організації для моніторингу тестування та оцінки безпеки розробника; автоматизовані механізми, що підтримують та, або впроваджують моніторинг тестування та оцінки безпеки розробника].

SA-11(4)	**ТЕСТУВАННЯ ТА ОЦІНЮВАННЯ РОЗРОБНИКА - РУЧНИЙ АНАЛІЗ КОДІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-11(04)_ODP[01]	**визначено конкретний код, який потребує ручного перегляду;**
	SA-11(04)_ODP[02]	**визначені процеси, процедури та/або методи, що використовуються для ручного перегляду коду;**
	SA-11(04)	повинен розробник системи, системного компонента або системної служби виконувати ручну перевірку коду **<SA-11(04)_ODP[01] специфічного коду>** з використанням **<SA-11(04)_ODP[02] процесів, процедур та/або методів>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються тестування безпеки розробника системи; процеси, процедури та, або техніки виконання ручного аналізу коду; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання системи, компонента системи або послуги системи; плани тестування та оцінки безпеки розробника системи; результати тестування та оцінки безпеки розробника системи; список коду, що вимагає перевірки вручну; записи ручного перегляду коду; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання системи та послуг; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який відповідає за тестування безпеки розробника; розробники системи; незалежний агент верифікації]. **Перевірка:** [ВИБІР: Процеси організації для моніторингу тестування та оцінки безпеки розробника; автоматизовані механізми, що підтримують та, або впроваджують моніторинг тестування та оцінки безпеки розробника].	

SA-11(5)	ТЕСТУВАННЯ ТА ОЦІНЮВАННЯ РОЗРОБНИКА - ТЕСТУВАННЯ НА ПРОНИКНЕННЯ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-11(05)_ODP[01]	**визначена широту тестування на проникнення;**
	SA-11(05)_ODP[02]	**изначено глибину тестування на проникнення;**
	SA-11(05)_ODP[03]	**constraints of penetration testing are defined;**
	SA-11(05)(a)[01]	зобов'язаний розробник системи, системного компонента або системної служби виконувати тестування на проникнення на наступному рівні суворості: <**SA-11(05)_ODP[01] ширина>**;
	SA-11(05)(a)[02]	зобов'язаний розробник системи, системного компонента або системної служби виконувати тестування на проникнення на наступному рівні суворості: **<SA-11(05)_ODP[02] глибина>**;
	SA-11(05)(b)	зобов'язаний розробник системи, системного компонента або системної служби проводити тестування на проникнення в умовах **<SA-11(05)_ODP[03]_обмежень>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються тестування безпеки розробника системи; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання системи, компонента системи або послуги системи; плани тестування та оцінки проникнення розробника системи; результати тестування та оцінки проникнення розробника системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання систем та послуг; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який відповідає за тестування безпеки розробника; розробники системи; незалежний агент верифікації]. **Перевірка:** [ВИБІР: Процеси організації для моніторингу тестування та оцінки безпеки розробника; автоматизовані механізми, що підтримують та, або впроваджують моніторинг тестування та оцінки безпеки розробника].	

SA-11(6)	ТЕСТУВАННЯ ТА ОЦІНЮВАННЯ РОЗРОБНИКА - АНАЛІЗ ПОВЕРХНІ АТАКИ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-11(06)	повинен розробник системи, системного компонента або системної служби виконувати аналіз вразливостей.

	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються тестування безпеки розробника системи; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання системи, компонента системи або послуги системи; плани тестування та оцінки безпеки розробника системи; результати тестування та оцінки безпеки розробника системи; записи поверхневих оглядів атаки; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання системи та послуг; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який відповідає за тестування безпеки розробника; персонал організації, який відповідає за управління конфігурацією; розробники системи]. **Перевірка:** [ВИБІР: Процеси організації для моніторингу тестування та оцінки безпеки розробника; автоматизовані механізми, що підтримують та, або впроваджують моніторинг тестування та оцінки безпеки розробника].

SA-11(7)	**ТЕСТУВАННЯ ТА ОЦІНЮВАННЯ РОЗРОБНИКА - ПЕРЕВІРКА ОБСЯГУ ТЕСТУВАННЯ ТА ОЦІНЮВАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-11(07)_ODP[01]	**визначена широта тестування та оцінки необхідних засобів контролю;**
	SA-11(07)_ODP[02]	**визначена глибина тестування та оцінки необхідних засобів контролю;**
	SA-11(07)[01]	повинен розробник системи, системного компонента або системної служби перевіряти, що обсяг тестування та оцінювання забезпечує повне покриття необхідних засобів контролю на **<SA-11(07)_ODP[01] ширину>**;
	SA-11(07)[02]	повинен розробник системи, системного компонента або системної служби перевіряти, що обсяг тестування та оцінювання забезпечує повне покриття необхідних засобів контролю на **<SA-11(07)_ODP[02] глибину>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються тестування безпеки розробника системи; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання системи, компонента системи або послуги системи; плани тестування та оцінки безпеки розробника системи; результати тестування та оцінки безпеки розробника системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання систем та послуг; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який відповідає за тестування безпеки розробника;	

	розробники системи; незалежний агент верифікації]. **Перевірка:** [ВИБІР: Процеси організації для моніторингу тестування та оцінки безпеки розробника; автоматизовані механізми, що підтримують та, або впроваджують моніторинг тестування та оцінки безпеки розробника].

SA-11(8)	**ТЕСТУВАННЯ ТА ОЦІНЮВАННЯ РОЗРОБНИКА - ДИНАМІЧНИЙ АНАЛІЗ КОДУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-11(08)[01]	повинен розробник системи, системного компонента або системної служби використовувати інструменти динамічного аналізу коду для виявлення недоліків помилок;
	SA-11(08)[02]	зобов'язаний розробник системи, системного компонента або системної служби документувати результати аналізу.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються тестування безпеки розробника системи; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання системи, компонента системи або послуги системи; плани тестування та оцінки безпеки розробника системи; результати тестування та оцінки безпеки розробника системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання систем та послуг; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який відповідає за тестування безпеки розробника; розробники системи; незалежний агент верифікації]. **Перевірка:** [ВИБІР: Процеси організації для моніторингу тестування та оцінки безпеки розробника; автоматизовані механізми, що підтримують та, або впроваджують моніторинг тестування та оцінки безпеки розробника].	

SA-11(9)	**ТЕСТУВАННЯ ТА ОЦІНЮВАННЯ РОЗРОБНИКА - ІНТЕРАКТИВНЕ ТЕСТУВАННЯ БЕЗПЕКИ ДОДАТКІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-11(09)[01]	повинен розробник системи, системного компонента або системної служби використовувати інтерактивні інструменти тестування безпеки додатків для виявлення недоліків;
	SA-11(09)[02]	зобов'язаний розробник системи, системного компонента або системної послуги документувати результати ідентифікації дефектів.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання систем та послуг; процедури тестування безпеки розробника системи; процедури тестування безпеки	

	інтерактивних додатків; тендерна документація; документація щодо придбання; угоди про рівень обслуговування; контракти на придбання системи, системного компонента або системної послуги; плани тестування та оцінки безпеки розробника системи; результати тестування та оцінки безпеки; звіти про відстеження недоліків безпеки та їх усунення; план забезпечення безпеки системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за придбання систем та послуг; персонал організації, відповідальний за інформаційну безпеку; персонал організації, відповідальний за тестування безпеки розробників; персонал організації, відповідальний за управління конфігурацією; розробники системи]. **Перевірка**: [ВИБІР: Процеси організації для інтерактивного тестування безпеки додатків; механізми підтримки та/або реалізації інтерактивного тестування безпеки додатків].

SA-12	**КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ**
	[Вилучено: включено до SR].

SA-12(1)	**КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - СТРАТЕГІЇ, ІНСТРУМЕНТИ ТА МЕТОДИ ЗАКУПІВЕЛЬ**
	[Вилучено: включено до SR-5].

SA-12(2)	**КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - АНАЛІЗ ПОСТАЧАЛЬНИКІВ**
	[Вилучено: включено до SR-6].

SA-12(3)	**КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - НАДІЙНЕ ПЕРЕВЕЗЕННЯ ТА ЗБЕРІГАННЯ**
	[Вилучено: включено до SR-3].

SA-12(4)	**КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - ДИВЕРСИФІКАЦІЯ ПОСТАЧАЛЬНИКІВ**
	[Вилучено: включено до SR-3 (1)].

SA-12(5)	**КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - ОБМЕЖЕННЯ ШКОДИ**
	[Вилучено: включено до SR-3 (2)].

SA-12(6)	**КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - МІНІМІЗАЦІЯ ЧАСУ ЗАКУПІВЕЛЬ**
	[Вилучено: включено до SR-5 (1)].

SA-12(7)	**КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - ОЦІНЮВАННЯ ПЕРЕД ВИБОРОМ, ПРИЙНЯТТЯМ ТА ОНОВЛЕННЯМ**
	[Вилучено: включено до SR-5 (2)].

SA-12(8)	**КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - ВИКОРИСТАННЯ ВСЕБІЧНОЇ РОЗВІДУВАЛЬНОЇ ІНФОРМАЦІЇ**
	[Вилучено: включено до SR-3 (2)].

SA-12(9)	**КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - ОПЕРАЦІЙНА БЕЗПЕКА**
	[Вилучено: включено до SR-7].

SA-12(10)	**КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - ПЕРЕВІРКА НА СПРАВЖНІСТЬ І НЕЗМІНЕНІСТЬ**
	[Вилучено: включено до SR-4 (3)].

SA-12(11)	**КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - ПЕРЕВІРКА НА СПРАВЖНІСТЬ І НЕЗМІНЕНІСТЬ**
	[Вилучено: включено до SR-6 (1)].

SA-12(12)	**КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - УГОДИ ПРО ПОВІДОМЛЕННЯ**
	[Вилучено: включено до SR-8].

SA-12(13)	**КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - КОМПОНЕНТИ КРИТИЧНИХ СИСТЕМ**
	[Вилучено: включено до MA-6 та RA-9].

SA-12(14)	**КЕРУВАННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ - ІДЕНТИЧНІСТЬ ТА ПРОСТЕЖУВАНІСТЬ**
	[Вилучено: включено до SR-4 (1) та SR-4(2)].

SA-12(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].

SA-14(1)	**КРИТИЧНІ КОМПОНЕНТИ БЕЗ ЖИТТЄЗДАТНИХ АЛЬТЕРНАТИВНИХ ДЖЕРЕЛ**
	[Вилучено: включено до SA-20].

SA-15	**ПРОЦЕСИ, СТАНДАРТИ ТА ІНСТРУМЕНТИ РОЗРОБКИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-15_ODP[01]	**визначено періодичність перегляду процесу розробки, стандартів, інструментів, опцій інструментів та конфігурацій інструментів;**
	SA-15_ODP[02]	**визначені вимоги до безпеки, яким має відповідати процес, стандарти, інструменти, опції інструментів та**

		конфігурації інструментів;
	SA-15_ODP[03]	**визначені вимоги до конфіденційності, яким має відповідати процес, стандарти, інструменти, опції інструментів та конфігурації інструментів;**
	SA-15a.01[01]	зобов'язаний розробник системи, системного компонента або системної служби дотримуватися задокументованого процесу розробки, який явно враховує вимоги безпеки;
	SA-15a.01[02]	зобов'язаний розробник системи, системного компонента або системної служби дотримуватися задокументованого процесу розробки, який чітко враховує вимоги щодо конфіденційності;
	SA-15a.02[01]	повинен розробник системи, системного компонента або системної служби дотримуватися задокументованого процесу розробки, який визначає стандарти, що використовуються в процесі розробки;
	SA-15a.02[02]	повинен розробник системи, системного компонента або системного служби дотримуватися задокументованого процесу розробки, який визначає інструменти, що використовуються в процесі розробки;
	SA-15a.03[01]	овинен розробник системи, системного компонента або системної служби дотримуватися задокументованого процесу розробки, який документує конкретний інструмент, що використовується в процесі розробки;
	SA-15a.03[02]	повинен розробник системи, системного компонента або системної служби дотримуватися задокументованого процесу розробки, який документує конкретні конфігурації інструментів, що використовуються в процесі розробки;
	SA-15a.04	повинен розробник системи, системного компонента або системної служби дотримуватися задокументованого процесу розробки, який документує, управляє та забезпечує цілісність змін у процесі та/або інструментах, що використовуються під час розробки;
	SA-15b.[01]	повинен розробник системи, системного компонента або системної служби дотримуватися задокументованого процесу розробки, в якому процес розробки, стандарти, інструменти, опції інструментів та конфігурації інструментів переглядаються **з <SA-15_ODP[01] частотою>**, щоб визначити, що процес, стандарти, інструменти, опції інструментів та конфігурації інструментів, вибрані та застосовані, задовольняють **<SA-15_ODP[02] вимоги безпеки>**;
	SA-15b.[02]	повинен розробник системи, системного компонента або системної служби дотримуватися задокументованого процесу розробки, в якому процес розробки, стандарти, інструменти, опції інструментів та конфігурації інструментів переглядаються з **<SA-15_ODP[01]**

		частотою>, щоб визначити, що процес, стандарти, інструменти, опції інструментів та конфігурації інструментів, обрані та застосовані, задовольняють **<SA-15_ODP[03] вимоги щодо конфіденційності>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІРІР: Політика придбання систем та послуг; процедури, що стосуються процесу розробки, стандартів та інструментів; процедури, що стосуються інтеграції вимог безпеки в процесі розробки; заявна документація; документація про придбання; угоди про рівень обслуговування; договори придбання системи, компонента системи або послуги системи; документація розробника системи з переліком параметрів інструменту, посібників з налаштування, записів управління конфігурацією; змінити записи контролю; записи контролю конфігурації; задокументовані огляди процесу розробки, стандартів, інструментів та варіантів, конфігурацій інструментів; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання системи та послуг; персонал організації, який відповідає за інформаційну безпеку; розробник системи].	

SA-15(1)	**ПРОЦЕС, СТАНДАРТИ ТА ІНСТРУМЕНТИ РОЗРОБКИ - ПОКАЗНИКИ ЯКОСТІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-15(01)_ODP[01]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {<SA-15(01)_ODP[02] частота>; <SA-15(01)_ODP[03] перегляд програми>; після доставки};**
	SA-15(01)_ODP[02]	**визначено періодичність надання доказів відповідності показників якості (якщо вибрано);**
	SA-15(01)_ODP[03]	**визначені проміжні етапи перегляду програми (якщо вибрано);**
	SA-15(01)(a)	повинен розробник системи, системного компонента або системної служби визначати метрики якості на початку процесу розробки;
	SA-15(01)(b)	повинен розробник системи, системного компонента або системної служби надавати докази відповідності показників якості **<SA-15(01)_ODP[01] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІРІР: Політика придбання систем та послуг; процедури, що стосуються процесу розробки, стандартів та інструментів; процедури, що стосуються інтеграції вимог безпеки в процесі розробки; заявна документація; документація про придбання; угоди про рівень обслуговування; договори придбання системи, компонента системи або послуги системи; документація розробника системи з переліком параметрів інструменту, посібників з налаштування, записів управління конфігурацією; змінити записи контролю;	

	записи контролю конфігурації; задокументовані огляди процесу розробки, стандартів, інструментів та варіантів, конфігурацій інструментів; інші відповідні документи або записи].

SA-15(3)	**ПРОЦЕС, СТАНДАРТИ ТА ІНСТРУМЕНТИ РОЗРОБКИ - ЗАСОБИ ВІДСТЕЖЕННЯ БЕЗПЕКИ ТА ПРИВАТНОСТІ**
Співбесіда:	[ВИБІР: Персонал організації, який відповідає за придбання системи та послуг; персонал організації, який відповідає за інформаційну безпеку; розробник системи].

	МЕТА ОЦІНКИ:
	Визначити, чи:
SA-15(03)_ODP[01]	**визначені точки прийняття рішень у життєвому циклі розробки системи;**
SA-15(03)_ODP[02]	**визначена широта аналізу критичності;**
SA-15(03)_ODP[03]	**визначено глибину аналізу критичності;**
SA-15(02)[01]	повинен розробник системи, системного компонента або системної служби обирати та використовувати інструменти відстеження безпеки для використання в процесі розробки;
SA-15(02)[02]	зобов'язаний розробник системи, системного компонента або системної служби обирати та використовувати інструменти відстеження приватності для використання в процесі розробки.

SA-15(2)	**ПРОЦЕС, СТАНДАРТИ ТА ІНСТРУМЕНТИ РОЗРОБКИ - ЗАСОБИ ВІДСТЕЖЕННЯ БЕЗПЕКИ ТА ПРИВАТНОСТІ**
	МЕТА ОЦІНКИ:
	Визначити, чи:
SA-15(02)[01]	повинен розробник системи, системного компонента або системної служби обирати та використовувати інструменти відстеження безпеки для використання в процесі розробки;
SA-15(02)[02]	зобов'язаний розробник системи, системного компонента або системної служби обирати та використовувати інструменти відстеження приватності для використання в процесі розробки.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ:
	Дослідження: [ВИБІРІР: Політика придбання систем та послуг; процедури, що стосуються процесу розробки, стандартів та інструментів; процедури, що стосуються інтеграції вимог безпеки в процесі розробки; заявна документація; документація про придбання; угоди про рівень обслуговування; договори придбання системи, компонента системи або послуги системи; документація розробника системи з переліком параметрів інструменту, посібників з налаштування, записів управління конфігурацією; змінити записи контролю; записи контролю конфігурації; задокументовані огляди процесу розробки, стандартів, інструментів та варіантів, конфігурацій інструментів; інші відповідні документи або записи].
	Співбесіда: [ВИБІР: Персонал організації, який відповідає за придбання системи та послуг; персонал організації, який відповідає за інформаційну безпеку; розробник системи].

		SA-15(03)(a)	повинен розробник системи, системного компонента або системного сервісу виконувати аналіз критичності в **<SA-15(03)_ODP[01] точках прийняття рішень>** в життєвому циклі розробки системи;
		SA-15(03)(b)[01]	повинен розробник системи, системного компонента або системного сервісу виконувати аналіз критичності на наступному рівні строгості: **<SA-15(03)_ODP[02] ширина>**;
		SA-15(03)(b)[02]	повинен розробник системи, системного компонента або системного сервісу виконувати аналіз критичності на наступному рівні строгості: **<SA-15(03)_ODP[03] глибина>** .
		ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються процесу розробки, стандартів та інструментів; процедури, що стосуються вимог до аналізу критичності системи, компонента системи або послуги системи; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання системи, компонента системи або послуги системи; документація з аналізу критичності; документація з аналізу впливу на бізнес; документація життєвого циклу розробки програмного забезпечення; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання системи та послуг; персонал організації, який відповідає за інформаційну безпеку; відповідальність організаційного персоналу за проведення аналізу критичності; розробник системи]. **Перевірка:** [ВИБІР: Процеси організації для проведення аналізу критичності; автоматизовані механізми, що підтримують та, або впроваджують аналіз критичності].	
SA-15(4)	**ПРОЦЕС, СТАНДАРТИ ТА ІНСТРУМЕНТИ РОЗРОБКИ - МОДЕЛЮВАННЯ ЗАГРОЗ ТА АНАЛІЗ ВРАЗЛИВОСТЕЙ**		
	[Вилучено: включено до SA-11(2)].		

SA-15(5)	**ПРОЦЕС, СТАНДАРТИ ТА ІНСТРУМЕНТИ РОЗРОБКИ - ЗМЕНШЕННЯ ПОВЕРХНІ АТАКИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-15(05)_ODP	**визначені порогові значення, до яких необхідно зменшити поверхню атаки;**
	SA-15(05)	зобов'язаний розробник системи, системного компонента або системної служби зменшити поверхню атаки до **<SA-15(05)_ODP межі>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються процесу розробки, стандартів та інструментів; процедури, що стосуються зменшення поверхні атаки; заявна документація; документація про придбання; угоди про рівень обслуговування; договори придбання системи або послуги системи; проєктна документація системи; схема мережі; налаштування конфігурації системи та супутньої документації, що встановлюють, забезпечують визначені організацією порогові значення для зменшення поверхонь атаки; перелік обмежених портів, протоколів, функцій та послуг; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання систем та послуг; персонал організації, який відповідає за інформаційну безпеку; відповідальність організаційного персоналу за порогові значення зменшення поверхні атаки; розробник системи]. **Перевірка:** [ВИБІР: Процеси організації для визначення порогів зменшення поверхні атаки].	

SA-15(6)	**ПРОЦЕС, СТАНДАРТИ ТА ІНСТРУМЕНТИ РОЗРОБКИ - ПОСТІЙНЕ ВДОСКОНАЛЕННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-15(06)	зобов'язаний розробник системи, системного компонента або системної служби впроваджувати чіткий процес постійного вдосконалення процесу розробки.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються процесу розробки, стандартів та інструментів; заявна документація; документація про придбання; угоди про рівень обслуговування; договори придбання системи, компонента системи або послуги системи; цілі та показники якості для вдосконалення процесу розробки системи; оцінки безпеки та, або огляди контролю якості процесу розробки системи; плани дій та етапи вдосконалення процесу розробки системи; інші відповідні документи або записи].	

		Співбесіда: [ВИБІР: Персонал організації, який відповідає за придбання систем та послуг; персонал організації, який відповідає за інформаційну безпеку; розробник системи].
SA-15(7)	**ПРОЦЕС, СТАНДАРТИ ТА ІНСТРУМЕНТИ РОЗРОБКИ АВТОМАТИЗОВАНИЙ АНАЛІЗ ВРАЗЛИВОСТЕЙ**	

МЕТА ОЦІНКИ:

Визначити, чи:

SA-15(07)_ODP[01]	**визначено періодичність проведення аналізу вразливостей;**
SA-15(07)_ODP[02]	**визначені інструменти, які використовуються для автоматизованого аналізу вразливостей;**
SA-15(07)_ODP[03]	**визначено персонал або ролі, яким мають бути передані результати інструментів та результати аналізу;**
SA-15(07)(a)	зобов'язаний розробник системи, системного компонента або системного сервісу виконувати автоматизований аналіз вразливостей **<SA-15(07)_ODP[01] частота>** з використанням **<SA-15(07)_ODP[02] інструментарію>**;
SA-15(07)(b)	зобов'язаний розробник системи, системного компоненту або системної служби визначати потенціал використання виявлених вразливостей **<SA-15(07)_ODP[01] частота>**;
SA-15(07)(c)	повинен розробник системи, системного компоненту або системної служби визначати потенційні заходи зменшення ризику **<SA-15(07)_ODP[01] частота>** для наданих вразливостей;
SA-15(07)(d)	повинен розробник системи, системного компонента або системної послуги надавати вихідні дані інструментів і результати аналізу **<SA-15(07)_ODP[01] частота>** персоналу або **<SA-15(07)_ODP[03] ролям>**.

ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ:

Дослідження: [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються процесу розробки, стандартів та інструментів; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання системи, компонента системи або послуги системи; засоби аналізу вразливості та супутньої документації; звіти про оцінку ризиків; результати аналізу вразливості; звіти про пом'якшення вразливості; документація щодо стратегії зменшення ризику; інші відповідні документи або записи].

Співбесіда: [ВИБІР: Персонал організації, який відповідає за придбання систем та послуг; персонал організації, який відповідає за інформаційну безпеку; розробник системи; персонал організації, що здійснює автоматизований аналіз вразливості в системі].

Перевірка: [ВИБІР: Процеси організації для аналізу вразливості інформаційних

	систем, системних компонентів або служб системи, що розробляється; автоматизовані механізми, що підтримують та, або впроваджують аналіз вразливості інформаційних систем, компонентів системи або служб системи, що розробляються].

SA-15(8)	**ПРОЦЕС, СТАНДАРТИ ТА ІНСТРУМЕНТИ РОЗРОБКИ - ПОВТОРНЕ ВИКОРИСТАННЯ ІНФОРМАЦІЇ ПРО ЗАГРОЗИ ТА ВРАЗЛИВОСТІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-15(08)[01]	повинен розробниксистеми, системного компонента або системної служби використовувати моделювання загроз з подібних систем, компонентів або служб для інформування про поточний процес розробки;
	SA-15(08)[02]	повинен розробник системи, системного компонента або системних служб використовувати аналіз вразливостей аналогічних систем, компонентів або служб для інформування поточного процесу розробки.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються процесу розробки, стандартів та інструментів; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання системи, компонента системи або послуги системи; засоби аналізу вразливості та супутньої документації; звіти про оцінку ризиків; результати аналізу вразливості; звіти про пом'якшення вразливості; документація щодо стратегії зменшення ризику; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання систем та послуг; персонал організації, який відповідає за інформаційну безпеку; розробник системи; персонал організації, що здійснює автоматизований аналіз вразливості в системі]. **Перевірка:** [ВИБІР: Процеси організації для аналізу вразливості інформаційних систем, системних компонентів або служб системи, що розробляється; автоматизовані механізми, що підтримують та, або впроваджують аналіз вразливості інформаційних систем, компонентів системи або служб системи, що розробляються].	

SA-15(9)	**ПРОЦЕС, СТАНДАРТИ ТА ІНСТРУМЕНТИ РОЗРОБКИ - ВИКОРИСТАННЯ РЕАЛЬНИХ ДАНИХ**
	[Вилучено: включено до SA-3(2)].

SA-15(10)	**ПРОЦЕС, СТАНДАРТИ ТА ІНСТРУМЕНТИ РОЗРОБКИ - ПЛАН РЕАГУВАННЯ НА ІНЦИДЕНТИ**
	МЕТА ОЦІНКИ: Визначити, чи:

	SA-15(10)[01]	зобов'язаний розробник системи, системного компонента або системної служби надавати план реагування на інциденти;
	SA-15(10)[02]	зобов'язаний розробник системи, системного компонента або системної служби впроваджувати план реагування на інциденти;
	SA-15(10)[03]	зобов'язаний розробник системи, системного компонента або системного служби впроваджувати план реагування на інциденти;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються процесу розробки, стандартів та інструментів; заявна документація; документація про придбання; угоди про рівень обслуговування; договори придбання системи або послуг; документація про придбання; заявна документація; угоди про рівень обслуговування; план реагування на аварії розробника; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання системи та послуг; персонал організації, який відповідає за інформаційну безпеку; розробник системи].	

SA-15(11)	**ПРОЦЕС, СТАНДАРТИ ТА ІНСТРУМЕНТИ РОЗРОБКИ - РЕЗЕРВУВАННЯ СИСТЕМИ АБО КОМПОНЕНТУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-15(11)	повинен розробник системи або компонента системи архівувати систему або компонент, що випускається або постачається, разом з відповідними доказами, що підтверджують остаточну перевірку безпеки та приватності.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються процесу розробки, стандартів та інструментів; заявна документація; документація про придбання; угоди про рівень обслуговування; договори придбання системи або послуг; документація про придбання; заявна документація; угоди про рівень обслуговування; план реагування на аварії розробника; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання системи та послуг; персонал організації, який відповідає за інформаційну безпеку; розробник системи].	

SA-15(12)	**ПРОЦЕС, СТАНДАРТИ ТА ІНСТРУМЕНТИ РОЗРОБКИ - МІНІМІЗАЦІЯ ПЕРСОНАЛЬНОЇ ІНФОРМАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-15(12)	зобов'язаний розробник системи або системного компонента

		мінімізувати використання персональної інформації в середовищах розробки та тестування.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання систем та послуг; процедури придбання систем та послуг; процедури, що стосуються процесу розробки; процедури, що стосуються мінімізації особистої інформації під час тестування, навчання та досліджень; політика обробки особистої iden⌕fiable інформації; процедури, що стосуються повноважень на проведення тестування з використанням особистої інформації; стандарти та інструменти; тендерна документація; угоди про рівень обслуговування; контракти на придбання системи або послуг; план захисту інформації системи; план забезпечення конфіденційності; інші відповідні документи чи записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за закупівлю; персонал організації, відповідальний за інформаційну безпеку та конфіденційність; розробник системи]. **Перевірка**: [ВИБІР: Процеси організації для мінімізації персональних даних у середовищах розробки та тестування; механізми, що сприяють мінімізації персональних даних у середовищах розробки та тестування].	

SA-16	НАВЧАННЯ, ЩО НАДАЄТЬСЯ РОЗРОБНИКАМИ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-16_ODP	**визначено навчання щодо правильного використання та експлуатації впроваджених функцій безпеки та приватності, засобів контролю та/або механізмів, що надаються розробником системи, системного компонента або системної служби;**
	SA-16	повинен розробник системи, системного компонента або системної служби проводити **<SA-16_ODP навчання>** щодо правильного використання та експлуатації впроваджених функцій, засобів управління та/або механізмів безпеки та приватності.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються навчання, яке проводить розробник; заявна документація; документація про придбання; угоди про рівень обслуговування; договори придбання системи, компонента системи або послуги системи; навчальні матеріали, надані розробником; записи про навчання; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання систем та послуг; персонал організації, який відповідає за безпеку системи; розробник системи; організаційні або сторонні розробники, які відповідають за підготовку системи, компонента системи чи служби системи].	

SA-17	ПРОЄКТ ТА АРХІТЕКТУРА БЕЗПЕКИ ТА ПРИВАТНОСТІ ДЛЯ РОЗРОБНИКА	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-17(a)[01]	повинен розробник системи, системного компонента або системної служби створювати специфікації проєкту та архітектури безпеки, які відповідають архітектурі безпеки організації, що є невід'ємною частиною архітектури підприємства організації;
	SA-17(a)[02]	повинен розробник системи, системного компонента або системної служби створювати проєкту та архітектури безпеки поиватності, які відповідають архітектурі приватності організації, що є невід'ємною частиною корпоративної архітектури організації;
	SA-17(b)[01]	зобов'язаний розробник системи, системного компонента або системної служби підготувати специфікацію проєкту та архітектуру безпеки, які точно і повно описують необхідну функціональність безпеки та розподіл засобів контролю між

		фізичними та логічними компонентами;
	SA-17(b)[02]	зобов'язаний розробник системи, системного компонента або системної служби підготувати специфікацію проєкту та архітектуру приватності, які точно і повно описують необхідну функціональність приватності та розподіл засобів контролю між фізичними та логічними компонентами;
	SA-17(c)[01]	повинен розробник системи, системного компонента або системного сервісу створювати проектну специфікацію та архітектуру безпеки, які описують, як окремі функції, механізми та сервіси безпеки працюють разом для забезпечення необхідних можливостей безпеки та єдиного підходу до захисту;
	SA-17(c)[02]	повинен розробник системи, системного компонента або системної служби створювати специфікацію проєкту та архітектуру приватності, які описують, як окремі функції, механізми та служби конфіденційності працюють разом для забезпечення необхідних можливостей приватності та єдиного підходу до захисту
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика придбання систем та послуг; політика архітектури підприємства; процедури, що стосуються архітектури безпеки розробника та специфікації проєкту для системи; заявна документація; документація про придбання; угоди про рівень обслуговування; договори придбання системи, компонента системи або послуги системи; специфікація проєкту та документація архітектури безпеки для системи; проєктна документація системи; налаштування конфігурації системи та відповідна документація; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання систем та послуг; персонал організації, який відповідає за інформаційну безпеку; розробник системи; персонал організації з архітектурою безпеки та дизайнерськими обов'язками].	

SA-17(1)	**ПРОЄКТ ТА АРХІТЕКТУРА БЕЗПЕКИ ТА ПРИВАТНОСТІ РОЗРОБНИКА - ФОРМАЛЬНА МОДЕЛЬ ПОЛІТИКИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-17(01)_ODP[01]	**повинен розробник системи, системного компонента або системної служби створювати специфікацію проєкту та архітектуру приватності, які описують, як окремі функції, механізми та служби приватності працюють разом для забезпечення необхідних можливостей конфіденційності та єдиного підходу до захисту**
	SA-17(01)_ODP[02]	**визначена політика приватності організації, яку необхідно застосовувати;**

	SA-17(01)(a)[01]	повинен розробник системи, системного компонента або системної служби, як невід'ємну частину процесу розробки, створювати формальну модель політики, що описує **<SA-17(01)_ODP[01] організаційну політику безпеки>**, яку необхідно впроваджувати;
	SA-17(01)(a)[02]	повинен розробник системи, системного компонента або системної служби, як невід'ємну частину процесу розробки, створювати формальну модель політики, що описує **<SA-17(01)_ODP[02] організаційну політику конфіденційності>**, яка підлягає виконанню;
	SA-17(01)(b)[01]	повинен розробник системи, системного компонента або системної служби доводити, що формальна модель політики є внутрішньо узгодженою і достатньою для забезпечення дотримання визначених елементів політики безпеки організації при її впровадженні;
	SA-17(01)(b)[02]	повинен розробник системи, системного компонента або системної служби доводити, що формальна модель політики є внутрішньо узгодженою і достатньою для забезпечення дотримання визначених елементів організаційної політики приватності при її впровадженні.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика придбання систем та послуг; політика архітектури підприємства; процедури, що стосуються архітектури безпеки розробника та специфікації проєкту для системи; заявна документація; документація про придбання; угоди про рівень обслуговування; договори придбання системи, компонента системи або послуги системи; специфікація проєкту та документація архітектури безпеки для системи; проєктна документація системи; налаштування конфігурації системи та відповідна документація; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання систем та послуг; персонал організації, який відповідає за інформаційну безпеку; розробник системи; персонал організації з архітектурою безпеки та дизайнерськими обов'язками].	

SA-17(2)	**ПРОЄКТ ТА АРХІТЕКТУРА БЕЗПЕКИ ТА ПРИВАТНОСТІ РОЗРОБНИКА - КОМПОНЕНТИ, ЩО НЕОБХІДНІ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-17(02)(a)[01]	зобов'язаний розробник системи, системного компонента або системної служби визначати апаратне забезпечення, що має відношення до безпеки;
	SA-17(02)(a)[02]	зобов'язаний розробник системи, системного компонента або системної служби визначати програмне забезпечення, що має відношення до безпеки;

	SA-17(02)(a)[03]	зобов'язаний розробник системи, системного компонента або системної служби визначати мікропрограмне забезпечення, що мають відношення до безпеки;
	SA-17(02)(b)	повинен розробник системи, системного компонента або системної служби надавати обґрунтування того, що визначення обладнання, програмного забезпечення та мікропрограмного забезпечення, що мають відношення до безпеки, є повним.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика придбання систем та послуг; політика архітектури підприємства; процедури, що стосуються архітектури безпеки розробника та специфікації проєкту для системи; заявна документація; документація про придбання; угоди про рівень обслуговування; договори придбання системи, компонента системи або послуги системи; специфікація проєкту та документація архітектури безпеки для системи; проєктна документація системи; налаштування конфігурації системи та відповідна документація; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання систем та послуг; персонал організації, який відповідає за інформаційну безпеку; розробник системи; персонал організації з архітектурою безпеки та дизайнерськими обов'язками].	

SA-17(3)	**ПРОЄКТ ТА АРХІТЕКТУРА БЕЗПЕКИ ТА ПРИВАТНОСТІ РОЗРОБНИКА - ФОРМАЛЬНА ВІДПОВІДНІСТЬ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-17(03)(a)[01]	зобов'язаний розробник системи, системного компонента або системної служби визначати апаратне забезпечення, що має відношення до безпеки;
	SA-17(03)(a)[02]	зобов'язаний розробник системи, системного компонента або системної служби визначати програмне забезпечення, що має відношення до безпеки;
	SA-17(03)(a)[03]	зобов'язаний розробник системи, системного компонента або системної служби визначати мікропрограми, що мають відношення до безпеки;
	SA-17(03)(b)	повинен розробник системи, системного компонента або системної служби надавати обґрунтування того, що визначення обладнання, програмного забезпечення та мікропрограмного забезпечення, що мають відношення до безпеки, є повним.
	SA-17(03)(c)	повинен розробник системи, системного компонента або системної служби демонструвати за допомогою неформальної демонстрації, що формальна специфікація верхнього рівня повністю охоплює інтерфейси до обладнання, програмного

		забезпечення та мікропрограмного забезпечення, що мають відношення до безпеки;
	SA-17(03)(d)	повинен розробник системи, системного компонента або системної служби доводити, що формальна специфікація верхнього рівня є точним описом впровадженого обладнання, програмного забезпечення та мікропрограмного забезпечення, що мають відношення до безпеки;
	SA-17(03)(e)	повинен розробник системи, системного компонента або системної служби описувати релевантні для безпеки апаратні, програмні та мікропрограмні механізми, які не розглядаються у формальній специфікації верхнього рівня, але є суто внутрішніми для релевантних для безпеки апаратних, програмних та мікропрограмних засобів.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика придбання систем та послуг; політика архітектури підприємства; формальна політична модель; процедури, що стосуються архітектури безпеки розробника та специфікації проєкту для системи; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання системи, компонента системи або послуги системи; офіційна технічна документація вищого рівня; архітектура безпеки системи та проєктна документація; проєктна документація системи; налаштування конфігурації системи та відповідна документація; документація, що описує механізми апаратного забезпечення, програмного забезпечення та програмного забезпечення, що стосуються безпеки, не зафіксовані в офіційній документації технічного завдання верхнього рівня; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання систем та послуг; персонал організації, який відповідає за інформаційну безпеку; розробник системи; персонал організації з архітектурою безпеки та дизайнерськими обов'язками].	

SA-17(4)	**ПРОЄКТ ТА АРХІТЕКТУРА БЕЗПЕКИ ТА ПРИВАТНОСТІ РОЗРОБНИКА - НЕФОРМАЛЬНА ВІДПОВІДНІСТЬ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-17(04)_ODP	**вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРА: {неформальна описова специфікація, переконливий аргумент за допомогою формальних методів як можлива};**
	SA-17(04)(a)[01]	повинен розробник системи, системного компонента або системної служби, як невід'ємну частину процесу розробки, створювати неформальну описову специфікацію верхнього рівня, яка визначає інтерфейси до релевантного для безпеки апаратного, програмного та мікропрограмного забезпечення з точки зору винятків;
	SA-17(04)(a)[02]	повинен розробник системи, системного компонента або

		системної служби, як невід'ємну частину процесу розробки, створювати неформальну описову специфікацію верхнього рівня, яка визначає інтерфейси до релевантного для безпеки апаратного, програмного та мікропрограмного забезпечення в термінах повідомлень про помилки;
	SA-17(04)(a)[03]	повинен розробник системи, системного компоненту або системної служби, як невід'ємну частину процесу розробки, створювати неформальну описову специфікацію верхнього рівня, яка визначає інтерфейси до релевантного для безпеки обладнання, програмного забезпечення та мікропрограмного забезпечення з точки зору наслідків;
	SA-17(04)(b)	повинен розробник системи, системного компонента або системної служби показувати за допомогою **<SA-17(04)_ODP ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>**, що описова специфікація верхнього рівня узгоджується з формальною моделлю політики;
	SA-17(04)(c)	повинен розробник системи, системного компонента або системної служби демонструвати за допомогою неформальної демонстрації, що описова специфікація верхнього рівня повністю охоплює інтерфейси до апаратного, програмного та мікропрограмного забезпечення, що мають відношення до безпеки;
	SA-17(04)(d)	повинен розробник системи, системного компонента або системної служби показувати, що описова специфікація верхнього рівня є точним описом інтерфейсів до релевантного для безпеки апаратного, програмного та мікропрограмного забезпечення;
	SA-17(04)(e)	повинен розробник системи, системного компонента або системної служби описувати релевантні для безпеки апаратні, програмні та мікропрограмні механізми, які не розглядаються в описовій специфікації верхнього рівня, але є суто внутрішніми для релевантних для безпеки апаратних, програмних та мікропрограмних засобів.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика придбання систем та послуг; політика архітектури підприємства; формальна політична модель; процедури, що стосуються архітектури безпеки розробника та специфікації проєкту для системи; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання системи, компонента системи або послуги системи; офіційна технічна документація вищого рівня; архітектура безпеки системи та проєктна документація; проєктна документація системи; налаштування конфігурації системи та відповідна документація; документація, що описує механізми апаратного забезпечення, програмного забезпечення та програмного забезпечення, що стосуються безпеки, не зафіксовані в офіційній документації технічного завдання верхнього рівня; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання систем та послуг; персонал організації, який відповідає за інформаційну безпеку;		

	розробник системи; персонал організації з архітектурою безпеки та дизайнерськими обов'язками].

SA-17(5)	**ПРОЄКТ ТА АРХІТЕКТУРА БЕЗПЕКИ ТА ПРИВАТНОСТІ РОЗРОБНИКА - КОНЦЕПТУАЛЬНИЙ ПРОЄКТ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-17(05)(a)	повинен розробник системи, системного компонента або системної служби проектувати та структурувати апаратне, програмне та мікропрограмне забезпечення, пов'язане з безпекою, таким чином, щоб використовувати повний, концептуально простий механізм захисту з чітко визначеною семантикою;
	SA-17(05)(b)	повинен розробник системи, системного компонента або системної служби внутрішньо структурувати обладнання, програмне забезпечення та вбудоване програмне забезпечення, пов'язане з безпекою, з урахуванням цього механізму.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика придбання систем та послуг; політика архітектури підприємства; формальна політична модель; процедури, що стосуються архітектури безпеки розробника та специфікації проєкту для системи; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання системи, компонента системи або послуги системи; офіційна технічна документація вищого рівня; архітектура безпеки системи та проєктна документація; проєктна документація системи; налаштування конфігурації системи та відповідна документація; документація, що описує механізми апаратного забезпечення, програмного забезпечення та програмного забезпечення, що стосуються безпеки, не зафіксовані в офіційній документації технічного завдання верхнього рівня; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання систем та послуг; персонал організації, який відповідає за інформаційну безпеку; розробник системи; персонал організації з архітектурою безпеки та дизайнерськими обов'язками].	

SA-17(6)	**ПРОЄКТ ТА АРХІТЕКТУРА БЕЗПЕКИ ТА ПРИВАТНОСТІ РОЗРОБНИКА - СТРУКТУРА ДЛЯ ТЕСТУВАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-17(06)	повинен розробник системи, системного компонента або системної служби структурувати обладнання, програмне забезпечення та вбудоване програмне забезпечення, пов'язане

		з безпекою, для полегшення тестування.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика придбання систем та послуг; політика архітектури підприємства; формальна політична модель; процедури, що стосуються архітектури безпеки розробника та специфікації проєкту для системи; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання системи, компонента системи або послуги системи; офіційна технічна документація вищого рівня; архітектура безпеки системи та проєктна документація; проєктна документація системи; налаштування конфігурації системи та відповідна документація; документація, що описує механізми апаратного забезпечення, програмного забезпечення та програмного забезпечення, що стосуються безпеки, не зафіксовані в офіційній документації технічного завдання верхнього рівня; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання систем та послуг; персонал організації, який відповідає за інформаційну безпеку; розробник системи; персонал організації з архітектурою безпеки та дизайнерськими обов'язками].	

SA-17(7)	**ПРОЄКТ ТА АРХІТЕКТУРА БЕЗПЕКИ ТА ПРИВАТНОСТІ РОЗРОБНИКА - СТРУКТУРА ДЛЯ НАЙМЕНШОГО ПРИВІЛЕЮ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-17(07)	повинен розробник 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.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика придбання систем та послуг; політика архітектури підприємства; формальна політична модель; процедури, що стосуються архітектури безпеки розробника та специфікації проєкту для системи; тендерна документація; документація про придбання; угоди про рівень обслуговування; договори придбання системи, компонента системи або послуги системи; офіційна технічна документація вищого рівня; архітектура безпеки системи та проєктна документація; проєктна документація системи; налаштування конфігурації системи та відповідна документація; документація, що описує механізми апаратного забезпечення, програмного забезпечення та програмного забезпечення, що стосуються безпеки, не зафіксовані в офіційній документації технічного завдання верхнього рівня; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання систем та послуг; персонал організації, який відповідає за інформаційну безпеку; розробник системи; персонал організації з архітектурою безпеки та дизайнерськими обов'язками].	

SA-17(8)	ПРОЄКТ ТА АРХІТЕКТУРА БЕЗПЕКИ ТА ПРИВАТНОСТІ РОЗРОБНИКА - ОРКЕСТРОВКА	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-17(08)_ODP[01]	**визначені критичні системи або компоненти системи;**
	SA-17(08)_ODP[02]	**визначені можливості, які повинні бути реалізовані системами або компонентами;**
	SA-17(08)	розроблені **<SA-17(08) _ODP[01] критичні системи>** з узгодженою поведінкою для реалізації **<SA-17(08) _ODP[02] спроможностей>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання систем та послуг; політика архітектури підприємства; процедури, що стосуються архітектури та дизайну безпеки та конфіденційності розробника; архітектура підприємства; архітектура безпеки; тендерна документація; документація щодо придбання; угоди про рівень обслуговування; контракти на придбання системи, системного компонента або системної послуги; документація щодо проектування системи; налаштування конфігурації системи та пов'язана з нею документація; документація розробника, що описує організацію проектування; план захисту інформації системи; план конфіденційності; інші відповідні документи чи записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за придбання систем та послуг; персонал організації, відповідальний за інформаційну безпеку та конфіденційність; розробник системи; персонал організації, відповідальний за архітектуру інформаційної безпеки].	

SA-17(9)	ПРОЄКТ ТА АРХІТЕКТУРА БЕЗПЕКИ ТА ПРИВАТНОСТІ РОЗРОБНИКА - РІЗНОМАНІТНІСТЬ ПРОЕКТУВАННЯ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-17(09)_ODP	**визначені критичні системи або компоненти системи, які мають бути спроектовані по-іншому;**
	SA-17(09)	використовуються різні конструкції для **<SA-17(09)_ODP критичних систем>**, щоб задовольнити загальний набір вимог або забезпечити еквівалентну функціональність.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика придбання систем та послуг; політика архітектури підприємства; процедури, що стосуються архітектури та дизайну безпеки та конфіденційності розробника; архітектура підприємства; архітектура безпеки; тендерна документація; документація щодо придбання; угоди про рівень	

	обслуговування; контракти на придбання системи, системного компонента або системної послуги; документація щодо проектування системи; налаштування конфігурації системи та пов'язана з нею документація; документація розробника, що описує організацію проектування; план захисту інформації системи; план конфіденційності; інші відповідні документи чи записи]. **Співбесіда**: [ВИБІР: Персонал організації, відповідальний за придбання систем та послуг; персонал організації, відповідальний за інформаційну безпеку та конфіденційність; розробник системи; персонал організації, відповідальний за архітектуру інформаційної безпеки].

SA-18	**ЗАХИСТ ТА ВИЯВЛЕННЯ ПІДРОБКИ**
	[Вилучено: включено до SR-9].

SA-18(1)	**ЗАХИСТ ТА ВИЯВЛЕННЯ ПІДРОБКИ - ЕТАПИ ЖИТТЄВОГО ЦИКЛУ РОЗРОБКИ СИСТЕМИ**
	[Вилучено: включено до SR-9 (1)].

SA-18(2)	**ЗАХИСТ ТА ВИЯВЛЕННЯ ПІДРОБКИ - ПЕРЕВІРКА СИСТЕМ АБО КОМПОНЕНТІВ**
	[Вилучено: включено до SR-10].

SA-19	**СПРАВЖНІСТЬ КОМПОНЕНТА**
	[Вилучено: включено до SR-11].

SA-19(1)	**СПРАВЖНІСТЬ КОМПОНЕНТА - НАВЧАННЯ БОРОТЬБІ З ПІДРОБЛЕННЯМ**
	[Вилучено: включено до SR-11 (1)].

SA-19(2)	**СПРАВЖНІСТЬ КОМПОНЕНТА - УПРАВЛІННЯ КОНФІГУРАЦІЄЮ ДЛЯ ОБСЛУГОВУВАННЯ ТА РЕМОНТУ КОМПОНЕНТІВ**
	[Вилучено: включено до SR-11 (2)].

SA-19(3)	**СПРАВЖНІСТЬ КОМПОНЕНТА - УТИЛІЗАЦІЯ КОМПОНЕНТІВ**
	[Вилучено: включено до SR-12].

SA-19(4)	**СПРАВЖНІСТЬ КОМПОНЕНТА - СКАНУВАННЯ НА ПІДРОБКУ**
	[Вилучено: включено до SR-11 (3)].

SA-20	**ІНДИВІДУАЛЬНА РОЗРОБКА КРИТИЧНИХ КОМПОНЕНТІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-20_ODP	**потрібно повторно реалізувати або налаштувати на замовлення критичні компоненти системи;**
	SA-20	**<SA-20_ODP критична система>** повторно реалізувати або

		налаштувати на замовлення
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються індивідуального розвитку важливих компонентів системи; проєктна документація системи; налаштування конфігурації системи та відповідна документація; документація життєвого циклу розробки системи, що стосується нестандартної розробки важливих компонентів системи; записи управління конфігурацією; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання систем та послуг; персонал організації, який відповідає за інформаційну безпеку; персонал організації, відповідальний за повторне впровадження або налаштування важливих компонентів системи]. **Перевірка:** [ВИБІР: Процеси організації для повторного впровадження або налаштування важливих компонентів системи; автоматизовані механізми, що підтримують та, або реалізують повторне впровадження або налаштування важливих компонентів системи].	

SA-21	**ПЕРЕВІРКА РОЗРОБНИКА**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-21_ODP[01]	**визначена система, компонент системи або системна служба, до яких має доступ розробник;**
	SA-21_ODP[02]	**визначені офіційні обов'язки, покладені на розробника;**
	SA-21_ODP[03]	**визначені додаткові критерії перевірки персоналу розробників;**
	SA-21a.	повинен розробник **<SA-21_ODP[01] системи, системного компонента або системної служби>** мати відповідні повноваження доступу, як визначено призначеними **<SA-21_ODP[02] уповноваженим органом організації>**;
	SA-21b.	повинен розробник **<SA-21_ODP[01] системи, системного компонента або системної служби>** відповідати **<SA-21_ODP[03] додатковим критеріям перевірки персоналу>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються індивідуального розвитку важливих компонентів системи; проєктна документація системи; налаштування конфігурації системи та відповідна документація; документація життєвого циклу розробки системи, що стосується нестандартної розробки важливих компонентів системи; записи управління конфігурацією; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання систем та послуг; персонал організації, який відповідає за інформаційну безпеку; персонал організації, відповідальний за повторне впровадження або	

	налаштування важливих компонентів системи]. **Перевірка:** [ВИБІР: Процеси організації для повторного впровадження або налаштування важливих компонентів системи; автоматизовані механізми, що підтримують та, або реалізують повторне впровадження або налаштування важливих компонентів системи].

SA-21(1)	**СКРИНІНГ РОЗРОБНИКА - ПЕРЕВІРКА СКРИНІНГУ**
	[Вилучено: включено до SA-21].

SA-22	**КОМПОНЕНТИ СИСТЕМИ, ЩО НЕ ПІДТРИМУЮТЬСЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SA-22_ODP[01]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {внутрішня підтримка; <SA-22_ODP[02] підтримка від зовнішніх постачальників>};**
	SA-22_ODP[02]	**визначена підтримка з боку зовнішніх постачальників (якщо обрано);**
	SA-22a.	**замінюються компоненти системи, якщо розробник, постачальник або виробник більше не надає підтримку цих компонентів;**
	SA-22b.	**<SA-22_ODP[01] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** надає варіанти альтернативних джерел для продовження підтримки непідтримуваних компонентів.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика придбання систем та послуг; процедури, що стосуються індивідуального розвитку важливих компонентів системи; проєктна документація системи; налаштування конфігурації системи та відповідна документація; документація життєвого циклу розробки системи, що стосується нестандартної розробки важливих компонентів системи; записи управління конфігурацією; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за придбання систем та послуг; персонал організації, який відповідає за інформаційну безпеку; персонал організації, відповідальний за повторне впровадження або налаштування важливих компонентів системи]. **Перевірка:** [ВИБІР: Процеси організації для повторного впровадження або налаштування важливих компонентів системи; автоматизовані механізми, що підтримують та, або реалізують повторне впровадження або налаштування важливих компонентів системи].	

SA-22(1)	**КОМПОНЕНТИ СИСТЕМИ, ЩО НЕ ПІДТРИМУЮТЬСЯ - АЛЬТЕРНАТИВНІ ДЖЕРЕЛА ДЛЯ ПОСТІЙНОЇ ПІДТРИМКИ**
	[Вилучено: включено до SA-22].

<table>
<tr><td>SA-23</td><td colspan="2">СПЕЦІАЛІЗАЦІЯ</td></tr>
<tr><td rowspan="5"></td><td colspan="2">МЕТА ОЦІНКИ:
Визначити, чи:</td></tr>
<tr><td>SA-23_ODP[01]</td><td>вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {модифікація дизайну; доповнення; реконфігурація};</td></tr>
<tr><td>SA-23_ODP[02]</td><td>визначені системи або компоненти системи, що підтримують важливі для місії послуги або функції;</td></tr>
<tr><td>SA-23</td><td>використовується <SA-23_ODP[01] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)> у <SA-23_ODP[02] системах або компонентах системи>, що підтримують основні послуги або функції, для підвищення довіри до цих систем або компонентів.</td></tr>
<tr><td colspan="2">ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:
Дослідження: [ВИБІР: Політика придбання систем та послуг; політика архітектури підприємства; процедури, що стосуються архітектури та дизайну безпеки та конфіденційності розробника; архітектура підприємства; архітектура безпеки; тендерна документація; документація щодо придбання; угоди про рівень обслуговування; контракти на придбання системи, системного компонента або системної послуги; документація щодо проектування системи; налаштування конфігурації системи та пов'язана з нею документація; документація розробника, що описує організацію проектування; план захисту інформації системи; план конфіденційності; інші відповідні документи чи записи].
Співбесіда: [ВИБІР: Персонал організації, відповідальний за придбання систем та послуг; персонал організації, відповідальний за інформаційну безпеку та конфіденційність; розробник системи; персонал організації, відповідальний за архітектуру інформаційної безпеки].</td></tr>
</table>

XVIII. КЛАС ЗАХОДІВ ЗАХИСТУ SC – ЗАХИСТ ІНФОРМАЦІЙНОЇ СИСТЕМИ ТА КОМУНІКАЦІЙ

SC-1	**ПОЛІТИКА ТА ПРОЦЕДУРИ ЗАХИСТУ СИСТЕМИ ТА КОМУНІКАЦІЙ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-01_ODP[01]	**визначено персонал або ролі, до яких має бути доведена політика захисту системи та комунікацій;**
	SC-01_ODP[02]	**визначено персонал або ролі, на які поширюються процедури захисту системи та комунікацій;**
	SC-01_ODP[03]	**вибрано жодне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {рівень організації; рівень місії/бізнес-процесу; рівень системи};**
	SC-01_ODP[04]	**визначено посадову особу, яка керуватиме політикою та процедурами захисту системи та комунікацій;**
	SC-01_ODP[05]	**визначена періодичність перегляду та оновлення поточної політики захисту системи та комунікацій;**
	SC-01_ODP[06]	**є події, які вимагають перегляду та оновлення поточної політики захисту системи та комунікацій;**
	SC-01_ODP[07]	**визначена періодичність перегляду та оновлення поточних процедур захисту системи та засобів зв'язку;**
	SC-01_ODP[08]	**є події, які вимагають перегляду та оновлення процедур захисту системи та комунікацій;**
	SC-01a.[01]	розроблена та задокументована політика захисту системи та комунікацій;
	SC-01a.[02]	поширюється політика захисту системи та комунікацій на **<SC-01_ODP[01] персонал або ролі>**;
	SC-01a.[03]	розроблені та задокументовані процедури захисту систем та засобів зв'язку для сприяння впровадженню політики захисту систем та засобів зв'язку, а також відповідні засоби контролю захисту систем та засобів зв'язку;
	SC-01a.[04]	поширюються процедури захисту системи та комунікацій на **<SC-01_ODP[02] персонал або ролі>**;
	SC-01a.01(a)[01]	відповідає **<SC-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** політика захисту системи та комунікацій призначенню;
	SC-01a.01(a)[02]	чи **<SC-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(S)>** політики захисту системи та комунікацій охоплює сферу дії;
	SC-01a.01(a)[03]	**<SC-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** системи та політика захисту омунікацій

		стосується ролей;
	SC-01a.01(a)[04]	політика захисту системи та комунікацій **<SC-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** стосується обов'язків;
	SC-01a.01(a)[05]	політика захисту системи та комунікацій **<SC-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** враховує зобов'язання керівництва;
	SC-01a.01(a)[06]	політика захисту системи та комунікацій **<SC-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** стосується координації між організаційними одиницями;
	SC-01a.01(a)[07]	політика захисту системи та комунікацій **<SC-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** забезпечує відповідність вимогам;
	SC-01a.01(b)	відповідає **<SC-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** система та політика захисту комунікацій чинним законам, виконавчим наказам, директивам, положенням, політикам, стандартам та настановам;
	SC-01b.	призначена **<SC-01_ODP[04] посадова особа>** для управління розробкою, документуванням та розповсюдженням політики та процедур захисту системи та зв'язку;
	SC-01c.01[01]	переглядається та оновлюється поточна політика захисту системи та комунікацій **<SC-01_ODP[05] частота>**;
	SC-01c.01[02]	переглядається та оновлюється поточна політика захисту системи та комунікацій після **<SC-01_ODP[06] подій>**;
	SC-01c.02[01]	переглядаються та оновлюються поточні процедури захисту системи та комунікацій **<SC-01_ODP[07] частота>**;
	SC-01c.02[02]	переглядаються та оновлюються поточні процедури захисту системи та комунікацій після **<SC-01_ODP[08] події>**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політики та процедури захисту системи та комунікацій; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал відповідальний за політику захисту системи та комунікацій; персонал, відповідальний за інформаційну безпеку].	

SC-2	**РОЗДІЛЕННЯ ФУНКЦІЙ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-02	розділена функціональність користувача, включаючи сервіси користувацького інтерфейсу, від функціональності управління системою.

	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту систем та комунікацій; процедури, що стосуються розділення додатків; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; розробник системи]. **Перевірка:** [ВИБІР: Відокремлення функціональності користувача від функцій управління інформаційною системою].

SC-2(1)	**РОЗДІЛЕННЯ ФУНКЦІЙ - ІНТЕРФЕЙСИ ДЛЯ НЕПРИВІЛЕЙОВАНИХ КОРИСТУВАЧІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-02(01)	запобігається представлення функціональності управління системою в інтерфейсі непривілейованим користувачам.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту систем та комунікацій; процедури, що стосуються розділення додатків; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; розробник системи]. **Перевірка:** [ВИБІР: Відокремлення функціональності користувача від функцій управління інформаційною системою].	

SC-2(2)	**РОЗДІЛЕННЯ ФУНКЦІЙ - ВІДОКРЕМЛЕННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-02(02)	зберігається інформація окремо від додатків та програмного забезпечення.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: Політика захисту системи та комунікацій; процедури, що стосуються розділення додатків та програмного забезпечення; документація з проектування системи; налаштування конфігурації системи та пов'язана з ними документація; записи аудиту системи; план захисту інформації системи; план забезпечення конфіденційності; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Системні/мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку та конфіденційність; розробник системи].	

	Перевірка: [ВИБІР: Відокремлення інформації про стан програми від програмного забезпечення].

SC-3	**ІЗОЛЯЦІЯ ФУНКЦІЙ БЕЗПЕКИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-03	ізольовані функції безпеки від інших функцій
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: Політика захисту системи та комунікацій; процедури, що стосуються розділення додатків та програмного забезпечення; документація з проектування системи; налаштування конфігурації системи та пов'язана з ними документація; записи аудиту системи; план захисту інформації системи; план забезпечення конфіденційності; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Системні/мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку та конфіденційність; розробник системи]. **Перевірка:** [ВИБІР: Відокремлення інформації про стан програми від програмного забезпечення].	

SC-3(1)	**ІЗОЛЯЦІЯ ФУНКЦІЙ БЕЗПЕКИ - РОЗДІЛЕННЯ АПАРАТНОГО ЗАБЕЗПЕЧЕННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-03(01)	застосовуються механізми розділення апаратних засобів для реалізації ізоляції функцій безпеки.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту систем та комунікацій; процедури, що стосуються ізоляції функції безпеки; проєктна документація системи; механізми апаратного розділення; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; розробник системи]. **Перевірка:** [ВИБІР: Розділення функцій безпеки від функцій, що не стосуються безпеки, в межах системи].	

SC-3(2)	**ІЗОЛЯЦІЯ ФУНКЦІЙ БЕЗПЕКИ - ФУНКЦІЇ УПРАВЛІННЯ ДОСТУПОМ ТА ПОТОКОМ**
	МЕТА ОЦІНКИ:

	Визначити, чи:	
	SC-03(02)[01]	ізольовані функції безпеки, що забезпечують управління доступом, які не пов'язані з безпекою;
	SC-03(02)[02]	ізольовані функції безпеки, що забезпечують контроль доступу, від інших функцій безпеки;
	SC-03(02)[03]	ізольовані функції безпеки, які не пов'язані з безпекою забезпечують контроль інформаційних потоків;
	SC-03(02)[04]	ізольовані функції безпеки, що забезпечують контроль інформаційних потоків, від інших функцій безпеки
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються ізоляції функції безпеки; перелік важливих функцій безпеки; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; розробник системи]. **Перевірка:** [ВИБІР: Ізоляція функцій безпеки, що забезпечують контроль доступу та управління потоком інформації].	

SC-3(3)	**ІЗОЛЯЦІЯ ФУНКЦІЙ БЕЗПЕКИ - МІНІМІЗАЦІЯ ФУНКЦІОНАЛЬНОСТІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-03(03)	мінімізовано кількість функцій, не пов'язаних з безпекою, що входять до сфери ізоляції, яка містить функції безпеки.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються ізоляції функції безпеки; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують границю ізоляції].	

SC-3(4)	**ІЗОЛЯЦІЯ ФУНКЦІЙ БЕЗПЕКИ - З'ЄДНАННЯ МОДУЛІВ ТА ЗВ'ЯЗНІСТЬ**
	МЕТА ОЦІНКИ: Визначити, чи:

	SC-03(04)[01]	мінімізовано кількість функцій, не пов'язаних з безпекою, що входять до межі ізоляції, яка містить функції безпеки.
	SC-03(04)[02]	реалізовані функції безпеки як значною мірою незалежні модулі, які мінімізують зв'язок між модулями.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються ізоляції функції безпеки; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для максимізації внутрішньої зв'язності в модулях та мінімізації зв'язку між модулями; автоматизовані механізми, що підтримують та, або реалізують функції безпеки як незалежні модулі].	

SC-3(5)	**ІЗОЛЯЦІЯ ФУНКЦІЙ БЕЗПЕКИ - БАГАТОРІВНЕВА СТРУКТУРА**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-03(05)	реалізовані функції безпеки як багаторівнева структура, що мінімізує взаємодію між шарами дизайну та уникає будь-якої залежності нижчих шарів від функціональності або коректності вищих шарів.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються ізоляції функції безпеки; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для максимізації внутрішньої зв'язності в модулях та мінімізації зв'язку між модулями; автоматизовані механізми, що підтримують та, або реалізують функції безпеки як незалежні модулі].	

SC-4	**ІНФОРМАЦІЯ В ЗАГАЛЬНИХ СИСТЕМНИХ РЕСУРСАХ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-04[01]	запобігається несанкціонована передача інформації через спільні системні ресурси;
	SC-04[02]	запобігається ненавмисна передача інформації через спільні системні ресурси.

	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту інформації у спільних системних ресурсах; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; розробник системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що запобігають несанкціонованому та ненавмисному передаванню інформації через спільні системні ресурси].

SC-4(1)	**ІНФОРМАЦІЯ В ЗАГАЛЬНИХ СИСТЕМНИХ РЕСУРСАХ - РІВНІ БЕЗПЕКИ**
	[Вилучено: включено до SC-4].

SC-4(2)	**ІНФОРМАЦІЯ В ЗАГАЛЬНИХ СИСТЕМНИХ РЕСУРСАХ - БАГАТОРІВНЕВА АБО ПЕРІОДИЧНА ОБРОБКА**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-04(02)_ODP	**визначені процедури для запобігання несанкціонованій передачі інформації через спільні ресурси;**
	SC-04(02)	запобігається несанкціонована передача інформації через спільні ресурси відповідно до **<SC-04(02)_ODP процедур>**, коли системна обробка явно перемикається між різними рівнями класифікації інформації або категоріями безпеки.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту інформації у спільних системних ресурсах; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; розробник системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що запобігають несанкціонованому та ненавмисному передаванню інформації через спільні системні ресурси].	

SC-5	**ЗАХИСТ ВІД АТАК «ВІДМОВА В ОБСЛУГОВУВАННІ»**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-05_ODP[01]	**визначені типи подій відмов в обслуговуванні, від яких потрібно захищати або обмежувати;**

	SC-05_ODP[02]	**вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {захистити від; обмежити};**
	SC-05_ODP[03]	**визначені засоби контролю для досягнення мети відмови в обслуговуванні за типом події відмови в обслуговуванні;**
	SC-05a.	наслідки **<SC-05_ODP[01] типи подій відмови в обслуговуванні>** є **<SC-05_ODP[02] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>**;
	SC-05b.	застосовуються **<SC-05_ODP[03] елементи керування за типом події відмови в обслуговуванні>** для досягнення мети захисту від відмови в обслуговуванні.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту інформації у спільних системних ресурсах; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; розробник системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що запобігають несанкціонованому та ненавмисному передаванню інформації через спільні системні ресурси].	

SC-5(1)	**ЗАХИСТ ВІД АТАК «ВІДМОВА В ОБСЛУГОВУВАННІ» - ОБМЕЖЕННЯ ВНУТРІШНІХ КОРИСТУВАЧІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-05(01)_ODP	**визначені атаки на відмову в обслуговуванні, для яких необхідно обмежити можливість їх запуску окремими особами;**
	SC-05(01)	обмежена можливість окремих осіб здійснювати **<SC-05(01)_ODP атаки на відмову в обслуговуванні>** проти інших систем.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБЕРІТЬ З: Політика захисту системи та комунікацій; процедури, що стосуються захисту відмови у наданні послуги; проєктна документація системи; план захисту інформації; перелік атак відмови в обслуговуванні, розпочатих приватними особами проти інформаційних систем; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, відповідальний за реагування на інциденти; розробник системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що обмежують можливість	

	запуску атак відмови в обслуговуванні проти інших інформаційних систем].

SC-5(2)	**ЗАХИСТ ВІД АТАК «ВІДМОВА В ОБСЛУГОВУВАННІ» - ПРОДУКТИВНІСТЬ, ПРОПУСКНА ЗДАТНІСТЬ ТА НАДМІРНІСТЬ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-05(02)	здійснюється управління ємністю, пропускною здатністю або іншими надлишковими ресурсами для обмеження наслідків інформаційних атак на відмову в обслуговуванні.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту відмови у наданні послуги; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, відповідальний за реагування на інциденти; розробник системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують управління пропускною спроможністю та надмірністю системи, щоб обмежити наслідки затоплення інформацією атак відмови в обслуговуванні].	

SC-5(3)	**ЗАХИСТ ВІД АТАК «ВІДМОВА В ОБСЛУГОВУВАННІ» - ВИЯВЛЕННЯ ТА МОНІТОРИНГ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-05(03)_ODP[01]	**визначені інструменти моніторингу для виявлення індикаторів атак на відмову в обслуговуванні;**
	SC-05(03)_ODP[02]	є системні ресурси, що підлягають моніторингу, достатніми для запобігання ефективним атакам на відмову в обслуговуванні;
	SC-05(03)(a)	використовуються **<SC-05(03)_ODP[01] засоби моніторингу>** для виявлення ознак атак на відмову в обслуговуванні, спрямованих на систему або запущених з неї;
	SC-05(03)(b)	здійснюється моніторинг **<SC-05(03)_ODP[02] системних ресурсів>** для визначення наявності достатніх ресурсів для запобігання ефективним атакам на відмову в обслуговуванні.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту відмови у наданні послуги; проєктна документація системи; документація засобів і методів моніторингу системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні	

	документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який відповідає за виявлення та моніторинг]. **Перевірка:** [ВИБІР: Автоматизовані механізми, інструменти, що реалізують моніторинг системи для атак відмови в обслуговуванні].

SC-6	**ДОСТУПНІСТЬ РЕСУРСІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-06_ODP[01]	**визначені ресурси, які необхідно виділити для захисту доступності ресурсів;**
	SC-06_ODP[02]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {priority; quota; <SC-06_ODP[03] controls>};**
	SC-06_ODP[03]	**визначені засоби контролю для захисту доступності ресурсів (якщо вибрано);**
	SC-06	захищено доступність ресурсів шляхом розподілу **<SC-06_ODP[01] ресурсів>** за **<SC-06_ODP[02] ВИБІРКОВИМ ЗНАЧЕННЯМ ПАРАМЕТРА(ів)>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту відмови у наданні послуги; проєктна документація системи; документація засобів і методів моніторингу системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який відповідає за виявлення та моніторинг]. **Перевірка:** [ВИБІР: Автоматизовані механізми, інструменти, що реалізують моніторинг системи для атак відмови в обслуговуванні].	

SC-7	**ДОСТУПНІСТЬ РЕСУРСІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-07_ODP	**вибрано вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРА: {фізично; логічно};**
	SC-07a.[01]	здійснюється моніторинг комунікацій на зовнішніх керованих інтерфейсах системи;
	SC-07a.[02]	контролюється зв'язок на зовнішніх керованих інтерфейсах

		системи;
	SC-07a.[03]	здійснюється моніторинг комунікацій на ключових внутрішніх керованих інтерфейсах всередині системи;
	SC-07a.[04]	контролюються комунікації на ключових внутрішніх керованих інтерфейсах системи;
	SC-07b.	підмережі для загальнодоступних компонентів системи **<SC-07_ODP ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>** відокремлені від внутрішніх мереж організації;
	SC-07c.	підключення до зовнішніх мереж або систем здійснюється лише через керовані інтерфейси, що складаються з пристроїв захисту кордонів, розташованих відповідно до організаційної архітектури безпеки та конфіденційності.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту відмови у наданні послуги; проєктна документація системи; документація засобів і методів моніторингу системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який відповідає за виявлення та моніторинг]. **Перевірка:** [ВИБІР: Автоматизовані механізми, інструменти, що реалізують моніторинг системи для атак відмови в обслуговуванні].	

SC-7(1)	**ЗАХИСТ ПЕРИМЕТРА - ФІЗИЧНО ВІДДІЛЕНІ ПІДМЕРЕЖІ**
	[Вилучено: включено до SC-7]].

SC-7(2)	**ЗАХИСТ ПЕРИМЕТРА - ПУБЛІЧНИЙ ДОСТУП**
	[Вилучено: включено до SC-7]].

SC-7(3)	**ЗАХИСТ ПЕРИМЕТРА - ТОЧКИ ДОСТУПУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-07(03)	обмежена кількість зовнішніх мережевих підключень до системи.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту відмови у наданні послуги; проєктна документація системи; документація засобів і методів моніторингу системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який відповідає за	

	виявлення та моніторинг]. **Перевірка:** [ВИБІР: Автоматизовані механізми, інструменти, що реалізують моніторинг системи для атак відмови в обслуговуванні].

SC-7(4)	**ЗАХИСТ ПЕРИМЕТРА - ЗОВНІШНІ КОМУНІКАЦІЙНІ СЛУЖБИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-07(04)_ODP	**визначено періодичність перегляду винятків з політики управління інформаційними потоками;**
	SC-07(04)(a)	реалізовано керований інтерфейс для кожної зовнішньої телекомунікаційної послуги;
	SC-07(04)(b)	встановлена політика потоку трафіку для кожного керованого інтерфейсу;
	SC-07(04)(c)[01]	захищена конфіденційність інформації, що передається через кожен інтерфейс;
	SC-07(04)(c)[02]	захищена цілісність інформації, що передається через кожен інтерфейс;
	SC-07(04)(d)	задокументовано кожен виняток з політики управління трафіком з обґрунтуванням місії або бізнес-потреби, а також тривалості такої потреби;
	SC-07(04)(e)[01]	переглядаються винятки з політики потоку трафіку **<SC-07(04)_ODP частота>**;
	SC-07(04)(e)[02]	потрібно видалити винятки з політики потоку трафіку, які більше не підтримуються чітко визначеною місією або бізнес-потребою;
	SC-07(04)(f)	запобігається несанкціонований обмін трафіком плану управління із зовнішніми мережами;
	SC-07(04)(g)	публікується інформація, яка дозволяє віддаленим мережам виявляти несанкціонований трафік площини керування з внутрішніх мереж;
	SC-07(04)(h)	фільтрується несанкціонований трафік з зовнішніх мереж.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту відмови у наданні послуги; проєктна документація системи; документація засобів і методів моніторингу системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який відповідає за виявлення та моніторинг]. **Перевірка:** [ВИБІР: Автоматизовані механізми, інструменти, що реалізують	

	моніторинг системи для атак відмови в обслуговуванні].

SC-7(5)	**ЗАХИСТ ПЕРИМЕТРА - ВІДМОВА ЗА ЗАМОВЧУВАННЯМ - ДОЗВІЛ ЗА ВИНЯТКОМ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-07(05)_ODP[01]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {на керованих інтерфейсах; для систем <SC-07(05)_ODP[02]>};**
	SC-07(05)_ODP[02]	**визначено системи, для яких трафік мережевого зв'язку заборонено за замовчуванням, а трафік мережевого зв'язку дозволено як виняток (якщо вибрано).**
	SC-07(05)[01]	заборонено мережевий комунікаційний трафік за замовчуванням **<SC-07(05)_ODP[01] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(S)>**;
	SC-07(05)[02]	дозволено мережевий комунікаційний трафік за винятком **<SC-07(05)_ODP[01] ВИБРАНЕ ЗНАЧЕННЯ(Я) ПАРАМЕТРА(ів)>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту відмови у наданні послуги; проєктна документація системи; документація засобів і методів моніторингу системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який відповідає за виявлення та моніторинг]. **Перевірка:** [ВИБІР: Автоматизовані механізми, інструменти, що реалізують моніторинг системи для атак відмови в обслуговуванні].	

SC-7(6)	**ЗАХИСТ ПЕРИМЕТРА - ВІДПОВІДЬ НА РОЗПІЗНАНІ ПОМИЛКИ**
	[Вилучено: включено до SC-7(18)].

SC-7(7)	**ЗАХИСТ ПЕРИМЕТРА - ЗАПОБІГАННЯ ПОДІЛУ ТУНЕЛЮВАННЯ ДЛЯ ВІДДАЛЕНИХ ПРИСТРОЇВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-07(07)_ODP	**визначені гарантії безпечного прокладання розділеному тунелюванню;**
	SC-07(07)	запобігається розділеному тунелюванню для віддалених пристроїв, що підключаються до систем організації, якщо

		розділене тунелюванню не захищено за допомогою **<SC-07(07)_ODP засоби захисту>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту периметра; проєктна документація системи; апаратне та програмне забезпечення системи; архітектура системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; розробник системи; персонал організації з обов'язками щодо захисту периметра]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують можливості захисту периметра; автоматизовані механізми, що підтримують, обмежують віддалені з'єднання].	

SC-7(8)	**ЗАХИСТ ПЕРИМЕТРА -- МАРШРУТИЗАЦІЯ ТРАФІКУ З АВТЕНТИФІКОВАНИХ ПРОКСІ-СЕРВЕРІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-07(08)_ODP[01]	**визначено внутрішній комунікаційний трафік для маршрутизації до зовнішніх мереж;**
	SC-07(08)_ODP[02]	**визначені зовнішні мережі, до яких має бути спрямований внутрішній комунікаційний трафік;**
	SC-07(08)	**<SC-07(08) _ODP[01] внутрішній комунікаційний трафік>** спрямовується до **<SC-07(08) _ODP[02] зовнішніх мереж>** через автентифіковані проксі-сервери на керованих інтерфейсах.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту периметра; проєктна документація системи; апаратне та програмне забезпечення системи; архітектура системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: адміністратори системи, мережі; персонал організації, відповідальний за інформаційну безпеку; розробник системи; персонал організації з обов'язками щодо захисту периметра]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують можливість захисту периметра; автоматизовані механізми, що реалізують виявлення та заперечення загрози вихідному комунікаційному трафіку; автоматизовані механізми, що реалізують аудит вихідного комунікаційного трафіку].	

SC-7(9)	**ЗАХИСТ ПЕРИМЕТРА - ОБМЕЖЕННЯ ТРАФІКУ ВИХІДНИХ**

	ПОВІДОМЛЕНЬ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-07(09)(a)[01]	виявлено вихідний комунікаційний трафік, що становить загрозу для зовнішніх систем;
	SC-07(09)(a)[02]	заборонено вихідний комунікаційний трафік, що становить загрозу для зовнішніх систем;
	SC-07(09)(b)	перевіряється ідентичність внутрішніх користувачів, пов'язаних з відмовою у зв’язку.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту периметра; проєктна документація системи; апаратне та програмне забезпечення системи; архітектура системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: адміністратори системи, мережі; персонал організації, відповідальний за інформаційну безпеку; розробник системи; персонал організації з обов'язками щодо захисту периметра]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують можливість захисту периметра; автоматизовані механізми, що реалізують виявлення та запереченння загрози вихідному комунікаційному трафіку; автоматизовані механізми, що реалізують аудит вихідного комунікаційного трафіку].	

SC-7(10)	**ЗАХИСТ ПЕРИМЕТРА - ЗАПОБІГАННЯ ЕКСФІЛЬТРАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-07(10)_ODP	**визначена періодичність проведення тестів на ексфільтрацію;**
	SC-07(09)(a)[02]	вдалося запобігти витоку інформації;
	SC-07(09)(b)	проводяться випробування на ексфільтрацію **<SC-07(10)_ODP періодичність >**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту периметра; проєктна документація системи; апаратне та програмне забезпечення системи; архітектура системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: адміністратори системи, мережі; персонал організації, відповідальний за інформаційну безпеку; розробник системи; персонал організації з обов'язками щодо захисту периметра].	

	Перевірка: [ВИБІР: Автоматизовані механізми, що реалізують можливість захисту периметра; автоматизовані механізми, що реалізують виявлення та запереченння загрози вихідному комунікаційному трафіку; автоматизовані механізми, що реалізують аудит вихідного комунікаційного трафіку].

SC-7(11)	**ЗАХИСТ ПЕРИМЕТРА - ОБМЕЖЕННЯ ТРАФІКУ ВХІДНИХ ПОВІДОМЛЕНЬ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-07(11)_ODP[01]	**визначені авторизовані джерела вхідних повідомлень для маршрутизації;**
	SC-07(11)_ODP[02]	**визначено авторизовані пункти призначення, до яких можна перенаправляти вхідні повідомлення від авторизованих джерел;**
	SC-07(11)	дозволено направляти лише вхідні повідомлення від **<SC-07(11) _ODP[01] авторизованих джерел>** до **<SC-07(11) _ODP[02] авторизованих пунктів призначення>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту периметра; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, відповідальний за інформаційну безпеку; розробник системи; персонал організації з обов'язками щодо захисту периметра]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують можливості захисту меж щодо пар адрес джерела, призначення].	

SC-7(12)	**ЗАХИСТ ПЕРИМЕТРА - ЗАХИСТ НА ОСНОВІ ХОСТУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-07(12)_ODP[01]	**визначені механізми захисту захисту периметру на основі хосту, які мають бути впроваджені;**
	SC-07(12)_ODP[02]	**визначені компоненти системи, в яких мають бути впроваджені механізми захисту захисту периметру на основі хосту;**
	SC-07(12)	реалізовано **<SC-07(12) _ODP[01] механізми захисту захисту периметру на основі хосту>** на **<SC-07(12) _ODP[02] системних компонентах>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ:	

	Дослідження: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту периметра; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, відповідальний за інформаційну безпеку; розробник системи; персонал організації з обов'язками щодо захисту периметра]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують можливості захисту меж щодо пар адрес джерела, призначення].

SC-7(13)	**ЗАХИСТ ПЕРИМЕТРА - ІЗОЛЯЦІЯ ЗАСОБІВ БЕЗПЕКИ, МЕХАНІЗМІВ І КОМПОНЕНТІВ ПІДТРИМКИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-07(13)_ODP	**визначені інструменти, механізми та компоненти підтримки інформаційної безпеки, які мають бути ізольовані від інших внутрішніх компонентів системи**
	SC-07(13)	ізольовані **<SC-07(13)_ODP засоби, механізми та компоненти підтримки інформаційної безпеки>** від інших внутрішніх компонентів системи шляхом впровадження фізично відокремлених підмереж з керованими інтерфейсами до інших компонентів системи.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту периметра; проєктна документація системи; апаратне та програмне забезпечення системи; архітектура системи; налаштування конфігурації системи та відповідна документація; перелік засобів безпеки та компонентів підтримки, які слід ізолювати від інших компонентів внутрішньої системи; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, відповідальний за інформаційну безпеку; персонал організації з обов'язками щодо охорони кордонів]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують ізоляцію інструментів, механізмів та компонентів інформаційної безпеки].	

SC-7(14)	**ЗАХИСТ ПЕРИМЕТРА - ЗАХИСТ ВІД НЕСАНКЦІОНОВАНИХ ФІЗИЧНИХ З'ЄДНАНЬ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-07(14)_ODP	**визначено керовані інтерфейси, які потрібно захистити від несанкціонованих фізичних з'єднань;**

	SC-07(14)	захищені **<SC-07(14)_ODP керовані інтерфейси>** від несанкціонованих фізичних підключень
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту периметра; проєктна документація системи; апаратне та програмне забезпечення системи; архітектура системи; налаштування конфігурації системи та відповідна документація; перелік засобів безпеки та компонентів підтримки, які слід ізолювати від інших компонентів внутрішньої системи; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, відповідальний за інформаційну безпеку; персонал організації з обов'язками щодо охорони кордонів]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують ізоляцію інструментів, механізмів та компонентів інформаційної безпеки].	

SC-7(15)	**ЗАХИСТ ПЕРИМЕТРА - МАРШРУТИЗАЦІЯ ДОСТУПУ ДО ПРИВІЛЕЙОВАНОЇ МЕРЕЖІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-07(15)[01]	мережеві привілейовані доступи маршрутизуються через спеціальний керований інтерфейс з метою контролю доступу;
	SC-07(15)[02]	мережеві привілейовані доступи маршрутизуються через спеціальний керований інтерфейс для цілей аудиту.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту периметра; проєктна документація системи; апаратне та програмне забезпечення системи; архітектура системи; налаштування конфігурації системи та відповідна документація; перелік засобів безпеки та компонентів підтримки, які слід ізолювати від інших компонентів внутрішньої системи; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, відповідальний за інформаційну безпеку; персонал організації з обов'язками щодо охорони кордонів]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують ізоляцію інструментів, механізмів та компонентів інформаційної безпеки].	

SC-7(16)	**ЗАХИСТ ПЕРИМЕТРА - ЗАПОБІГАННЯ ВИЯВЛЕННЮ КОМПОНЕНТІВ І ПРИСТРОЇВ**
	МЕТА ОЦІНКИ:

	Визначити, чи:	
	SC-07(16)	запобігається виявлення певних компонентів системи, які представляють керований інтерфейс.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту периметра; проєктна документація системи; апаратне та програмне забезпечення системи; архітектура системи; налаштування конфігурації системи та відповідна документація; перелік засобів безпеки та компонентів підтримки, які слід ізолювати від інших компонентів внутрішньої системи; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, відповідальний за інформаційну безпеку; персонал організації з обов'язками щодо охорони кордонів]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують ізоляцію інструментів, механізмів та компонентів інформаційної безпеки].	

SC-7(17)	**ЗАХИСТ ПЕРИМЕТРА - АВТОМАТИЧНЕ ПРИМУСОВЕ ВИКОНАННЯ ФОРМАТІВ ПРОТОКОЛІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-07(17)	дотримуються форматів протоколів.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту периметра; проєктна документація системи; апаратне та програмне забезпечення системи; архітектура системи; налаштування конфігурації системи та відповідна документація; перелік засобів безпеки та компонентів підтримки, які слід ізолювати від інших компонентів внутрішньої системи; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, відповідальний за інформаційну безпеку; персонал організації з обов'язками щодо охорони кордонів]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують ізоляцію інструментів, механізмів та компонентів інформаційної безпеки].	

SC-7(18)	**ЗАХИСТ ПЕРИМЕТРА - ЗБІЙ У БЕЗПЕЦІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-07(18)	запобігають входу систем у незахищені стани в разі

		аварійного завершення роботи пристрою захисту периметра.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту периметра; проєктна документація системи; апаратне та програмне забезпечення системи; архітектура системи; налаштування конфігурації системи та відповідна документація; перелік засобів безпеки та компонентів підтримки, які слід ізолювати від інших компонентів внутрішньої системи; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, відповідальний за інформаційну безпеку; персонал організації з обов'язками щодо охорони кордонів]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують ізоляцію інструментів, механізмів та компонентів інформаційної безпеки].	

SC-7(19)	**ЗАХИСТ ПЕРИМЕТРА - БЛОКУВАННЯ КОМУНІКАЦІЇ ВІД ХОСТІВ, ЩО НАЛАШТОВАНІ ПОЗА ОРГАНІЗАЦІЄЮ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-07(19)_ODP	**заборонено системам переходити в небезпечні стани в разі операційної відмови пристрою захисту периметру.**
	SC-07(19)[01]	блокується вхідний комунікаційний трафік між **<SC-07(19)_ODP клієнтами зв'язку>**, які незалежно налаштовані кінцевими користувачами та зовнішніми постачальниками послуг;
	SC-07(19)[02]	блокується вихідний комунікаційний трафік між **<SC-07(19)_ODP клієнтами зв'язку>**, які незалежно налаштовані кінцевими користувачами та зовнішніми постачальниками послуг.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР:Політика захисту системи та комунікацій; процедури, що стосуються захисту периметра; проєктна документація системи; апаратне та програмне забезпечення системи; архітектура системи; налаштування конфігурації системи та відповідна документація; перелік клієнтів зв'язку, які самостійно налаштовуються кінцевими користувачами та зовнішніми постачальниками послуг; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, відповідальний за інформаційну безпеку; персонал організації з обов'язками щодо захисту периметра]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують блокування вхідного та вихідного комунікаційного трафіку між клієнтами зв'язку, незалежно налаштованими кінцевими користувачами та	

	зовнішніми постачальниками послуг].

SC-7(20)	**ЗАХИСТ ПЕРИМЕТРА - ДИНАМІЧНА ІЗОЛЯЦІЯ ТА ВІДОКРЕМЛЕННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-07(20)_ODP	**визначено компоненти системи, які мають бути динамічно ізольовані від інших компонентів системи;**
	SC-07(20)	передбачено можливість динамічної ізоляції **<SC-07(20)_ODP системних компонентів>** від інших системних компонентів.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР:Політика захисту системи та комунікацій; процедури, що стосуються захисту периметра; проєктна документація системи; апаратне та програмне забезпечення системи; архітектура системи; налаштування конфігурації системи та відповідна документація; перелік клієнтів зв'язку, які самостійно налаштовуються кінцевими користувачами та зовнішніми постачальниками послуг; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, відповідальний за інформаційну безпеку; персонал організації з обов'язками щодо захисту периметра]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують блокування вхідного та вихідного комунікаційного трафіку між клієнтами зв'язку, незалежно налаштованими кінцевими користувачами та зовнішніми постачальниками послуг].	

SC-7(21)	**ЗАХИСТ ПЕРИМЕТРА - ІЗОЛЯЦІЯ СИСТЕМНИХ КОМПОНЕНТІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-07(21)_ODP[01]	**визначені компоненти системи, які мають бути ізольовані механізмами захисту периметра;**
	SC-07(21)_ODP[02]	**визначені місії та/або бізнес-функції, які повинні підтримуватися компонентами системи, ізольованими механізмами захисту периметра;**
	SC-07(21)	застосовуються механізми захисту кордонів для ізоляції **<SC-07(21)_ODP[01] системних компонентів>**, що підтримують **<SC-07(21)_ODP[02] місії та/або бізнес-функції>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР:Політика захисту системи та комунікацій; процедури, що стосуються захисту периметра; проєктна документація системи; апаратне та програмне забезпечення системи; архітектура системи; налаштування конфігурації системи та відповідна документація; перелік клієнтів зв'язку, які	

	самостійно налаштовуються кінцевими користувачами та зовнішніми постачальниками послуг; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, відповідальний за інформаційну безпеку; персонал організації з обов'язками щодо захисту периметра]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують блокування вхідного та вихідного комунікаційного трафіку між клієнтами зв'язку, незалежно налаштованими кінцевими користувачами та зовнішніми постачальниками послуг].

SC-7(22)	**ЗАХИСТ ПЕРИМЕТРА - ОКРЕМІ ПІДМЕРЕЖІ ДЛЯ ПІДКЛЮЧЕННЯ ДО РІЗНИХ ДОМЕНІВ БЕЗПЕКИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-07(22)	реалізовано окремі мережеві адреси для підключення до систем у різних доменах безпеки.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР:Політика захисту системи та комунікацій; процедури, що стосуються захисту периметра; проєктна документація системи; апаратне та програмне забезпечення системи; архітектура системи; налаштування конфігурації системи та відповідна документація; перелік клієнтів зв'язку, які самостійно налаштовуються кінцевими користувачами та зовнішніми постачальниками послуг; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, відповідальний за інформаційну безпеку; персонал організації з обов'язками щодо захисту периметра]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують блокування вхідного та вихідного комунікаційного трафіку між клієнтами зв'язку, незалежно налаштованими кінцевими користувачами та зовнішніми постачальниками послуг].	

SC-7(23)	**ЗАХИСТ ПЕРИМЕТРА - ВІДКЛЮЧЕННЯ ФУНКЦІЇ ЗВОРОТНОГО ЗВ'ЯЗКУ ВІДПРАВНИКА ПРО ПОМИЛКУ ПЕРЕВІРКИ ПРОТОКОЛУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-07(23)	вимкнено зворотній зв'язок з відправниками у разі помилки перевірки формату протоколу.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту периметра; проєктна документація системи; апаратне та	

	програмне забезпечення системи; архітектура системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, відповідальний за інформаційну безпеку; розробник системи; персонал організації з обов'язками щодо захисту периметра]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують відключення зворотного зв’язку відправникам про помилку перевірки формату протоколу].

SC-7(24)	**ЗАХИСТ ПЕРИМЕТРА - ПЕРСОНАЛЬНІ ДАНІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-07(24)_ODP	**визначені правила обробки для систем, які обробляють персональну дані;**
	SC-07(24)(a)	застосовуються **<SC-07(24)_ODP правила обробки>** до персональних даних в системах, які обробляють інформацію, що ідентифікує особу;
	SC-07(24)(b)[01]	здійснюється моніторинг дозволеної обробки на зовнішніх інтерфейсах до систем, які обробляють персональні дані;
	SC-07(24)(b)[02]	здійснюється моніторинг дозволеної обробки на ключових внутрішніх кордонах систем, які обробляють персональні дані;
	SC-07(24)(c)	задокументовано кожен виняток для систем, які обробляють персональні дані;
	SC-07(24)(d)[01]	переглядаються винятки для систем, які обробляють персональні дані;
	SC-07(24)(d)[02]	вилучено винятки для систем, які обробляють персональні дані.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту периметра; проєктна документація системи; апаратне та програмне забезпечення системи; архітектура системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, відповідальний за інформаційну безпеку; розробник системи; персонал організації з обов'язками щодо захисту периметра]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують відключення зворотного зв’язку відправникам про помилку перевірки формату протоколу].	

SC-7(25)	**ЗАХИСТ ПЕРИМЕТРА - ЗЄДНАННЯ З НЕСЕКРЕТНИМИ НАЦІОНАЛЬНИМИ СИСТЕМАМИ БЕЗПЕКИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-07(25)_ODP[01]	**визначена несекретна національна система безпеки, якій заборонено пряме підключення до зовнішньої мережі;**
	SC-07(25)_ODP[02]	**визначено пристрій граничного захисту, необхідний для прямого підключення до зовнішньої мережі;**
	SC-07(25)	підмережі розділені **<SC-07(29)_ODP[01] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА>**, щоб ізолювати **<SC-07(29)_ODP[02] критичні компоненти та функції системи>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту кордонів; проектна документація системи; апаратне та програмне забезпечення системи; архітектура системи; налаштування конфігурації системи та відповідна документація; аналіз критичності; записи аудиту системи; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Системні/мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробник системи; персонал організації, відповідальний за захист кордонів]. **Перевірка:** [ВИБІР: Механізми, що розділяють критичні компоненти та функції системи].	

SC-7(26)	**ЗАХИСТ ПЕРИМЕТРА - ЗЄДНАННЯ З СЕКРЕТНИМИ НАЦІОНАЛЬНИМИ СИСТЕМАМИ БЕЗПЕКИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-07(26)_ODP	**визначено пристрій граничного захисту, необхідний для прямого підключення до зовнішньої мережі;**
	SC-07(26)	заборонено пряме підключення секретної системи національної безпеки до зовнішньої мережі без використання **<SC-07(26)_ODP пристрій захисту перимтеру>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту кордонів; проектна документація системи; апаратне та програмне забезпечення системи; архітектура системи; налаштування конфігурації системи та відповідна документація; аналіз критичності; записи аудиту системи; план захисту інформації системи; інші відповідні документи або записи].	

	Співбесіда: [ВИБІР: Системні/мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробник системи; персонал організації, відповідальний за захист кордонів]. **Перевірка:** [ВИБІР: Механізми, що розділяють критичні компоненти та функції системи].

SC-7(27)	**ЗАХИСТ ПЕРИМЕТРА - ЗЄДНАННЯ З СЕКРЕТНИМИ НЕ НАЦІОНАЛЬНИМИ СИСТЕМАМИ БЕЗПЕКИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-07(27)_ODP[01]	**визначена несекретна, недержавна система безпеки, якій заборонено пряме підключення до зовнішньої мережі;**
	SC-07(27)_ODP[02]	**визначено пристрій прикордонного захисту, необхідний для прямого підключення несекретної, недержавної системи безпеки до зовнішньої мережі;**
	SC-07(27)	заборонено пряме підключення **<SC-07(27) _ODP[01] несекретної недержавної системи безпеки>** до зовнішньої мережі без використання **<SC-07(27) _ODP[02] прикордонного захисного пристрою>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту кордонів; проектна документація системи; апаратне та програмне забезпечення системи; архітектура системи; налаштування конфігурації системи та відповідна документація; аналіз критичності; записи аудиту системи; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Системні/мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробник системи; персонал організації, відповідальний за захист кордонів]. **Перевірка:** [ВИБІР: Механізми, що розділяють критичні компоненти та функції системи].	

SC-7(28)	**ЗАХИСТ ПЕРИМЕТРА - ЗЄДНАННЯ З ЗАГАЛЬНОДОСТУПНИМИ МЕРЕЖАМИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-07(28)_ODP	**визначено систему, якій заборонено пряме підключення до загальнодоступної мережі;**
	SC-07(28)	заборонено пряме підключення **<SC-07(28)_ODP системи>** до загальнодоступної мережі.

	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту кордонів; проектна документація системи; апаратне та програмне забезпечення системи; архітектура системи; налаштування конфігурації системи та відповідна документація; аналіз критичності; записи аудиту системи; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Системні/мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробник системи; персонал організації, відповідальний за захист кордонів]. **Перевірка:** [ВИБІР: Механізми, що розділяють критичні компоненти та функції системи].

SC-7(29)	**ЗАХИСТ ПЕРИМЕТРА - ОКРЕМІ ПІДМЕРЕЖІ ДЛЯ ІЗОЛЯЦІЇ ФУНКЦІЙ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-07(29)_ODP[01]	**вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {фізично; логічно};**
	SC-07(29)_ODP[02]	визначені критичні компоненти системи та функції, що підлягають ізоляції;
	SC-07(29)	підмережі розділені **<SC-07(29) _ODP[01] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>** для ізоляції **<SC-07(29) _ODP[02] критично важливих компонентів і функцій системи>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту кордонів; проектна документація системи; апаратне та програмне забезпечення системи; архітектура системи; налаштування конфігурації системи та відповідна документація; аналіз критичності; записи аудиту системи; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Системні/мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробник системи; персонал організації, відповідальний за захист кордонів]. **Перевірка:** [ВИБІР: Механізми, що розділяють критичні компоненти та функції системи].	

SC-8	**КОНФІДЕНЦІЙНІСТЬ ТА ЦІЛІСНІСТЬ ПЕРЕДАЧІ**
	МЕТА ОЦІНКИ: Визначити, чи:

	SC-07(29)_ODP[01]	**вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {фізично; логічно};**
	SC-07(29)_ODP[02]	визначені критичні компоненти системи та функції, що підлягають ізоляції;
	SC-07(29)	підмережі розділені **<SC-07(29) _ODP[01] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>** для ізоляції **<SC-07(29) _ODP[02] критично важливих компонентів і функцій системи>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються конфіденційності та цілісності передачі; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, відповідальний за інформаційну безпеку; розробник системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують конфіденційність та, або цілісність передачі].	

SC-8(1)	**КОНФІДЕНЦІЙНІСТЬ ТА ЦІЛІСНІСТЬ ПЕРЕДАЧІ - КРИПТОГРАФІЧНИЙ ЗАХИСТ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-08(01)_ODP	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {запобігти несанкціонованому розголошенню інформації; виявити зміни в інформації};**
	SC-08(01)	застосовуються механізми криптографічного захисту до <**SC-08(01)_ODP ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(S)>** під час передавання.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються конфіденційності та цілісності передачі; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, відповідальний за інформаційну безпеку; розробник системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують конфіденційність та, або цілісність передачі].	

SC-8(2)	**КОНФІДЕНЦІЙНІСТЬ ТА ЦІЛІСНІСТЬ ПЕРЕДАЧІ - ПОПЕРЕДНЯ І ПОСТОБРОБКА**

	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-08(02)_ODP	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {конфіденційність; цілісність};**
	SC-08(02)[01]	зберігається інформація **<SC-08(02) _ODP ВИБІРКОВЕ ЗНАЧЕННЯ(Я) ПАРАМЕТРА(ів) >** під час підготовки до передачі;
	SC-08(02)[02]	зберігається інформація **<SC-08(02) _ODP ВИБІРКОВЕ ЗНАЧЕННЯ(Я) ПАРАМЕТРА(ів) >** під час приймання.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються конфіденційності та цілісності передачі; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, відповідальний за інформаційну безпеку; розробник системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують конфіденційність та, або цілісність передачі].	

SC-8(3)	**КОНФІДЕНЦІЙНІСТЬ ТА ЦІЛІСНІСТЬ ПЕРЕДАЧІ - КРИПТОГРАФІЧНИЙ ЗАХИСТ ПОВІДОМЛЕНЬ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-08(03)_ODP	**визначено альтернативні фізичні засоби контролю для захисту зовнішніх повідомлень;**
	SC-08(03)	впроваджено криптографічні механізми для захисту зовнішніх повідомлень, якщо інше не захищено **<SC-08(03)_ODP альтернативні фізичні засоби контролю>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються конфіденційності та цілісності передачі; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, відповідальний за інформаційну безпеку; розробник системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують конфіденційність та, або цілісність передачі].	

SC-8(4)	**КОНФІДЕНЦІЙНІСТЬ ТА ЦІЛІСНІСТЬ ПЕРЕДАЧІ - ПРИХОВУВАННЯ АБО РАНДОМІЗАЦІЯ КОМУНІКАЦІЇ**

	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-08(04)_ODP	**визначені альтернативні фізичні засоби контролю для захисту від несанкціонованого розкриття шаблонів комунікації;**
	SC-08(04)	застосовуються криптографічні механізми для приховування або рандомізації шаблонів комунікації, якщо інше не захищено **<SC-08(04)_ODP альтернативні фізичні засоби контролю>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються конфіденційності та цілісності передачі; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, відповідальний за інформаційну безпеку; розробник системи]. **Перевірка:** [ВИБІР: Криптографічні механізми, що підтримують та, або реалізують приховування або рандомізацію шаблонів зв'язку; автоматизовані механізми, що підтримують та, або впроваджують альтернативні фізичні запобіжні заходи; організаційні процеси для визначення та впровадження альтернативних фізичних гарантій].	

SC-8(5)	**КОНФІДЕНЦІЙНІСТЬ ТА ЦІЛІСНІСТЬ ПЕРЕДАЧІ - ЗАХИЩЕНА СИСТЕМА РОЗПОДІЛУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-08(05)_ODP[01]	**визначено захищену систему розподілу;**
	SC-08(05)_ODP[02]	вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {запобігти несанкціонованому розголошенню інформації; виявити зміни в інформації};
	SC-08(05)	реалізовано **<SC-08(05) _ODP[01] захищену систему розподілу>** до **<SC-08(05) _ODP[02] ВИБІРКОВОГО ЗНАЧЕННЯ ПАРАМЕТРА(ів)**> під час передавання.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються конфіденційності та цілісності передачі даних; проектна документація системи; налаштування конфігурації системи та пов'язана з нею документація; записи аудиту системи; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Системні/мережеві адміністратори; персонал організації,	

	відповідальний за інформаційну безпеку; розробник системи]. **Перевірка:** [ВИБІР: Криптографічні механізми, що підтримують та/або реалізують приховування або рандомізацію шаблонів зв'язку; механізми, що підтримують та/або реалізують захищені системи розподілу].

SC-9	**КОНФІДЕНЦІЙНІСТЬ ПЕРЕДАЧІ**
	[Вилучено: включено до SC-8].

SC-10	**ВІДКЛЮЧЕННЯ МЕРЕЖІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-10_ODP	**визначено період бездіяльності, після якого система розриває мережеве з'єднання, пов'язане з сеансом зв'язку;**
	SC-08(05)_ODP[02]	мережеве з'єднання, пов'язане з сеансом зв'язку, розірвано в кінці сеансу або після **<SC-10_ODP період часу>** бездіяльності.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБЕРІТЬ З: політика захисту системи та комунікацій; процедури розв'язання проблеми відключення мережі; проєктна документація системи; план захисту інформації; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, відповідальний за інформаційну безпеку; розробник системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують можливість відключення мережі].	

SC-11	**ДОВІРЕНИЙ КАНАЛ ЗВ'ЯЗКУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-11_ODP[01]	**вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {фізично; логічно};**
	SC-11_ODP[02]	**визначені функції безпеки системи;**
	SC-11a.	передбачено **<SC-11_ODP[01] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>** ізольований надійний канал зв'язку для комунікацій між користувачем та довіреними компонентами системи;
	SC-11b.	дозволено користувачам звертатися до надійного каналу зв'язку для зв'язку між користувачем та **<SC-11_ODP[02] функціями безпеки>** системи, включаючи, як мінімум,

		автентифікацію та повторну автентифікацію.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБЕРІТЬ З: політика захисту системи та комунікацій; процедури розв'язання проблеми відключення мережі; проєктна документація системи; план захисту інформації; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, відповідальний за інформаційну безпеку; розробник системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують можливість відключення мережі].	

SC-11(1)	**ДОВІРЕНИЙ КАНАЛ ЗВ'ЯЗКУ - ЛОГІЧНА ІЗОЛЯЦІЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-11(01)_ODP	**визначені функції безпеки системи;**
	SC-11(01)(a)	надається надійний канал зв'язку, який можна беззаперечно відрізнити від інших каналів зв'язку;
	SC-11(01)(b)	ініційовано довірений канал зв'язку для комунікацій між **<SC-11(01)_ODP функції безпеки>** системи та користувачем.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються надійних шляхів зв'язку; план захисту інформації; проєктна документація системи; налаштування конфігурації системи та відповідна документація; результати оцінки незалежними випробувальними організаціями; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, відповідальний за інформаційну безпеку; розробник системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують довірені шляхи зв'язку].	

SC-12	**ВСТАНОВЛЕННЯ ТА УПРАВЛІННЯ КРИПТОГРАФІЧНИМИ КЛЮЧАМИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-12_ODP	**визначені вимоги до генерації, розповсюдження, зберігання, доступу та знищення ключів;**
	SC-12[01]	встановлюються криптографічні ключі, коли в системі використовується криптографія відповідно до **< SC-12_ODP**

		вимог >;
	SC-12[02]	здійснюється управління криптографічними ключами, коли в системі використовується криптографія, відповідно до **<SC-12_ODP вимог >**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються встановлення та управління криптографічним ключем; проєктна документація системи; криптографічні механізми; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, відповідальний за інформаційну безпеку; персонал організації, відповідальний за встановлення та, або управління криптографічним ключем]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують встановлення та управління криптографічним ключем].	

SC-12(1)	**ВСТАНОВЛЕННЯ ТА УПРАВЛІННЯ КРИПТОГРАФІЧНИМИ КЛЮЧАМИ - ДОСТУПНІСТЬ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-12(01)	зберігається доступність інформації у випадку втрати криптографічних ключів користувачами.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються встановлення, управління та відновлення криптографічного ключа; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, відповідальний за інформаційну безпеку; персонал організації, відповідальний за створення та управління криптографічним ключем]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують встановлення та управління криптографічним ключем].	

SC-12(2)	**ВСТАНОВЛЕННЯ ТА УПРАВЛІННЯ КРИПТОГРАФІЧНИМИ КЛЮЧАМИ - СИМЕТРИЧНІ КЛЮЧІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-12(02)_ODP	**вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {підтверджено; схвалено};**

	SC-12(02)[01]	симетричні криптографічні ключі виробляються з використанням технології та процесів управління ключами <**SC-12(02)_ODP ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА>**;
	SC-12(02)[02]	симетричні криптографічні ключі контролюються за допомогою технології та процесів управління ключами **<SC-12(02)_ODP ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА>**;
	SC-12(02)[03]	симетричні криптографічні ключі розподіляються з використанням технології та процесів управління ключами **<SC-12(02)_ODP ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються встановлення та управління криптографічним ключем; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; перелік криптографічних продуктів, підтверджених уповноваженим органом; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, відповідальний за інформаційну безпеку; розробник системи; персонал організації, відповідальний за створення та управління криптографічним ключем]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують симетричне встановлення та управління криптографічним ключем].	

SC-12(3)	**ВСТАНОВЛЕННЯ ТА УПРАВЛІННЯ КРИПТОГРАФІЧНИМИ КЛЮЧАМИ - АСИМЕТРИЧНІ КЛЮЧІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-12(03)_ODP	**вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {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 вимо};**
	SC-12(03)[01]	створюються асиметричні криптографічні ключі за допомогою **<SC-12(03)_ODP ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>**;
	SC-12(03)[02]	контролюються асиметричні криптографічні ключі за допомогою **<SC-12(03)_ODP ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>**;
	SC-12(03)[03]	розподіляються асиметричні криптографічні ключі за допомогою **<SC-12(03)_ODP ВИБРАНЕ ЗНАЧЕННЯ**

		ПАРАМЕТРА>.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються встановлення та управління криптографічним ключем; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; перелік криптографічних продуктів, затверджених уповноваженим органом; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, відповідальний за інформаційну безпеку; розробник системи; персонал організації, відповідальний за створення та управління криптографічним ключем; персонал організації, відповідальний за сертифікати відкритих ключів]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують асиметричне встановлення та управління криптографічним ключем].	

SC-12(4)	**ВСТАНОВЛЕННЯ ТА УПРАВЛІННЯ КРИПТОГРАФІЧНИМИ КЛЮЧАМИ - СЕРТИФІКАТИ PKI**
	[Вилучено: включено до SC-12 (3)].

SC-12(5)	**ВСТАНОВЛЕННЯ ТА УПРАВЛІННЯ КРИПТОГРАФІЧНИМИ КЛЮЧАМИ - СЕРТИФІКАТИ PKI, АПАРАТНІ ТОКЕНИ**
	[Вилучено: включено до SC-12 (3)].

SC-12(6)	**ВСТАНОВЛЕННЯ ТА УПРАВЛІННЯ КРИПТОГРАФІЧНИМИ КЛЮЧАМИ - ФІЗИЧНИЙ КОНТРОЛЬ КЛЮЧІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-12(06)	зберігається фізичний контроль над криптографічними ключами, коли інформація, що зберігається, шифрується зовнішніми постачальниками послуг.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту кордонів; проектна документація системи; апаратне та програмне забезпечення системи; архітектура системи; налаштування конфігурації системи та відповідна документація; аналіз критичності; записи аудиту системи; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Системні/мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; розробник системи; персонал організації, відповідальний за захист кордонів]. **Перевірка:** [ВИБІР: Механізми, що розділяють критичні компоненти та функції системи].	

SC-13	**КРИПТОГРАФІЧНИЙ ЗАХИСТ**

	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-13_ODP[01]	**визначено використання криптографічних засобів;**
	SC-13_ODP[02]	**визначено типи криптографії для кожного вказаного криптографічного використання;**
	SC-13a.	ідентифіковано **<SC-13_ODP[01] криптографічне використання>**;
	SC-13b.	реалізовано **<SC-13_ODP[02] типи криптографії>** для кожного вказаного криптографічного використання (визначеного в SC-13_ODP[01]).
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються криптографічного захисту; проєктна документація системи; налаштування конфігурації системи та відповідна документація; сертифікати перевірки криптографічного модуля; перелік перевірених криптографічних модулів; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; розробник системи; персонал організації, відповідальний за криптографічний захист]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують криптографічний захист].	

SC-13(1)	**КРИПТОГРАФІЧНИЙ ЗАХИСТ - СТАНДАРТНА КРИПТОГРАФІЯ**
	[Вилучено: включено до SC-13].

SC-13(2)	**КРИПТОГРАФІЧНИЙ ЗАХИСТ - ЗАТВЕРДЖЕНА УПОВНОВАЖЕНИМ ОРГАНОМ КРИПТОГРАФІЯ**
	[Вилучено: включено до SC-13].

SC-13(3)	**КРИПТОГРАФІЧНИЙ ЗАХИСТ - ОСОБИ БЕЗ ОФІЦІЙНИХ ПОВНОВАЖЕНЬ**
	[Вилучено: включено до SC-13].

SC-13(4)	**КРИПТОГРАФІЧНИЙ ЗАХИСТ - ЦИФРОВІ ПІДПИСИ**
	[Вилучено: включено до SC-13].

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**
	МЕТА ОЦІНКИ: Визначити, чи:

	SC-15_ODP	**потрібно визначати винятки, коли потрібно дозволити віддалену активацію;**
	SC-15a.	заборонено віддалену активацію пристроїв і програм для спільних обчислень, окрім **<SC-15_ODP винятків, де віддалена активація має бути дозволена>**;
	SC-15b.	надаються чіткі вказівки щодо використання користувачам, які фізично присутні біля пристроїв.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються спільних обчислень; політика та процедури контролю доступу; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; розробник системи; персонал організації, відповідальний за управління спільними обчислювальними пристроями]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують управління віддаленою активацією спільних обчислювальних пристроїв; автоматизовані механізми, що забезпечують індикацію використання спільних обчислювальних пристроїв].	

SC-15(1)	**СПІЛЬНІ ОБЧИСЛЮВАЛЬНІ ПРИСТРОЇ - ФІЗИЧНЕ ЧИ ЛОГІЧНЕ ВІДКЛЮЧЕННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-15(01)_ODP	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {фізичний; логічний};**
	SC-15(01)	відключення **<SC-15(01) _ODP ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** пристроїв для спільних обчислень забезпечується у спосіб, що підтримує простоту використання.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються спільних обчислень; політика та процедури контролю доступу; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; розробник системи; персонал організації, відповідальний за управління спільними обчислювальними пристроями]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують фізичне відключення спільних обчислювальних пристроїв].	

SC-15(2)	СПІЛЬНІ ОБЧИСЛЮВАЛЬНІ ПРИСТРОЇ - БЛОКУВАННЯ ТРАФІКУ ВХІДНИХ І ВИХІДНИХ ПОВІДОМЛЕНЬ
	[Вилучено: включено до SC-7].

SC-15(3)	СПІЛЬНІ ОБЧИСЛЮВАЛЬНІ ПРИСТРОЇ - ВІДКЛЮЧЕННЯ ТА ВИДАЛЕННЯ В БЕЗПЕЧНИХ РОБОЧИХ ЗОНАХ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-15(03)_ODP[01]	**визначені системи або компоненти системи, з яких мають бути відключенні або видаленні пристрої для спільних обчислень;**
	SC-15(03)_ODP[02]	**визначені безпечні робочі зони, де пристрої для спільних обчислень мають бути відключенні або видаленні з систем чи компонентів системи;**
	SC-15(03)	пристрої та програми для спільних обчислень відключенні або видаленні з **<SC-15(03)_ODP[01] систем або системних компонентів>** в **<SC-15(03)_ODP[02] захищених робочих зонах>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються спільних обчислень; політика та процедури контролю доступу; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; перелік безпечних робочих місць; інформаційні системи або компоненти системи в захищених робочих зонах, де спільні обчислювальні пристрої слід вимкнути або видалити; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, відповідальний за управління спільними обчислювальними пристроями]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують можливість вимкнення спільних обчислювальних пристроїв].	

SC-15(4)	СПІЛЬНІ ОБЧИСЛЮВАЛЬНІ ПРИСТРОЇ - ЧІТКА ІДЕНТИФІКАЦІЯ ПОТОЧНИХ УЧАСНИКІВ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-15(04)_ODP	**є онлайн-зустрічі та конференції, для яких необхідно чітко вказувати поточних учасників, визначеними;**
	SC-15(04)	надається явна вказівка на поточних учасників **<SC-15(04)_ODP онлайн-зустрічей і конференцій>**.

	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються спільних обчислень; політика та процедури контролю доступу; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; перелік видів зустрічей та телеконференцій, що вимагають чіткого зазначення поточних учасників; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, відповідальний за управління спільними обчислювальними пристроями]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують можливість вказувати учасників на спільних обчислювальних пристроях].

SC-16	**ПЕРЕДАЧА АТРИБУТІВ БЕЗПЕКИ ТА ПРИВАТНОСТІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-16_ODP[01]	**визначені атрибути безпеки, які будуть пов'язані з інформацією, що обмінюється;**
	SC-16_ODP[02]	**визначені атрибути приватності, які будуть пов'язані з інформацією, що обмінюється;**
	SC-16[01]	пов'язані **<SC-16_ODP[01] атрибути безпеки>** з інформацією, якою обмінюються системи;
	SC-16[02]	пов'язані **<SC-16_ODP[01] атрибути безпеки>** з інформацією, якою обмінюються компоненти системи;
	SC-16[03]	пов'язані **<SC-16_ODP[02] атрибути приватності**> з інформацією, якою обмінюються системи;
	SC-16[04]	пов'язані **<SC-16_ODP[02] атрибути приватності>** з інформацією, якою обмінюються компоненти системи.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються передачі атрибутів безпеки; політика та процедури контролю доступу; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують передачу атрибутів безпеки між інформаційними системами].	

SC-16(1)	**ПЕРЕДАЧА АТРИБУТІВ БЕЗПЕКИ ТА ПРИВАТНОСТІ - ПЕРЕВІРКА**

	ЦІЛІСНОСТІ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-16_ODP[01]	**визначені атрибути безпеки, які будуть пов'язані з інформацією, що обмінюється;**
	SC-16_ODP[02]	**визначені атрибути приватності, які будуть пов'язані з інформацією, що обмінюється;**
	SC-16[01]	пов'язані **<SC-16_ODP[01] атрибути безпеки>** з інформацією, якою обмінюються системи;
	SC-16[02]	пов'язані **<SC-16_ODP[01] атрибути безпеки>** з інформацією, якою обмінюються компоненти системи;
	SC-16[03]	пов'язані **<SC-16_ODP[02] атрибути приватності>** з інформацією, якою обмінюються системи;
	SC-16[04]	пов'язані **<SC-16_ODP[02] атрибути приватності>** з інформацією, якою обмінюються компоненти системи.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються передачі атрибутів безпеки; політика та процедури контролю доступу; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують перевірку цілісності переданих атрибутів безпеки].	

SC-16(2)	**ПЕРЕДАЧА АТРИБУТІВ БЕЗПЕКИ ТА ПРИВАТНОСТІ - МЕХАНІЗМ АНТИСПУФІНГУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-16(02)	впроваджені механізми боротьби зі спуфінгом, щоб не дозволити зловмисникам фальсифікувати атрибути безпеки, які вказують на успішне застосування процесу захисту.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика захисту системи та комунікацій; процедура передачі атрибутів безпеки та конфіденційності; політика та процедури контролю доступу; проектна документація системи; налаштування конфігурації системи та пов'язана з нею документація; записи аудиту системи; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Системні/мережеві адміністратори; персонал організації,	

	відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Механізми, що підтримують та/або реалізують механізми боротьби зі спуфінгом].

SC-16(3)	**ПЕРЕДАЧА АТРИБУТІВ БЕЗПЕКИ ТА ПРИВАТНОСТІ - КРИПТОГРАФІЧНА ПРИВ'ЯЗКА**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-16(03)_ODP	**визначені механізми або методи прив'язки атрибутів безпеки та приватності до інформації, що передається;**
	SC-16(03)	реалізовані **<SC-16(03)_ODP механізми або методи>** для прив'язки атрибутів безпеки та приватності до інформації, що передається.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика захисту системи та комунікацій; процедура передачі атрибутів безпеки та конфіденційності; політика та процедури контролю доступу; проектна документація системи; налаштування конфігурації системи та пов'язана з нею документація; записи аудиту системи; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Системні/мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Механізми, що підтримують та/або реалізують механізми боротьби зі спуфінгом].	

SC-17	**СЕРТИФІКАТИ ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-17b.	тільки затверджені сертифікати відкритого ключа включені до сховищ довіри або сховищ сертифікатів, якими керує організація.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика захисту системи та комунікацій; процедура передачі атрибутів безпеки та конфіденційності; політика та процедури контролю доступу; проектна документація системи; налаштування конфігурації системи та пов'язана з нею документація; записи аудиту системи; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Системні/мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Механізми, що підтримують та/або реалізують механізми боротьби зі спуфінгом].	

SC-18	МОБІЛЬНИЙ КОД	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-18a.[01]	визначено прийнятний мобільний код;
	SC-18a.[02]	визначено неприйнятний мобільний код;
	SC-18a.[03]	визначені прийнятні технології мобільного кодування;
	SC-18a.[04]	визначені неприйнятні технології мобільного коду;
	SC-18b.[01]	дозволено використання мобільного коду в системі;
	SC-18b.[02]	відстежується використання мобільного коду в системі;
	SC-18b.[03]	контролюється використання мобільного коду в системі.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури адресації мобільного коду; обмеження використання мобільного коду, політика та процедури впровадження мобільного коду; перелік прийнятних мобільних кодів та технологій мобільних кодів; перелік неприйнятних мобільних кодів та мобільних технологій; авторизаційні записи; записи моніторингу системи; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, відповідальний за управління мобільним кодом]. **Перевірка:** [ВИБІР: Організаційний процес контролю, авторизації, моніторингу та обмеження мобільного коду; автоматизовані механізми підтримки та, або реалізації управління мобільним кодом; автоматизовані механізми підтримки та, або реалізації моніторингу мобільного коду].	

SC-18(1)	МОБІЛЬНИЙ КОД	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-18(01)_ODP[01]	**визначено неприйнятний мобільний код для ідентифікації;**
	SC-18(01)_ODP[02]	**визначені коригувальні дії, які необхідно вжити при виявленні неприйнятного мобільного коду;**
	SC-18(01)[01]	ідентифіковано **<SC-18(01)_ODP[01] неприйнятний мобільний код>**;

	SC-18(01)[02]	вживаються **<SC-18(01)_ODP[02] коригувальні дії>** у разі виявлення неприйнятного мобільного коду.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури адресації мобільного коду; обмеження використання мобільного коду, політика та процедури впровадження мобільного коду; перелік прийнятних мобільних кодів та технологій мобільних кодів; перелік неприйнятних мобільних кодів та мобільних технологій; авторизаційні записи; записи моніторингу системи; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, відповідальний за управління мобільним кодом]. **Перевірка:** [ВИБІР: Організаційний процес контролю, авторизації, моніторингу та обмеження мобільного коду; автоматизовані механізми підтримки та, або реалізації управління мобільним кодом; автоматизовані механізми підтримки та, або реалізації моніторингу мобільного коду].	

SC-18(2)	**МОБІЛЬНИЙ КОД - ПРИДБАННЯ, РОЗРОБКА ТА ВИКОРИСТАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-18(02)_ODP	**визначені вимоги до мобільного коду для придбання, розробки та використання мобільного коду для розгортання в системі;**
	SC-18(02)[01]	**відповідає придбання мобільного коду, який буде розгорнуто в системі, вимогам <SC-18(02)_ODP щодо мобільного коду>;**
	SC-18(02)[02]	відповідає розробка мобільного коду, який буде розгорнуто в системі, вимогам **<SC-18(02)_ODP вимоги до мобільного коду >**;
	SC-18(02)[03]	відповідає використання мобільного коду, який буде розгорнуто в системі, вимогам **<SC-18(02)_ODP вимоги до мобільного коду >**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури адресації мобільного коду; обмеження використання мобільного коду, політика та процедури впровадження мобільного коду; перелік прийнятних мобільних кодів та технологій мобільних кодів; перелік неприйнятних мобільних кодів та мобільних технологій; авторизаційні записи; записи моніторингу системи; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, відповідальний за управління мобільним кодом]. **Перевірка:** [ВИБІР: Організаційний процес контролю, авторизації, моніторингу	

	та обмеження мобільного коду; автоматизовані механізми підтримки та, або реалізації управління мобільним кодом; автоматизовані механізми підтримки та, або реалізації моніторингу мобільного коду].

SC-18(3)	**МОБІЛЬНИЙ КОД - ЗАПОБІГАННЯ ЗАВАНТАЖЕННЯ ТА ВИКОНАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-18(03)_ODP	**визначено неприйнятний мобільний код, який потрібно запобігти завантаженню та виконанню;**
	SC-18(03)[01]	запобігається завантаження **<SC-18(03)_ODP неприйнятний мобільний код>**;
	SC-18(03)[02]	запобігається виконання **<SC-18(03)_ODP неприйнятний мобільний код>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури адресації мобільного коду; обмеження використання мобільного коду, політика та процедури впровадження мобільного коду; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; розробник системи; персонал організації, відповідальний за управління мобільним кодом]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що перешкоджають завантаженню та виконанню неприйнятного мобільного коду].	

SC-18(4)	**МОБІЛЬНИЙ КОД - ЗАПОБІГАННЯ АВТОМАТИЧНОГО ВИКОНАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-18(04)_ODP[01]	**визначено програмні додатки, в яких необхідно запобігти автоматичному виконанню мобільного коду;**
	SC-18(04)_ODP[02]	**визначені дії, які повинна виконати система перед виконанням мобільного коду;**
	SC-18(04)[01]	запобігається автоматичне виконання мобільного коду в **<SC-18(04)_ODP[01] програмних додатках>**;
	SC-18(04)[02]	виконуються **<SC-18(04)_ODP[02] дії>** перед виконанням мобільного коду.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури адресації мобільного коду; обмеження використання мобільного коду; політика	

	та процедури впровадження мобільного коду; проєктна документація системи; налаштування конфігурації системи та відповідна документація; перелік програмних програм, для яких повинно бути заборонено автоматичне виконання мобільного коду; перелік дій, необхідних перед виконанням мобільного коду; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; розробник системи; персонал організації, відповідальний за управління мобільним кодом]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що запобігають автоматичному виконанню неприйнятного мобільного коду; автоматизовані механізми, що забезпечують дії, які слід вжити до виконання мобільного коду].

SC-18(5)	**МОБІЛЬНИЙ КОД - ДОЗВІЛ ВИКОНАННЯ ТІЛЬКИ В ОБМЕЖЕНИХ СЕРЕДОВИЩАХ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-18(05)	дозволено виконання дозволеного мобільного коду лише в обмеженому середовищі віртуальної машини.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури адресації мобільного коду; дозволи на використання мобільного коду; обмеження використання мобільного коду; проєктна документація системи; налаштування конфігурації системи та відповідна документація; перелік обмежених середовищ віртуальних машин, для яких дозволено виконання організаційно прийнятного мобільного коду; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; розробник системи; персонал організації, відповідальний за управління мобільним кодом]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що дозволяють виконувати дозволений мобільний код в обмежених середовищах віртуальної машини].	

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)**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-20a.[01]	надається додаткова автентифікації та перевірки цілісності джерела даних разом з офіційними даними розпізнавання імен, які система повертає у відповідь на запити дозволу імен/адрес;

	SC-20a.[02]	надаються дані перевірки цілісності разом з офіційними даними розпізнавання імен, які система повертає у відповідь на запити дозволу імен/адрес;
	SC-20b.[01]	передбачено засоби для вказівки статусу безпеки дочірніх зон (і чи підтримує дочірня зона служби безпечного дозволу) при роботі в розподіленому, ієрархічному просторі імен;
	SC-20b.[02]	передбачено засоби для перевірки ланцюжка довіри між батьківськими та дочірніми доменами під час роботи в розподіленому ієрархічному просторі імен.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються служби захисту імен, адрес (авторитетне джерело); проєктна документація системи; налаштування конфігурації системи та відповідна документація; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, відповідальний за управління DNS]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або впроваджують безпечну службу дозволу імен, адрес].	

SC-20(1)	**БЕЗПЕЧНА СЛУЖБА ІМЕН/АДРЕС (УПОВНОВАЖЕНЕ ДЖЕРЕЛО) - ДОЧІРНІЙ ПІДПРОСТІР**
	[Вилучено: включено до SC-20].

SC-20(2)	**БЕЗПЕЧНА СЛУЖБА ІМЕН, АДРЕС (УПОВНОВАЖЕНЕ ДЖЕРЕЛО) - ДЖЕРЕЛО ДАНИХ ТА ЦІЛІСНІСТЬ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-20(02)[01]	надаються справжні джерела походження запитів внутрішніх імен/адрес;
	SC-20(02)[02]	передбачено артефакти захисту цілісність запитів внутрішніх імен/адрес.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються служби захисту імен, адрес (авторитетне джерело); проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, відповідальний за управління DNS]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або впроваджують захист походження та цілісності даних для внутрішніх запитів	

	служби дозволу імен, адрес].

SC-21	**БЕЗПЕЧНА СЛУЖБА ІМЕН, АДРЕС (УПОВНОВАЖЕНЕ ДЖЕРЕЛО) - ДЖЕРЕЛО ДАНИХ ТА ЦІЛІСНІСТЬ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-21[01]	реалізується запит перевірки автентичності джерела даних для відповідей на запит дозволу імен/адрес, які система отримує від авторитетних джерел;
	SC-21[02]	реалізується запит автентифікація походження даних на основі відповідей з дозволу імен/адрес, які система отримує від авторитетних джерел;
	SC-21[03]	реалізується запит перевірки цілісності даних для відповідей на запит дозволу імен/адрес, які система отримує від авторитетних джерел;
	SC-21[04]	виконується перевірка цілісності даних для відповідей на запит про дозвіл імен/адрес, які система отримує від авторитетних джерел.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються служби захисту імен, адрес (авторитетне джерело); проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, відповідальний за управління DNS]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або впроваджують захист походження та цілісності даних для внутрішніх запитів служби дозволу імен, адрес].	

SC-21(1)	**БЕЗПЕЧНА СЛУЖБА ІМЕН/АДРЕС (РЕКУРСИВНИЙ АБО КЕШУВАЛЬНИЙ ПЕРЕТВОРЮВАЧ) - ДЖЕРЕЛО ДАНИХ ТА ЦІЛІСНІСТЬ**
	[Вилучено: включено до SC-21].

SC-22	**АРХІТЕКТУРА ТА ЗАБЕЗПЕЧЕННЯ СЛУЖБИ ІМЕН/АДРЕС**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-22[01]	є системи, які спільно надають послуги з визначення імен/адрес для організації, відмовостійкими;
	SC-22[02]	реалізовано в системах, які спільно надають послуги з

		вирішення імен/адрес для організації, внутрішній розподіл ролей;
	SC-22[03]	реалізовано в системах, які спільно надають послуги з вирішення імен/адрес для організації, зовнішній розподіл ролей
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються служби захисту імен, адрес (авторитетне джерело); проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, відповідальний за управління DNS]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або впроваджують захист походження та цілісності даних для внутрішніх запитів служби дозволу імен, адрес].	

SC-23	**АВТЕНТИФІКАЦІЯ СЕСІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-23	захищено автентифікацію сеансів зв'язку.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються справжності сесії; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або впроваджують автентичність сеансу].	

SC-23(1)	**АВТЕНТИФІКАЦІЯ СЕСІЇ - АНУЛЮВАННЯ ІДЕНТИФІКАТОРА СЕАНСУ ЗВ'ЯЗКУ ПРИ ВИХОДІ З СИСТЕМИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-23(01)	анулюються ідентифікатори сеансу після виходу користувача або іншого припинення сеансу зв'язку.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються справжності сесії; проєктна документація системи; налаштування	

	конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або впроваджують автентичність сеансу].

SC-21(2)	**АВТЕНТИФІКАЦІЯ СЕСІЇ - ІНІЦІЙОВАНІ КОРИСТУВАЧЕМ ВИХОДИ ТА ПОВІДОМЛЕННЯ**
	[Вилучено: включено до SC-21(1)].

SC-23(3)	**АВТЕНТИФІКАЦІЯ СЕСІЇ - УНІКАЛЬНІ ІДЕНТИФІКАТОРИ СЕАНСІВ З РАНДОМІЗАЦІЄЮ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-23(03)_ODP	**визначено вимоги до випадковості для генерації унікального ідентифікатора сеансу для кожного сеансу;**
	SC-23(03)[01]	генерується унікальний ідентифікатор сеансу для кожного сеансу з **<SC-23(03)_вимоги до випадковості ODP>**;
	SC-23(03)[02]	розпізнаються лише системні ідентифікатори сеансів.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються справжності сесії; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують створення та моніторинг унікальних ідентифікаторів сеансу; автоматизовані механізми, що підтримують та, або реалізують вимоги щодо випадковості].	

SC-21(4)	**АВТЕНТИФІКАЦІЯ СЕСІЇ - УНІКАЛЬНІ ІДЕНТИФІКАТОРИ СЕАНСІВ З РАНДОМІЗАЦІЄЮ**
	[Вилучено: включено до SC-23(3)].

SC-23(5)	**АВТЕНТИФІКАЦІЯ СЕСІЇ - УНІКАЛЬНІ ІДЕНТИФІКАТОРИ СЕАНСІВ З РАНДОМІЗАЦІЄЮ**
	МЕТА ОЦІНКИ: Визначити, чи:

	SC-23(05)_ODP	**визначено центри сертифікації, які будуть допущені до перевірки встановлення захищених сеансів;**
	SC-23(05)	дозволено використовувати лише <**SC-23(05)_ODP сертифіковані органи>** для перевірки встановлення захищених сеансів.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються справжності сесії; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують створення та моніторинг унікальних ідентифікаторів сеансу; автоматизовані механізми, що підтримують та, або реалізують вимоги щодо випадковості].	

SC-24	**УВЕДЕННЯ У ВІДОМИЙ СТАН**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-24_ODP[01]	**визначені типи відмов системи, за яких компоненти системи переходять до відомого стану;**
	SC-24_ODP[02]	відомий стан системи, до якого переходять компоненти системи у випадку її відмови;
	SC-24_ODP[03]	потрібно зберігати інформацію про стан системи у випадку її збою;
	SC-24	<**SC-24_ODP[01] типи системних збоїв на компонентах системи>** призводять до <**SC-24_ODP[02] відомого стану системи>**, зберігаючи при цьому <**SC-24_ODP[03] інформацію про стан системи>** у збої.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються відмови системи до відомого стану; проєктна документація системи; налаштування конфігурації системи та відповідна документація; перелік відмов, що вимагають відмови системи у відомому стані; інформація про стан, яка повинна зберігатися при відмові системи; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; розробник системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують можливість відомого стану відмов; автоматизовані механізми, що зберігають інформацію про стан системи у разі відмови системи].	

SC-25	ТОНКІ ВУЗЛИ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-25_ODP	**потрібно використовувати компоненти системи з мінімальною функціональністю та обсягом зберігання інформації;**
	SC-25[01]	використовується мінімальна функціональність для <**SC-25_ODP компонентів системи**>;
	SC-25[02]	виділено мінімальне сховище інформації на <**SC-25_ODP компоненти системи**>.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються використання тонких вузлів; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують тонкі вузли].	

SC-26	ПРИМАНКА ДЛЯ ЗЛОВМИСНИКІВ (DECOYS)	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-26[01]	є в системах організації компоненти, спеціально розроблені для того, щоб стати мішенню зловмисних атак, і чи є в них засоби для виявлення таких атак;
	SC-26[02]	є в організаційних компонентах системи, спеціально розроблені для того, щоб стати мішенню зловмисних атак, і чи є в них засоби для відбиття таких атак;
	SC-26[03]	включені в організаційні компоненти системи, спеціально розроблені для того, щоб бути мішенню зловмисних атак, для аналізу таких атак.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються використання приманок; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; розробник системи].	

	Перевірка: [ВИБЕРІТЬ З: Автоматизовані механізми, що підтримують та, або впроваджують приманки].

SC-26(1)	**ПРИМАНКА ДЛЯ ЗЛОВМИСНИКІВ (HONEYPOTS) - ВИЯВЛЕННЯ ШКІДЛИВОГО КОДУ**
	[Вилучено: включено до SC-35].

SC-27	**НЕЗАЛЕЖНІ ВІД ПЛАТФОРМИ ЗАСТОСУНКИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-27_ODP	**визначені незалежні від платформи додатки, які мають бути включені в системи організації;**
	SC-27	включені **<SC-27_ODP незалежні від платформи додатки>** в системи організації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються незалежних від платформи додатків; проєктна документація системи; налаштування конфігурації системи та відповідна документація; перелік незалежних від платформи програм; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; розробник системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або впроваджують незалежні від платформи програми].	

SC-28	**ЗАХИСТ ІНФОРМАЦІЇ В СТАНІ СПОКОЮ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-28_ODP	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {конфіденційність; цілісність};**
	SC-28_ODP[02]	**є інформація в стані спокою, яка потребує захисту;**
	SC-28	захищено **<SC-28_ODP[01] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** з **<SC-28_ODP[02] інформація в стані спокою>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту інформації в стані спокою; проєктна документація системи; налаштування конфігурації системи та відповідна документація; криптографічні механізми та пов'язана з ними конфігураційна документація; перелік інформації в стані спокою, що вимагає конфіденційності та захисту цілісності; інші відповідні	

	документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; розробник системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або впроваджують захист конфіденційності та цілісності для інформації, що перебуває в стані спокою].

SC-28(1)	**ЗАХИСТ ІНФОРМАЦІЇ В СТАНІ СПОКОЮ - КРИПТОГРАФІЧНИЙ ЗАХИСТ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-28(01)_ODP[01]	**визначена інформація, яка потребує криптографічного захисту;**
	SC-28(01)_ODP[02]	**є в системі компоненти або носії, що потребують криптографічного захисту;**
	SC-28(01)[01]	реалізовані криптографічні механізми для запобігання несанкціонованому розкриттю **<SC-28(01)_ODP[01] інформації>**, що знаходиться в стані спокою на **<SC-28(01)_ODP[02] системних компонентах або носіях>**;
	SC-28(01)[02]	реалізовані криптографічні механізми для запобігання несанкціонованій модифікації **<SC-28(01)_ODP[01] інформації>**, що знаходиться в стані спокою на **<SC-28(01)_ODP[02] системних компонентах або носіях>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту інформації в стані спокою; проєктна документація системи; налаштування конфігурації системи та відповідна документація; криптографічні механізми та пов'язана з ними конфігураційна документація; перелік інформації в стані спокою, що вимагає конфіденційності та захисту цілісності; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; розробник системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або впроваджують захист конфіденційності та цілісності для інформації, що перебуває в стані спокою].	

SC-28(2)	**ЗАХИСТ ІНФОРМАЦІЇ В СТАНІ СПОКОЮ - АВТОНОМНЕ СХОВИЩЕ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-28(02)_ODP	**потрібно вилучати інформацію з онлайн-сховища та**

		зберігати її в офлайн-сховищі в безпечному місці;
	SC-28(02)[01]	вилучено **<SC-28(02)_ODP інформацію>** з онлайн-сховища;
	SC-28(02)[02]	зберігається **<SC-28(02)_ODP інформація>** в автономному режимі в безпечному місці.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються захисту інформації в стані спокою; проєктна документація системи; налаштування конфігурації системи та відповідна документація; криптографічні механізми та пов'язана з ними конфігураційна документація; перелік інформації в стані спокою, що вимагає конфіденційності та захисту цілісності; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; розробник системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або впроваджують захист конфіденційності та цілісності для інформації, що перебуває в стані спокою].	

SC-28(3)	**ЗАХИСТ ІНФОРМАЦІЇ В СТАНІ СПОКОЮ - КРИПТОГРАФІЧНІ КЛЮЧІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-28(03)_ODP[01]	**вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {<SC-28(03)_ODP[02] гарантії>; апаратно-захищене сховище ключів};**
	SC-28(03)_ODP[02]	**визначені заходи безпеки для захисту зберігання криптографічних ключів (якщо вибрано);**
	SC-28(03)	забезпечено захищене зберігання криптографічних ключів за допомогою **<SC-28(03)_ODP[01] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика захисту системи та комунікацій; процедура передачі атрибутів безпеки та конфіденційності; політика та процедури контролю доступу; проектна документація системи; налаштування конфігурації системи та пов'язана з нею документація; записи аудиту системи; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Системні/мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку]. **Перевірка:** [ВИБІР: Механізми, що підтримують та/або реалізують механізми боротьби зі спуфінгом].	

SC-29	**ГЕТЕРОГЕННІСТЬ**

	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-29_ODP	**визначені компоненти системи, які потребують різноманітного набору інформаційних технологій, що мають бути використані при впровадженні системи;**
	SC-29	використовується різноманітний набір інформаційних технологій для **<SC-29_ODP компоненти системни>** при впровадженні системи.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; проєктна документація системи; налаштування конфігурації системи та відповідна документація; перелік технологій, що застосовуються в системі; документація про придбання; договори придбання компонентів або послуг системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який відповідає за придбання, розробку та впровадження системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або впроваджують використання різноманітного набору інформаційних технологій].	

SC-29(1)	**ГЕТЕРОГЕННІСТЬ - МЕТОДИ ВІРТУАЛІЗАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-29(01)_ODP	**визначена частота, з якою потрібно змінювати різноманітність операційних систем і додатків, розгорнутих за допомогою методів віртуалізації;**
	SC-29(01)	застосовуються методи віртуалізації для підтримки розгортання різноманітних операційних систем та додатків, які змінюються **<SC-29(01)_ODP частота>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; проєктна документація системи; налаштування конфігурації системи та відповідна документація; перелік технологій, що застосовуються в системі; документація про придбання; договори придбання компонентів або послуг системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який відповідає за придбання, розробку та впровадження системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або впроваджують використання різноманітного набору інформаційних технологій].	

SC-30	МАСКУВАННЯ ТА ХИБНИЙ НАПРЯМ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-30_ODP[01]	**визначені методи маскування та хибного напряму, які будуть застосовані для того, щоб заплутати і ввести в оману супротивників, які потенційно можуть націлитися на системи;**
	SC-30_ODP[02]	**визначені системи, для яких повинні застосовуватися методи маскування та хибного напряму;**
	SC-30_ODP[03]	**визначені часові періоди для застосування методів маскування та хибного напряму;**
	SC-30	застосовуються **<SC-30_ODP[01] методи маскування та хибного напряму>** для **<SC-30_ODP[02] систем>** протягом **<SC-30_ODP[03] періодів часу>**, щоб заплутати та ввести супротивника в оману.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; проєктна документація системи; налаштування конфігурації системи та відповідна документація; перелік технологій, що застосовуються в системі; документація про придбання; договори придбання компонентів або послуг системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який відповідає за придбання, розробку та впровадження системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або впроваджують використання різноманітного набору інформаційних технологій].	

SC-30(1)	МАСКУВАННЯ ТА ХИБНИЙ НАПРЯМ - МЕТОДИ ВІРТУАЛІЗАЦІЇ
	[Вилучено: включено до SC-29(1)].

SC-30(2)	МАСКУВАННЯ ТА ХИБНИЙ НАПРЯМ - ВИПАДКОВІСТЬ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-30(02)_ODP	**визначені методи, що застосовуються для внесення випадковості в операції та активи організації;**
	SC-30(02)	застосовуються **<SC-30(02)_ODP методи>** для внесення випадковості в операції та активи організації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; проєктна документація системи; налаштування конфігурації системи та відповідна документація; перелік технологій, що застосовуються в системі; документація	

	про придбання; договори придбання компонентів або послуг системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який відповідає за придбання, розробку та впровадження системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або впроваджують використання різноманітного набору інформаційних технологій].

SC-30(3)	**МАСКУВАННЯ ТА ХИБНИЙ НАПРЯМ - ЗМІНА МІСЦЯ ОБРОБКИ ТА ЗБЕРІГАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-30(03)_ODP[01]	**потрібно змінювати місця обробки та/або зберігання;**
	SC-30(03)_ODP[02]	**вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {<SC-30(03)_ODP[03] часова частота>; випадкові часові інтервали};**
	SC-30(03)_ODP[03]	**визначена періодичність зміни місця обробки та/або зберігання (якщо вибрано);**
	SC-30(03)	змінено місце розташування **<SC-30(03) _ODP[01] обробки та/або зберігання> <SC-30(03) _ODP[02] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; політика та процедури управління конфігурацією; процедури, що стосуються методів маскування та хибного напряму для системи; перелік місць обробки, зберігання, які слід змінювати через організаційні інтервали часу; змінити записи контролю; записи управління конфігурацією; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, відповідальний за зміну місць обробки та, або зберігання]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують змінні місця обробки та, або зберігання].	

SC-30(4)	**МАСКУВАННЯ ТА ХИБНИЙ НАПРЯМ - НЕПРАВДИВА ІНФОРМАЦІЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-30(04)_ODP	**визначені компоненти системи, для яких використовується реалістична, але неправдива**

		інформація про стан їхньої безпеки;
	SC-30(04)	використовується реалістична, але неправдива інформація про стан безпеки або стан **<SC-30(04)_ODP компонентів системи>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; політика та процедури управління конфігурацією; процедури, що стосуються методів маскування та хибного напряму для системи; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, відповідальний за визначення та використання реалістичної, але оманливої інформації про стан безпеки компонентів системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують використання реалістичної, але оманливої інформації про стан безпеки компонентів системи].	

SC-30(5)	**МАСКУВАННЯ ТА ХИБНИЙ НАПРЯМ - МАСКУВАННЯ СИСТЕМНИХ КОМПОНЕНТІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-30(05)_ODP[01]	**визначені методи, які будуть використані для приховування або маскування компонентів системи;**
	SC-30(05)_ODP[02]	**визначені компоненти системи, які мають бути приховані або замасковані за допомогою методів (визначених у SC-30(05)_ODP[01]);**
	SC-30(05)	застосовуються **<SC-30(05)_ODP[01] методи>** для приховування або маскування **<SC-30(05)_ODP[02] компонентів системи>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; політика та процедури управління конфігурацією; процедури, що стосуються методів маскування та хибного напряму для системи; проєктна документація системи; налаштування конфігурації системи та відповідна документація; перелік методів, що застосовуються для приховування або замаскування компонентів системи; перелік компонентів системи, які слід приховати або замаскувати; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, відповідальний за приховування компонентів системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або	

	впроваджують методи для приховування системних компонентів].

SC-31	**АНАЛІЗ ПРИХОВАНОГО КАНАЛУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-31_ODP	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {сховище; час};**
	SC-31a.	виконується аналіз прихованих каналів для виявлення тих аспектів зв'язку в системі, які є потенційними шляхами для прихованих **<SC-31_ODP ВИБРАНЕ ЗНАЧЕННЯ(Я) ПАРАМЕТРА(ів)>** каналів;
	SC-31b.	оцінено максимальну пропускну здатність цих каналів.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються аналізу прихованих каналів; проєктна документація системи; налаштування конфігурації системи та відповідна документація; документація про аналіз прихованих каналів; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який несе відповідальність за таємний аналіз каналів; розробники, інтегратори інформаційних систем]. **Перевірка:** [ВИБІР: Організаційний процес для проведення аналізу прихованих каналів; автоматизовані механізми, що підтримують та, або впроваджують аналіз прихованих каналів; автоматизовані механізми, що підтримують та, або реалізують можливість оцінки пропускної можливості прихованих каналів].	

SC-31(1)	**АНАЛІЗ ПРИХОВАНОГО КАНАЛУ - ТЕСТУВАННЯ ПРИХОВАНИХ КАНАЛІВ ДЛЯ ЕКСПЛУАТАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-31(01)	тестується підмножини визначених прихованих каналів, щоб визначити, які канали можна використовувати.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються аналізу прихованих каналів; проєктна документація системи; налаштування конфігурації системи та відповідна документація; список прихованих каналів; документація про аналіз прихованих каналів; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який несе	

	відповідальність за прихований аналіз каналів] **Перевірка:** [ВИБІР: Організаційний процес для тестування прихованих каналів; автоматизовані механізми, що підтримують та, або впроваджують тестування аналізу прихованих каналів].

SC-31(2)	**АНАЛІЗ ПРИХОВАНОГО КАНАЛУ - МАКСИМАЛЬНА ПРОПУСКНА ЗДАТНІСТЬ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-31(02)_ODP[01]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {сховище; час};**
	SC-31(02)_ODP[02]	**визначені значення максимальної пропускної здатності для виявлених прихованих каналів;**
	SC-31(02)	зменшується максимальна пропускна здатність для ідентифікованих прихованих **<SC-31(02)_ODP[01] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(S)>** каналів до **< SC-31(02)_ODP[02] значень>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються аналізу прихованих каналів; контракти на придбання інформаційних систем або послуг; документація про придбання; проєктна документація системи; налаштування конфігурації системи та відповідна документація; документація про аналіз прихованих каналів; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який несе відповідальність за таємний аналіз каналів; розробники, інтегратори інформаційних систем]. **Перевірка:** [ВИБІР: Організаційний процес для проведення аналізу прихованих каналів; автоматизовані механізми, що підтримують та, або впроваджують аналіз прихованих каналів; автоматизовані механізми, що підтримують та, або реалізують можливість зменшення пропускної можливості прихованих каналів].	

SC-31(3)	**АНАЛІЗ ПРИХОВАНОГО КАНАЛУ - ВИМІРЮВАННЯ ПРОПУСКНУ ЗДАТНІСТЬ В РОБОЧИХ СЕРЕДОВИЩАХ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-31(03)_ODP	**визначена підмножина ідентифікованих прихованих каналів, пропускна здатність яких має бути виміряна в операційному середовищі системи;**

	SC-31(03)	вимірюється пропускна здатність **<SC-31(03)_ODP підмножини ідентифікованих прихованих каналів>** у операційному середовищі системи.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються аналізу прихованих каналів; проєктна документація системи; налаштування конфігурації системи та відповідна документація; документація про аналіз прихованих каналів; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який несе відповідальність за таємний аналіз каналів; розробники, інтегратори інформаційних систем]. **Перевірка:** [ВИБІР: Організаційний процес для проведення аналізу прихованих каналів; автоматизовані механізми, що підтримують та, або впроваджують аналіз прихованих каналів; автоматизовані механізми, що підтримують та, або реалізують можливість вимірювання пропускної можливості прихованих каналів].	

SC-32	**ПОДІЛ СИСТЕМИ НА ЧАСТИНИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-32_ODP[01]	**повинні компоненти системи перебувати в окремих фізичних або логічних доменах або середовищах, виходячи з обставин фізичного або логічного поділу компонентів;**
	SC-32_ODP[02]	**вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРА: {фізичний; логічний};**
	SC-32_ODP[03]	**визначені обставини для фізичного або логічного розділення компонентів;**
	SC-32	розділена система на **<SC-32_ODP[01] компоненти системи>**, що знаходяться в окремих **<SC-32_ODP[02] ЗНАЧЕННЯ ВИБРАНОГО ПАРАМЕТРА>** доменах або середовищах на основі **<SC-32_ODP[03] обставин для фізичного або логічного поділу компонентів>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються розділення системи; проєктна документація системи; налаштування конфігурації системи та відповідна документація; архітектура системи; перелік фізичних доменів (або середовищ) системи; схеми об'єктів системи; схеми мережі системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який встановлює, налаштовує та, або підтримує інформаційну систему; розробники, інтегратори	

	інформаційних систем]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують фізичне розділення компонентів системи].

SC-32(1)	**ПОДІЛ СИСТЕМИ НА ЧАСТИНИ - ВІДОКРЕМЛЕНІ ФІЗИЧНІ ДОМЕНИ ДЛЯ ПРИВІЛЕЙОВАНИХ ФУНКЦІЙ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-32(01)	розділено привілейовані функції на окремі фізичні домени.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються розбиття системи на частини; проектна документація системи; налаштування конфігурації системи та пов'язана з нею документація; архітектура системи; перелік фізичних доменів (або середовищ) системи; схеми об'єктів системи; схеми мережі системи; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Системні/мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; персонал організації, який встановлює, налаштовує та/або обслуговує систему; системні розробники/інтегратори]. **Перевірка:** [ВИБІР: Механізми, що підтримують та/або реалізують фізичне розділення компонентів системи].	

SC-33	**ПІДГОТОВКА ЦІЛІСНОСТІ ПЕРЕДАЧІ**
	[Вилучено: включено до SC-8].

SC-34	**НЕЗМІНЮВАНІ ВИКОНАВЧІ ПРОГРАМИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-34_ODP[01]	**визначені компоненти системи, для яких операційне середовище та додатки мають завантажуватися та виконуватися з апаратних носіїв, призначених лише для читання;**
	SC-34_ODP[02]	**визначено додатки, які мають завантажуватися та виконуватися з апаратних носіїв, призначених лише для читання;**
	SC-34a.	завантажується та виконується операційне середовище для **<SC-34_ODP[01] системних компонентів>** з апаратного носія, доступного лише для читання;
	SC-34b.	**<SC-34_ODP[02] додатки>** для **<SC-34_ODP[01] компонентів системи>** завантажуються та виконуються з апаратного носія, доступного лише для читання.

	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються розбиття системи на частини; проектна документація системи; налаштування конфігурації системи та пов'язана з нею документація; архітектура системи; перелік фізичних доменів (або середовищ) системи; схеми об'єктів системи; схеми мережі системи; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Системні/мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; персонал організації, який встановлює, налаштовує та/або обслуговує систему; системні розробники/інтегратори]. **Перевірка:** [ВИБІР: Механізми, що підтримують та/або реалізують фізичне розділення компонентів системи].

SC-34(1)	**НЕЗМІНЮВАНІ ВИКОНАВЧІ ПРОГРАМИ - ВІДСУТНІСТЬ СХОВИЩА ДОСТУПНОГО ДЛЯ ЗАПИСУ ІНФОРМАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-34(01)_ODP	**визначено компоненти системи, які мають бути використані без можливості запису інформації;**
	SC-34(01)	використовуються **<SC-34(01)_ODP компоненти системи>** без записуваної пам'яті, яка зберігається після перезапуску компонента або увімкнення/вимкнення живлення.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються не модифікованих виконуваних програм; проєктна документація системи; налаштування конфігурації системи та відповідна документація; архітектура системи; перелік компонентів системи, які будуть використовуватися без можливості записування; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який встановлює, налаштовує та, або підтримує інформаційну систему; розробники, інтегратори інформаційних систем]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують використання компонентів без записуваного сховища; автоматизовані механізми, що підтримують та, або впроваджують постійне не записане сховище при перезапуску компонента та увімкненні, вимкненні живлення].	

SC-34(2)	**НЕЗМІНЮВАНІ ЗДІЙСНЮВАНІ ПРОГРАМИ - ЗАХИСТ ЦІЛІСНОСТІ НА НОСІЇ, ПРИДАТНОМУ ТІЛЬКИ ДЛЯ ЧИТАННЯ**
	МЕТА ОЦІНКИ: Визначити, чи:

	SC-34(02)[01]	захищена цілісність інформації перед зберіганням на носіях, призначених лише для читання;
	SC-34(02)[02]	є носій інформації контрольованим після того, як така інформація була записана на нього;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються не модифікованих виконуваних програм; проєктна документація системи; налаштування конфігурації системи та відповідна документація; архітектура системи; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який встановлює, налаштовує та, або підтримує інформаційну систему; розробники, інтегратори інформаційних систем]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують можливість захисту цілісності інформації на носіях, доступних лише для читання, до зберігання та після запису інформації на носій].	

SC-34(3)	**НЕЗМІНЮВАНІ ПРОГРАМИ, ЩО ВИКОНУЮТЬСЯ - АПАРАТНИЙ ЗАХИСТ**
	[Вилучено: перенесено до SC-51].

SC-35	**РОЗПІЗНАВАННЯ ПРИМАНОК ДЛЯ ЗЛОВМИСНИКІВ (HONEYCLIENT)**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-35	ввімкнуті компоненти системи, які активно намагаються ідентифікувати мережевий шкідливий код та шкідливі вебсайти.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються розпізнавання приманок для зловмисників (honeyclient); проєктна документація системи; налаштування конфігурації системи та відповідна документація; компоненти системи, розгорнуті для ідентифікації шкідливих вебсайтів та, або веб-шкідливого коду; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; розробник системи; персонал організації, який встановлює, налаштовує та, або підтримує інформаційну систему; розробники, інтегратори інформаційних систем]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або впроваджують розпізнавання приманок для зловмисників (honeyclient)].	

SC-36	**РОЗПОДІЛЕНА ОБРОБКА ТА ЗБЕРІГАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-36_ODP[01]	**потрібно розподіляти компоненти обробки між кількома локаціями/доменами;**
	SC-36_ODP[02]	**вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {фізичні локації; логічні домени};**
	SC-36_ODP[03]	**потрібно розподіляти компоненти сховища між кількома локаціями/доменами;**
	SC-36_ODP[04]	**вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {фізичні локації; логічні домени};**
	SC-36[01]	розділені **<SC-36_ODP[01] компоненти обробки>** по **<SC-36_ODP[02] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>**;
	SC-36[02]	розділені **<SC-36_ODP[03] компоненти сховища>** по **<SC-36_ODP[04] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються розпізнавання приманок для зловмисників (honeyclient); проєктна документація системи; налаштування конфігурації системи та відповідна документація; компоненти системи, розгорнуті для ідентифікації шкідливих вебсайтів та, або веб-шкідливого коду; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; розробник системи; персонал організації, який встановлює, налаштовує та, або підтримує інформаційну систему; розробники, інтегратори інформаційних систем]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або впроваджують розпізнавання приманок для зловмисників (honeyclient)].	

SC-36(1)	**РОЗПОДІЛЕНА ОБРОБКА ТА ЗБЕРІГАННЯ - МЕТОДИ ОПИТУВАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-36(01)_ODP[01]	**є компоненти розподіленої обробки та зберігання даних, для яких слід застосовувати методи опитування для виявлення потенційних збоїв, помилок або компрометації;**
	SC-36(01)_ODP[02]	**визначені дії, які необхідно вжити у відповідь на виявлені несправності, помилки або компрометацію;**
	SC-36(01)(a)	застосовуються методи опитування для виявлення потенційних несправностей, помилок або компрометації **<SC-36(01)_ODP[01] компонентів розподіленої обробки та**

		зберігання даних>;
	SC-36(01)(b)	вживаються **<SC-36(01)_ODP[02] дії>** у відповідь на ідентифіковано несправності, помилки або компрометацію.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; проєктна документація системи; налаштування конфігурації системи та відповідна документація; архітектура системи; перелік розподілених компонентів обробки та зберігання, що підлягають опитуванню; методи опитування системи та відповідна документація чи записи; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який встановлює, налаштовує та, або підтримує інформаційну систему; розробники, інтегратори інформаційних систем]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або впроваджують методи опитування].	

SC-36(2)	**РОЗПОДІЛЕНА ОБРОБКА ТА ЗБЕРІГАННЯ - СИНХРОНІЗАЦІЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-36(02)_ODP	**визначено дублікати систем або системних компонентів, що підлягають синхронізації;**
	SC-36(02)	синхронізовані **<SC-36(02)_ODP дублікати систем або компонентів системи>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика захисту системи та комунікацій; проектна документація системи; налаштування конфігурації системи та пов'язана з нею документація; архітектура системи; перелік розподілених компонентів обробки та зберігання даних, що підлягають опитуванню; методи опитування системи та пов'язана з ними документація або записи; записи аудиту системи; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Системні/мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; персонал організації, який встановлює, налаштовує та/або обслуговує систему; системні розробники/інтегратори]. **Перевірка:** [ВИБІР: Механізми, що підтримують та/або реалізують дублюючу синхронізацію системи або системних компонентів].	

SC-37	**ПОЗАСМУГОВІ КАНАЛИ**
	МЕТА ОЦІНКИ: Визначити, чи:

	SC-37_ODP[01]	**потрібно використовувати позасмугові канали для фізичної доставки або електронної передачі інформації, компонентів системи або пристроїв окремим особам або системі;**
	SC-37_ODP[02]	**визначено інформацію, компоненти системи або пристрої для використання позасмугових каналів для фізичної доставки або електронної передачі;**
	SC-37_ODP[03]	**визначені особи або системи, до яких фізична доставка або електронна передача інформації, системних компонентів або пристроїв має бути досягнута за допомогою використання позасмугових каналів;**
	SC-37	використовуються **<SC-37_ODP[01] позасмугові канали>** для фізичної доставки або електронної передачі **<SC-37_ODP[02] інформації, системних компонентів або пристроїв>** до **<SC-37_ODP[03] осіб або систем>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються використання позасмугових каналів; політика та процедури контролю доступу; політика і процедури ідентифікації та автентифікації; проєктна документація системи; архітектура системи; налаштування конфігурації системи та відповідна документація; список позасмугових каналів; типи інформації, компоненти системи або пристрої, що вимагають використання позасмугових каналів для фізичного постачання або електронної передачі уповноваженим особам або інформаційним системам; записи фізичного постачання; записи електронної передачі; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який встановлює, налаштовує та, або підтримує інформаційну систему; персонал організації, що дозволяє, встановлює, налаштовує, експлуатує та, або використовує позасмугові канали; розробники, інтегратори інформаційних систем]. **Перевірка:** [ВИБІР: Процеси організації для використання позасмугових каналів; автоматизовані механізми, що підтримують та, або реалізують використання позасмугових каналів].	

SC-37(1)	**ПОЗАСМУГОВІ КАНАЛИ - ЗАБЕЗПЕЧЕННЯ ДОСТАВЛЕННЯ ТА ПЕРЕДАЧІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-37(01)_ODP[01]	**потрібно застосовувати засоби контролю для забезпечення того, щоб тільки визначені особи або системи отримували певну інформацію, компоненти системи або пристрої;**
	SC-37(01)_ODP[02]	**визначені особи або системи, призначені для отримання певної інформації, компоненти системи або пристрої;**

	SC-37(01)_ODP[03]	**визначено інформацію, компоненти системи або пристрої, доступ до яких мають лише окремі особи або системи**
	SC-37(01)	застосовуються **<SC-37(01)_ODP[01] засоби контролю>** для забезпечення того, щоб тільки **<SC-37(01)_ODP[02] особи або системи>** отримували **<SC-37(01)_ODP[03] інформацію, компоненти системи або пристрої>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються використання позасмугових каналів; політика та процедури контролю доступу; політика і процедури ідентифікації та автентифікації; проєктна документація системи; архітектура системи; налаштування конфігурації системи та відповідна документація; перелік гарантій безпеки, які застосовуватимуться для забезпечення отримання визначеними особами або інформаційними системами інформації, визначеної організацією, компонентів системи або пристроїв; перелік гарантій безпеки для доставки призначеної інформації, компонентів системи або пристроїв до зазначених осіб або інформаційних систем; перелік інформації, компонентів системи або пристроїв, що передаються призначеним особам або інформаційним системам; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який встановлює, налаштовує та, або підтримує інформаційну систему; персонал організації, що дозволяє, встановлює, налаштовує, експлуатує та, або використовує позасмугові канали; розробники, інтегратори інформаційних систем]. **Перевірка:** [ВИБІР: Процеси організації для використання позасмугових каналів; автоматизовані механізми, що підтримують та, або реалізують використання позасмугових каналів; автоматизовані механізми, що підтримують, впроваджують запобіжні заходи для забезпечення доставки призначеної інформації, компонентів системи або пристроїв].	

SC-38	**БЕЗПЕКА ОПЕРАЦІЙ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-38_ODP	**визначені засоби контролю заходів з безпеки операцій, які будуть застосовуватися для захисту ключової інформації організації протягом усього життєвого циклу розробки системи;**
	SC-38	застосовуються **<SC-38_ODP засоби контролю заходів з безпеки операцій>** для захисту ключової інформації організації протягом життєвого циклу розробки системи.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються безпеки операцій; план захисту інформації; перелік гарантій безпеки операцій; оцінки контролю безпеки; оцінки ризиків; оцінки загроз та вразливості;	

	плани дій та етапи; документація життєвого циклу розробки системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, що встановлює, налаштовує та, або підтримує інформаційну систему; розробники, інтегратори інформаційних систем]. **Перевірка:** [ВИБІР: Процеси організації для захисту організаційної інформації в SDLC; автоматизовані механізми, що підтримують та, або впроваджують запобіжні заходи для захисту організаційної інформації в рамках SDLC].

SC-39	**ІЗОЛЯЦІЯ ПРОЦЕСУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-39	підтримується окремий домен виконання для кожного процесу, що виконується в системі.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Проєктна документація системи; архітектура системи; документація про незалежну перевірку; документація про тестування та оцінку, інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Розробники, інтегратори інформаційних систем; архітектор безпеки системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують окремі домени виконання для кожного процесу виконання].	

SC-39(1)	**ІЗОЛЯЦІЯ ПРОЦЕСУ - АПАРАТНЕ РОЗДІЛЕННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-39(01)	реалізовано апаратне розділення для розділення процесів.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; проєктна документація системи; налаштування конфігурації системи та відповідна документація; архітектура системи; документація системи для апаратних механізмів розділення; документація системи від постачальників, виробників або розробників; документація про незалежну перевірку та перевірку; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; розробник системи; персонал організації, що встановлює, налаштовує та, або підтримує інформаційну систему; розробники, інтегратори інформаційних систем]. **Перевірка:** [ВИБІР: Можливість системи, що реалізує механізми розділення	

	апаратного забезпечення для розділення процесів].

SC-39(2)	**ІЗОЛЯЦІЯ ПРОЦЕСУ - ІЗОЛЯЦІЯ ПОТОКІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-39(02)_ODP	**визначено багатопотокову обробку, для якої потрібно підтримувати окремий домен виконання для кожного потоку;**
	SC-39(02)	підтримується окремий домен виконання для кожного потоку у **<SC-39(02)_ODP багатопотокової обробки>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; проєктна документація системи; налаштування конфігурації системи та відповідна документація; архітектура системи; список доменів виконання системи для кожного потоку в багатопотоковій обробці; документація системи для багатопотокової обробки; документація системи від постачальників, виробників або розробників; документація про незалежну перевірку та перевірку; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; розробник системи; персонал організації, що встановлює, налаштовує та, або підтримує інформаційну систему; розробники, інтегратори інформаційних систем]. **Перевірка:** [ВИБІР: Можливість системи, що реалізує окремий домен виконання для кожного потоку в багатопотоковій обробці].	

SC-40	**ЗАХИСТ БЕЗДРОТОВОГО З'ЄДНАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-40_ODP[01]	**потрібно захищати зовнішні бездротові з'єднання від певних типів атак на параметри сигналу;**
	SC-40_ODP[02]	**визначено типи атак на параметри сигналу або посилання на джерела таких атак, від яких потрібно захищати зовнішні бездротові з'єднання;**
	SC-40_ODP[03]	**потрібно захищати внутрішні бездротові з'єднання від певних типів атак на параметри сигналу;**
	SC-40_ODP[04]	**визначені типи атак на параметри сигналу або посилання на джерела таких атак, від яких потрібно захищати внутрішні бездротові з'єднання;**
	SC-40[01]	захищені зовнішні **<SC-40_ODP[01] бездротові з'єднання>** від **<SC-40_ODP[02] типів атак на параметри сигналу або посилання на джерела таких атак>**.

	SC-40[02]	захищені внутрішні **<SC-40_ODP[03] бездротові з'єднання>** від **<SC-40_ODP[04] типів атак на параметри сигналу або посилання на джерела для таких атак>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; політика та процедури контролю доступу; процедури, що стосуються захисту бездротового зв'язку; проєктна документація системи; схеми бездротової мережі; налаштування конфігурації системи та відповідна документація; архітектура системи; типи або внутрішні та зовнішні бездротові посилання; типи атак параметрів сигналу або посилання на джерела атак; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; розробник системи; персонал організації, що встановлює, налаштовує та, або підтримує інформаційну систему; персонал організації, що дозволяє, встановлює, налаштовує та, або підтримує внутрішні та зовнішні бездротові зв'язки]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують захист бездротових ліній зв'язку].	

SC-40(1)	**ЗАХИСТ БЕЗДРОТОВОГО З'ЄДНАННЯ - ЕЛЕКТРОМАГНІТНІ ПЕРЕШКОДИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-40(01)_ODP	**визначено рівень захисту від впливу навмисних електромагнітних перешкод;**
	SC-40(01)	реалізовані криптографічні механізми, які забезпечують < **<SC-40(01)_ODP рівень захисту>** від впливу навмисних електромагнітних перешкод.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; політика та процедури контролю доступу; процедури, що стосуються захисту бездротового зв'язку; проєктна документація системи; схеми бездротової мережі; налаштування конфігурації системи та відповідна документація; архітектура системи; апаратне та програмне забезпечення комунікацій системи; результати категоризації безпеки; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; розробник системи; персонал організації, що встановлює, налаштовує та, або підтримує інформаційну систему; персонал організації, що дозволяє, встановлює, налаштовує та, або підтримує внутрішні та зовнішні бездротові зв'язки]. **Перевірка:** [ВИБІР: Криптографічні механізми, що забезпечують захист від наслідків навмисних електромагнітних перешкод].	

SC-40(2)	ЗАХИСТ БЕЗДРОТОВОГО З'ЄДНАННЯ - ЗМЕНШЕННЯ ПОТЕНЦІАЛУ ВИЯВЛЕННЯ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-40(02)_ODP	**визначено рівень зниження, якого необхідно досягти для зменшення потенціалу виявлення бездротових з'єднань;**
	SC-40(02)	впроваджено криптографічні механізми для зменшення потенціалу виявлення бездротових з'єднань до <**SC-40(02)_ODP рівня зменшення>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; політика та процедури контролю доступу; процедури, що стосуються захисту бездротового зв'язку; проєктна документація системи; схеми бездротової мережі; налаштування конфігурації системи та відповідна документація; архітектура системи; апаратне та програмне забезпечення комунікацій системи; результати категоризації безпеки; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; розробник системи; персонал організації, що встановлює, налаштовує та, або підтримує інформаційну систему; персонал організації, що дозволяє, встановлює, налаштовує та, або підтримує внутрішні та зовнішні бездротові зв'язки]. **Перевірка:** [ВИБІР: Криптографічні механізми, що забезпечують захист від наслідків навмисних електромагнітних перешкод].	

SC-40(3)	ЗАХИСТ БЕЗДРОТОВОГО З'ЄДНАННЯ - ІМІТАЦІЙНИЙ АБО МАНІПУЛЯТИВНИЙ ОБМІН ПОВІДОМЛЕННЯМИ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-40(03)	впроваджені криптографічні механізми для визначення та відхилення бездротових передач, які є навмисними спробами досягти імітаційного або маніпулятивного обміну повідомленнями на основі параметрів сигналу.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; політика та процедури контролю доступу; процедури, що стосуються проєктної документації системи; схеми бездротової мережі; налаштування конфігурації системи та відповідна документація; архітектура системи; апаратне та програмне забезпечення комунікацій системи; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який	

	відповідає за інформаційну безпеку; розробник системи; персонал організації, що встановлює, налаштовує та, або підтримує інформаційну систему; персонал організації, що дозволяє, встановлює, налаштовує та, або підтримує внутрішні та зовнішні бездротові зв'язки]. **Перевірка:** [ВИБІР: Криптографічні механізми, що забезпечують захист бездротового зв'язку від обману імітаційних або маніпулятивних комунікацій].

SC-41	**ДОСТУП ДО ПОРТІВ ТА ПРИСТРОЇВ ВВЕДЕННЯ, ВИВЕДЕННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-41_ODP[01]	**визначено порти підключення або пристрої вводу/виводу, які потрібно відключити або видалити;**
	SC-41_ODP[02]	**вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {фізично; логічно};**
	SC-41_ODP[03]	**визначені системи або компоненти системи з портами підключення або пристроями вводу/виводу, які потрібно відключити або видалити;**
	SC-41	**<SC-41_ODP[01] порти підключення або пристрої вводу/виводу>** є **<SC-41_ODP[02] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>** відключити або видалити на **<SC-41_ODP[03] системах або системних компонентах>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; політика та процедури контролю доступу; процедури, що стосуються проєктної документації системи; схеми бездротової мережі; налаштування конфігурації системи та відповідна документація; архітектура системи; апаратне та програмне забезпечення комунікацій системи; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; розробник системи; персонал організації, що встановлює, налаштовує та, або підтримує інформаційну систему; персонал організації, що дозволяє, встановлює, налаштовує та, або підтримує внутрішні та зовнішні бездротові зв'язки]. **Перевірка:** [ВИБІР: Криптографічні механізми, що перешкоджають ідентифікації бездротових передавачів].	

SC-42	**МОЖЛИВОСТІ ДАТЧИКА ТА ДАНІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-42_ODP[01]	**вибрано одне або більше з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {використання пристроїв, що мають <SC-**

		42_ODP[02] можливості зондування довкілля> на <SC-42_ODP[03] об'єктах, територіях або системах}; дистанційна активація можливостей зондування довкілля на організаційних системах або системних компонентах з наступними винятками: <SC-42_ODP[04] винятки, де дозволяється дистанційна активація датчиків>};
	SC-42_ODP[02]	**визначені можливості зондування навколишнього середовища в пристроях (якщо вибрано);**
	SC-42_ODP[03]	**визначені об'єкти, зони або системи, на яких заборонено використання пристроїв, що мають можливості зондування навколишнього середовища (якщо вони були обрані);**
	SC-42_ODP[04]	**визначено винятки, коли дозволено віддалену активацію датчиків (якщо вибрано);**
	SC-42_ODP[05]	**визначено групу користувачів, яким необхідно надати явну вказівку про використання датчика;**
	SC-42a.	заборонено **<SC-42_ODP[01] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>**;
	SC-42b.	надається явна вказівка на використання датчика для **<SC-42_ODP[05] групи користувачів**>.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються можливостей датчиків та збору даних; політика та процедури контролю доступу; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; розробник системи; персонал організації, що встановлює, налаштовує та, або підтримує інформаційну систему; персонал організації, відповідальний за роботу датчика]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують засоби контролю доступу для віддаленої активації можливостей датчика системи; автоматизовані механізми, що реалізують можливість індикації використання датчика].	

SC-42(1)	**МОЖЛИВОСТІ ДАТЧИКА ТА ДАНІ - ЗВІТУВАННЯ ПЕРЕД УПОВНОВАЖЕНИМИ АБО ПОСАДОВИМИ ОСОБАМИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-42(01)_ODP	**визначені датчики, які будуть використовуватися для збору даних або інформації;**
	SC-42(01)	налаштована система таким чином, щоб дані або інформація, **<SC-42(01)_ODP зібрані датчиками>**, повідомлялися лише уповноваженим особам або ролям.

	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; політика та процедури контролю доступу; можливість датчика та збір даних; проєктна документація системи; налаштування конфігурації системи та відповідна документація; архітектура системи; перелік заходів, що застосовуються для забезпечення того, щоб дані або інформація, зібрані датчиками, використовувались лише у дозволених цілях; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, що встановлює, налаштовує та, або підтримує інформаційну систему; персонал організації, відповідальний за роботу датчика]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або впроваджують заходи для забезпечення того, щоб інформація датчика використовувалася лише в дозволених цілях; можливість збору інформації датчиків для системи].

SC-42(2)	**МОЖЛИВОСТІ ДАТЧИКА ТА ДАНІ - ДОЗВОЛЕНЕ ВИКОРИСТАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-42(02)_ODP	**потрібно вживати заходів для того, щоб дані або інформація, зібрані датчиками, використовувалися лише в дозволених цілях;**
	SC-42(02)	застосовуються **<SC-42(02)_ODP заходи>** таким чином, щоб дані або інформація, зібрані **<SC-42(01)_ODP датчиками>**, використовувалися лише в дозволених цілях
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; політика та процедури контролю доступу; можливість датчика та збір даних; проєктна документація системи; налаштування конфігурації системи та відповідна документація; архітектура системи; перелік заходів, що застосовуються для забезпечення того, щоб дані або інформація, зібрані датчиками, використовувались лише у дозволених цілях; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, що встановлює, налаштовує та, або підтримує інформаційну систему; персонал організації, відповідальний за роботу датчика]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або впроваджують заходи для забезпечення того, щоб інформація датчика використовувалася лише в дозволених цілях; можливість збору інформації датчиків для системи].	

SC-42(3)	**МОЖЛИВОСТІ ДАТЧИКА ТА ДАНІ - ЗАБОРОНА ВИКОРИСТАННЯ**

	ПРИСТРОЇВ
	[Вилучено: перенесено до SC-42].

SC-42(4)	**МОЖЛИВОСТІ ДАТЧИКА ТА ДАНІ - ПОВІДОМЛЕННЯ ПРО ЗБІР**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-42(04)_ODP[01]	**визначені заходи, які сприятимуть повідомленню осіб про збір персональних даних;**
	SC-42(04)_ODP[02]	визначені датчики, які збирають персональні дані;
	SC-42(04)	застосовуються **<SC-42(04)_ODP[01] заходи>** для полегшення усвідомлення особою того, що персональні дані збираються за допомогою **<SC-42(04)_ODP[02] датчиків>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються обмежень щодо використання; обмеження використання; політика та процедури впровадження; авторизаційні записи; записи моніторингу системи; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який встановлює, налаштовує та, або підтримує інформаційну систему]. **Перевірка:** [ВИБІР: Процеси організації для дозволу, моніторингу та контролю використання компонентів з обмеженнями щодо використання; Автоматизовані механізми, що підтримують та, або впроваджують дозвіл, моніторинг та контроль використання компонентів з обмеженнями використання].	

SC-42(5)	**МОЖЛИВОСТІ ДАТЧИКА ТА ДАНІ - МІНІМІЗАЦІЯ ЗБОРУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-42(05)_ODP	**визначені датчики, які налаштовані на мінімізацію збору непотрібних персональних даних;**
	SC-42(05)	використовуються **<SC-42(05)_ODP датчики>**, налаштовані на мінімізацію збору персональних даних, які не є необхідними.

	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються обмежень щодо використання; обмеження використання; політика та процедури впровадження; авторизаційні записи; записи моніторингу системи; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який встановлює, налаштовує та, або підтримує інформаційну систему]. **Перевірка:** [ВИБІР: Процеси організації для дозволу, моніторингу та контролю використання компонентів з обмеженнями щодо використання; Автоматизовані механізми, що підтримують та, або впроваджують дозвіл, моніторинг та контроль використання компонентів з обмеженнями використання].

SC-43	**ОБМЕЖЕННЯ ВИКОРИСТАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-43_ODP	**визначені компоненти, для яких мають бути встановлені обмеження на використання та настанови щодо впровадження;**
	SC-43a.	встановлені обмеження на використання та настанови щодо впровадження для **<SC-43_ODP компонентів>**;
	SC-43b.[01]	дозволено використання **<SC-43_ODP компонентів>** у системі;
	SC-43b.[02]	здійснюється моніторинг використання **<SC-43_ODP компонентів>** в системі;
	SC-43b.[03]	контролюється використання **<SC-43_ODP компонентів>** в системі.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються обмежень щодо використання; обмеження використання; політика та процедури впровадження; авторизаційні записи; записи моніторингу системи; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який встановлює, налаштовує та, або підтримує інформаційну систему]. **Перевірка:** [ВИБІР: Процеси організації для дозволу, моніторингу та контролю використання компонентів з обмеженнями щодо використання; Автоматизовані механізми, що підтримують та, або впроваджують дозвіл, моніторинг та контроль використання компонентів з обмеженнями використання].	

SC-44	**ЕКРАНОВАНІ КАМЕРИ**

	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-44_ODP	**визначена система, компонент системи або місце, де має бути застосований потенціал екранованої камери;**
	SC-44	використовується в системі **<SC-44_ODP, системному компоненті або місці розташування>** можливість застосування екранованої камери
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика захисту системи та комунікацій; процедури, що стосуються обмежень щодо використання; обмеження використання; політика та процедури впровадження; авторизаційні записи; записи моніторингу системи; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який встановлює, налаштовує та, або підтримує інформаційну систему]. **Перевірка:** [ВИБІР: Процеси організації для дозволу, моніторингу та контролю використання компонентів з обмеженнями щодо використання; Автоматизовані механізми, що підтримують та, або впроваджують дозвіл, моніторинг та контроль використання компонентів з обмеженнями використання].	

SC-45	**СИНХРОНІЗАЦІЯ СИСТЕМИ З ЧАСОМ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-45	**синхронізовані системні годинники всередині системи та між системами і системними компонентами.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика захисту системи та комунікацій; процедури синхронізації часу; проектна документація системи; налаштування конфігурації системи та пов'язана з нею документація; записи аудиту системи; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Системні/мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; персонал організації, який встановлює, налаштовує та/або обслуговує систему; системні розробники/інтегратори]. **Перевірка:** [ВИБІР: Механізми, що підтримують та/або реалізують дублюючу синхронізацію системи або системних компонентів].	

SC-45(1)	**СИНХРОНІЗАЦІЯ СИСТЕМИ З ЧАСОМ - СИНХРОНІЗАЦІЯ З АВТОРИТЕТНИМ ДЖЕРЕЛОМ ЧАСУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	

	SC-45(01)_ODP[01]	**визначено частоту, на якій потрібно порівнювати внутрішній системний годинник з авторитетним джерелом часу;**
	SC-45(01)_ODP[02]	**визначено авторитетне джерело часу, з яким буде порівнюватися внутрішній системний годинник;**
	SC-45(01)_ODP[03]	**визначено період часу для порівняння внутрішнього системного годинника з авторитетним джерелом часу;**
	SC-45(01)(a)	порівнюються внутрішні системні годинники **<SC-45(01)_ODP[01] частота>** з **<SC-45(01)_ODP[02] авторитетним джерелом часу>**;
	SC-45(01)(b)	синхронізовано внутрішній системний годинник з авторитетним джерелом часу, якщо різниця у часі більша за **<SC-45(01)_ODP[03] часовий період>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика захисту системи та комунікацій; процедури синхронізації часу; проектна документація системи; налаштування конфігурації системи та пов'язана з нею документація; записи аудиту системи; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Системні/мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; персонал організації, який встановлює, налаштовує та/або обслуговує систему; системні розробники/інтегратори]. **Перевірка:** [ВИБІР: Механізми, що підтримують та/або реалізують дублюючу синхронізацію системи або системних компонентів].	

SC-45(2)	**СИНХРОНІЗАЦІЯ СИСТЕМИ З ЧАСОМ - ВТОРИННЕ АВТОРИТЕТНЕ ДЖЕРЕЛО ЧАСУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-45(02)(a)	**є вторинне авторитетне джерело часу, яке знаходиться в іншому географічному регіоні, ніж первинне авторитетне джерело часу;**
	SC-45(02)(b)	синхронізовано внутрішній системний годинник з вторинним авторитетним джерелом часу, якщо первинне авторитетне джерело часу недоступне.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика захисту системи та комунікацій; процедури синхронізації часу; проектна документація системи; налаштування конфігурації системи та пов'язана з нею документація; записи аудиту системи; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Системні/мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; персонал організації, який встановлює,	

	налаштовує та/або обслуговує систему; системні розробники/інтегратори]. **Перевірка:** [ВИБІР: Механізми, що підтримують та/або реалізують дублюючу синхронізацію системи або системних компонентів].

SC-46	**ЗАБЕЗПЕЧЕННЯ ВИКОНАННЯ МІЖДОМЕННОЇ ПОЛІТИКИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-46_ODP	**вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {фізично; логічно};**
	SC-46	реалізовано механізм застосування політики **<SC-46_ODP ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА>** між фізичними та/або мережевими інтерфейсами для з'єднувальних доменів безпеки.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика захисту системи та комунікацій; процедури синхронізації часу; проектна документація системи; налаштування конфігурації системи та пов'язана з нею документація; записи аудиту системи; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Системні/мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; персонал організації, який встановлює, налаштовує та/або обслуговує систему]. **Перевірка:** [ВИБІР: Механізми підтримки та/або впровадження міждоменної політики].	

SC-47	**АЛЬТЕРНАТИВНИЙ ШЛЯХ ЗВ'ЯЗКУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-47_ODP	**визначені альтернативні шляхи зв'язку для системних операцій та контролю операцій системи;**
	SC-47	встановлені **<SC-47_ODP альтернативні шляхи зв'язку>** для системних операцій та контролю операцій системи.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика захисту системи та комунікацій; процедури синхронізації часу; проектна документація системи; налаштування конфігурації системи та пов'язана з нею документація; записи аудиту системи; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Системні/мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; персонал організації, який встановлює, налаштовує та/або обслуговує систему]. **Перевірка:** [ВИБІР: Механізми підтримки та/або впровадження міждоменної	

	політики].

SC-48	**ПЕРЕМІЩЕННЯ ДАТЧИКА**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-48_ODP[01]	**визначені датчики та можливості моніторингу, які необхідно перемістити;**
	SC-48_ODP[02]	**визначені місця, куди будуть переміщені датчики та засоби моніторингу;**
	SC-48_ODP[03]	**визначені умови або обставини для переміщення датчиків і можливостей моніторингу;**
	SC-48	переміщуються **<SC-48_ODP[01] датчики і засоби моніторингу>** до **<SC-48_ODP[02] місць розташування>** за **<SC-48_ODP[03] умов або обставин>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика захисту системи та комунікацій; процедури синхронізації часу; проектна документація системи; налаштування конфігурації системи та пов'язана з нею документація; записи аудиту системи; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Системні/мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; персонал організації, який встановлює, налаштовує та/або обслуговує систему]. **Перевірка:** [ВИБІР: Механізми підтримки та/або впровадження міждоменної політики].	

SC-48(1)	**ДИНАМІЧНЕ ПЕРЕМІЩЕННЯ СЕНСОРІВ ТА МОНІТОРИНГ МОЖЛИВОСТЕЙ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-48(01)_ODP[01]	**визначені датчики та засоби моніторингу, що підлягають динамічному переміщенню;**
	SC-48(01)_ODP[02]	**визначені місця, куди будуть динамічно переміщуватися датчики та засоби моніторингу;**
	SC-48(01)_ODP[03]	**визначені умови або обставини для динамічного переміщення датчиків і можливостей моніторингу;**
	SC-48(01)	**<SC-48(01)_ODP[01] датчики та засоби моніторингу>** динамічно переміщуються до **<SC-48(01)_ODP[02] місць розташування>** за **<SC-48(01)_ODP[03] умов або обставин>**.

	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика захисту системи та комунікацій; процедури синхронізації часу; проектна документація системи; налаштування конфігурації системи та пов'язана з нею документація; записи аудиту системи; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Системні/мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; персонал організації, який встановлює, налаштовує та/або обслуговує систему]. **Перевірка:** [ВИБІР: Механізми підтримки та/або впровадження міждоменної політики].

SC-49	**ПРИМУСОВЕ АПАРАТНЕ РОЗДІЛЕННЯ ТА ПОЛІТИКА ЗАБЕЗПЕЧЕННЯ ВИКОНАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-49_ODP	**визначені домени безпеки, які потребують апаратного розділення та механізмів забезпечення дотримання політики;**
	SC-49	впроваджено механізми апаратного розділення та застосування політик між **<SC-49_ODP доменами безпеки>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика захисту системи та комунікацій; процедури синхронізації часу; проектна документація системи; налаштування конфігурації системи та пов'язана з нею документація; записи аудиту системи; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Системні/мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; персонал організації, який встановлює, налаштовує та/або обслуговує систему]. **Перевірка:** [ВИБІР: Механізми підтримки та/або впровадження міждоменної політики].	

SC-50	**ПРИМУСОВЕ ПРОГРАМНЕ РОЗДІЛЕННЯ ТА ПОЛІТИКА ЗАБЕЗПЕЧЕННЯ ВИКОНАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-50_ODP	**визначені домени безпеки, які потребують програмного розділення та механізмів забезпечення дотримання політик;**
	SC-50	впроваджено програмне розділення та механізми застосування політик між **<SC-50_ODP доменами безпеки>**.

	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика захисту системи та комунікацій; процедури синхронізації часу; проектна документація системи; налаштування конфігурації системи та пов'язана з нею документація; записи аудиту системи; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Системні/мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; персонал організації, який встановлює, налаштовує та/або обслуговує систему]. **Перевірка:** [ВИБІР: Механізми підтримки та/або впровадження міждоменної політики].

SC-51	**АПАРАТНИЙ ЗАХИСТ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SC-51_ODP[01]	**визначено компоненти системної прошивки, які потребують апаратного захисту від запису;**
	SC-51_ODP[02]	**визначені уповноважені особи, які повинні виконувати процедури вимкнення та повторного ввімкнення апаратного захисту від запису;**
	SC-51a.	використовується апаратний захист від запису для **<SC-51_ODP[01] компонентів мікропрограми системи>**;
	SC-51b.[01]	впроваджено спеціальні процедури для **<SC-51_ODP[02] уповноважених осіб>** для ручного вимкнення апаратного захисту від запису для модифікацій мікропрограми;
	SC-51b.[02]	реалізовано спеціальні процедури для **<SC-51_ODP[02] уповноважених осіб>** для повторного увімкнення захисту від запису перед поверненням до робочого режиму.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика захисту системи та комунікацій; процедури синхронізації часу; проектна документація системи; налаштування конфігурації системи та пов'язана з нею документація; записи аудиту системи; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда**: [ВИБІР: Системні/мережеві адміністратори; персонал організації, відповідальний за інформаційну безпеку; персонал організації, який встановлює, налаштовує та/або обслуговує систему]. **Перевірка:** [ВИБІР: Процеси організації модифікації системного програмного забезпечення; механізми, що підтримують та/або реалізують апаратний захист від запису системного програмного забезпечення].	

XVIII. КЛАС ЗАХОДІВ ЗАХИСТУ SI – ЦІЛІСНІСТЬ СИСТЕМИ ТА ІНФОРМАЦІЇ

SI-1	**ПОЛІТИКА І ПРОЦЕДУРИ ЦІЛІСНОСТІ ІНФОРМАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-01_ODP[01]	**визначено персонал або ролі, до яких має бути доведена політика цілісності системи та інформації;**
	SI-01_ODP[02]	**визначено персонал або ролі, на які поширюються процедури цілісності системи та інформації ;**
	SI-01_ODP[03]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {рівень організації; рівень місії/бізнес-процесу; рівень системи};**
	SI-01_ODP[04]	**визначено посадову особу, відповідальну за управління системою та політикою і процедурами цілісності інформації;**
	SI-01_ODP[05]	**визначено періодичність перегляду та оновлення поточної політики цілісності системи та інформації;**
	SI-01_ODP[06]	**є події, які вимагають перегляду та оновлення поточної політики цілісності системи та інформації;**
	SI-01_ODP[07]	**визначено частоту, з якою переглядаються та оновлюються поточні цілісності системи та інформації;**
	SI-01_ODP[08]	**є події, які вимагають перегляду та оновлення процедур забезпечення цілісності системи та інформації;**
	SI-01a.[01]	розроблена та задокументована політика цілісності системи та інформації;
	SI-01a.[02]	поширюється політика цілісності системи та інформації на **<SI-01_ODP[01] персонал або ролі>**;
	SI-01a.[03]	розроблені та задокументовані процедури цілісності системи та інформації для сприяння впровадженню політики забезпечення системної та інформаційної цілісності та пов'язаних з нею засобів контролю системної та інформаційної цілісності;
	SI-01a.[04]	поширюються процедури забезпечення цілісності системи та інформації на **<SI-01_ODP[02] персонал або ролі>**;
	SI-01a.01(a)[01]	відповідає **<SI-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** політиці цілісності системи та інформації;
	SI-01a.01(a)[02]	політика цілісності системи та інформації **<SI-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** звертається до сфери дії;
	SI-01a.01(a)[03]	стосується **<SI-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** політики цілісності системи та

		інформації;
	SI-01a.01(a)[04]	політика цілісності системи та інформації **<SI-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** враховує обов'язки;
	SI-01a.01(a)[05]	враховує <**SI-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** зобов'язання керівництва політика цілісності системи та інформації;
	SI-01a.01(a)[06]	передбачає **<SI-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** політика політика цілісності системи та інформації координацію між структурними підрозділами організації;
	SI-01a.01(a)[07]	відповідає вимогам **<SI-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** політиці цілісності системи та інформації;
	SI-01a.01(b)	відповідає **<SI-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** політиці цілісності системи та інформації чинним законам, виконавчим наказам, директивам, положенням, політикам, стандартам та настановам;
	SI-01b.	призначено **<SI-01_ODP[04] посадову особу >** для управління розробкою, документуванням та розповсюдженням політики та процедур забезпечення цілісності системи та інформації;
	SI-01c.01[01]	переглядається та оновлюється поточна політика цілісності системи та інформації **<SI-01_ODP[05] частота>**;
	SI-01c.01[02]	переглядається та оновлюється поточна політика цілісності системи та інформації після <**SI-01_ODP[06] подій>**;
	SI-01c.02[01]	переглядаються та оновлюються поточні процедури цілісності системи та інформації **<SI-01_ODP[07] частота>**;
	SI-01c.02[02]	переглядаються та оновлюються поточні процедури цілісності системи та інформації **<SI-01_ODP[08] подій>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політики та процедури захисту цілісності системи та інформації; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал відповідальний за політику цілісності системи та інформації; персонал, відповідальний за інформаційну безпеку].	

SI-2	**ВИПРАВЛЕННЯ ДЕФЕКТІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-02_ODP	**визначено період часу, протягом якого необхідно встановити оновлення програмного забезпечення, пов'язані з безпекою, після виходу оновлень;**

SI-02a.[01]	виявлено недоліки системи;
SI-02a.[02]	повідомляється про недоліки системи;
SI-02a.[03]	виправлені недоліки системи;
SI-02b.[01]	перевіряються оновлення програмного забезпечення, пов'язані з усуненням недоліків, на ефективність перед встановленням;
SI-02b.[02]	перевіряються оновлення програмного забезпечення, пов'язані з виправленням дефектів, на наявність потенційних побічних ефектів перед встановленням;
SI-02b.[03]	перевіряються оновлення прошивки, пов'язані з усуненням недоліків, на ефективність перед встановленням;
SI-02b.[04]	перевіряються оновлення прошивки, пов'язані з усуненням недоліків, на наявність потенційних побічних ефектів перед встановленням;
SI-02c.[01]	встановлено оновлення програмного забезпечення, що стосуються безпеки, протягом **<SI-02_ODP часовий проміжок>** з моменту випуску оновлень;
SI-02c.[02]	встановлено оновлення мікропрограми, що стосуються безпеки, протягом **<SI-02_ODP часового періоду**> з моменту випуску оновлень;
SI-02d.	включено відновлення порушених прав у процес управління організаційною конфігурацією.

ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:

Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються усунення недоліків; процедури, що стосуються управління конфігурацією; перелік недоліків та уразливостей, які потенційно можуть вплинути на інформаційну систему; перелік останніх заходів щодо усунення недоліків безпеки, здійснених в системі (наприклад, перелік встановлених виправлень, пакетів оновлень, виправлення та інші оновлення програмного забезпечення для виправлення недоліків системи); результати тестування від встановлення програмного забезпечення та оновлення мікропрограми для виправлення недоліків системи; записи про встановлення, контроль змін для оновлення програмного забезпечення та мікропрограми, що стосується безпеки; інші відповідні документи або записи].

Співбесіда: [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який встановлює, налаштовує та, або підтримує інформаційну систему; персонал організації, відповідальний за усунення недоліків; персонал організації, відповідальний за управління конфігурацією].

Перевірка: [ВИБІР: Процеси організації для виявлення, звітування та виправлення недоліків системи; організаційний процес встановлення оновлень програмного забезпечення та мікропрограми; автоматизовані механізми підтримки та, або впровадження звітності та виправлення недоліків системи; автоматизовані механізми, що підтримують та, або впроваджують тестові

	оновлення програмного забезпечення та мікропрограми].

SI-2(1)	**ВИПРАВЛЕННЯ ДЕФЕКТІВ - ЦЕНТРАЛІЗОВАНЕ УПРАВЛІННЯ**
	[Вилучено: перенесено до PL-09].

SI-2(2)	**ВИПРАВЛЕННЯ ДЕФЕКТІВ - АВТОМАТИЗОВАНЕ ВИПРАВЛЕННЯ ДЕФЕКТІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-02(02)_ODP[01]	**визначені автоматизовані механізми для визначення того, чи встановлені на компонентах системи відповідні оновлення програмного забезпечення та мікропрограми, що мають відношення до безпеки;**
	SI-02(02)_ODP[02]	**визначено частоту, з якою слід визначати, чи встановлюються на компонентах системи відповідні оновлення програмного забезпечення та мікропрограми, що стосуються безпеки;**
	SI-02(02)	встановлені на компонентах системи відповідні оновлення програмного забезпечення та мікропрограми, що стосуються безпеки, з **<SI-02(02)_ODP[02] частотою>** за допомогою **<SI-02(02)_ODP[01] автоматизованих механізмів>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються усунення недоліків; автоматизовані механізми підтримки централізованого управління усуненням недоліків; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, що встановлює, налаштовує та, або підтримує інформаційну систему; персонал організації, відповідальний за усунення недоліків]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що використовуються для визначення стану компонентів системи щодо усунення недоліків].	

SI-2(3)	**ВИПРАВЛЕННЯ ДЕФЕКТІВ - ЧАС ДЛЯ УСУНЕННЯ ДЕФЕКТІВ ТА ОРІЄНТИРИ ДЛЯ КОРИГУВАЛЬНИХ ДІЙ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-02(03)_ODP	**визначені контрольні показники для вжиття коригувальних заходів;**
	SI-02(03)(a)	вимірюється час між виявленням дефекту та його усуненням;

	SI-02(03)(b)	були встановлені **<SI-02(03)_ODP орієнтири>** для вжиття коригувальних дій.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються усунення недоліків; проєктна документація системи; налаштування конфігурації системи та відповідна документація; перелік еталонів для вжиття коригувальних заходів щодо виявлених недоліків; записи, що містять відмітки про час виявлення недоліків та подальші заходи щодо їх усунення; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, що встановлює, налаштовує та, або підтримує інформаційну систему; персонал організації, відповідальний за усунення недоліків]. **Перевірка:** [ВИБІР: Процеси організації для виявлення, звітування та виправлення недоліків системи; автоматизовані механізми, що використовуються для вимірювання часу між виявленням та усуненням недоліків].	

SI-2(4)	**ВИПРАВЛЕННЯ ДЕФЕКТІВ - АВТОМАТИЧНІ ЗАСОБИ УПРАВЛІННЯ ВИПРАВЛЕННЯМИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-02(04)_ODP	**визначені компоненти системи, які потребують автоматизованих інструментів управління виправленнями для полегшення усунення дефектів;**
	SI-02(04)]	застосовуються автоматизовані засоби управління виправленнями для полегшення виправлення недоліків у **<SI-02(04)_ODP компонентах>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються виправлення дефектів; автоматизовані механізми, що підтримують усунення несправностей та автоматичне оновлення програмного забезпечення, мікропрограми; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи останніх оновлень програмного забезпечення та мікропрограми, що стосуються безпеки, автоматично встановлюються на компоненти системи; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який встановлює, налаштовує та, або підтримує інформаційну систему; персонал організації, відповідальний за виправлення дефектів]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують автоматичне оновлення програмного забезпечення, мікропрограми].	

SI-2(5)	**ВИПРАВЛЕННЯ ДЕФЕКТІВ - АВТОМАТИЧНЕ ОНОВЛЕННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-02(05)_ODP[01]	**визначено оновлення програмного забезпечення та мікропрограм, що стосуються безпеки, які мають бути автоматично встановлені на компоненти системи;**
	SI-02(05)_ODP[02]	**визначено компоненти системи, які потребують автоматичного встановлення оновлень програмного забезпечення, пов'язаного з безпекою;**
	SI-02(05)	**<SI-02(05) _ODP[01] оновлення програмного забезпечення та мікропрограми, що стосуються безпеки>**, встановлено автоматично до **<SI-02(05) _ODP[02] компонентів системи>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються виправлення дефектів; автоматизовані механізми, що підтримують усунення несправностей та автоматичне оновлення програмного забезпечення, мікропрограми; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи останніх оновлень програмного забезпечення та мікропрограми, що стосуються безпеки, автоматично встановлюються на компоненти системи; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який встановлює, налаштовує та, або підтримує інформаційну систему; персонал організації, відповідальний за виправлення дефектів]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що реалізують автоматичне оновлення програмного забезпечення, мікропрограми].	

SI-2(6)	**ВИПРАВЛЕННЯ ДЕФЕКТІВ - ВИДАЛЕННЯ ПОПЕРЕДНІХ ВЕРСІЙ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-02(06)_ODP	**потрібно видаляти компоненти програмного забезпечення та мікропрограми після встановлення оновлених версій;**
	SI-02(06)	видаляються попередні версії **<SI-02(06)_ODP програмне забезпечення та компоненти мікропрограми>** після встановлення оновлених версій.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ:	

	Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються виправлення дефектів; автоматизовані механізми, що підтримують виправлення дефектів; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи про видалення програмного забезпечення та компонентів мікропрограми після встановлення оновлених версій; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який встановлює, налаштовує та, або підтримує інформаційну систему; персонал організації, відповідальний за виправлення дефектів]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або здійснюють видалення попередніх версій програмного забезпечення, прошивки].

SI-3	**ЗАХИСТ ВІД ШКІДЛИВОГО КОДУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-03_ODP[01]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {підписаний; непідписаний};**
	SI-03_ODP[02]	**визначено частоту, з якою механізми захисту від шкідливого коду виконують сканування;**
	SI-03_ODP[03]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {кінцева точка; точки входу та виходу з мережі};**
	SI-03_ODP[04]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {block malicious code; quarantitne malicious code; take <SI-03_ODP[05] action>};**
	SI-03_ODP[05]	**визначено дії, яких слід вжити у відповідь на виявлення шкідливого коду (якщо вибрано);**
	SI-03_ODP[06]	**визначено персонал або ролі, які мають бути сповіщені при виявленні шкідливого коду;**
	SI-03a.[01]	реалізовано **<SI-03_ODP[01] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** механізми захисту від зловмисного коду у точках входу та виходу з системи для виявлення зловмисного коду;
	SI-03a.[02]	впроваджено **<SI-03_ODP[01] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** механізми захисту від зловмисного коду в точках входу та виходу з системи для викорінення зловмисного коду;
	SI-03b.	оновлюються механізми захисту від зловмисного коду автоматично з появою нових випусків відповідно до політики та процедур управління конфігурацією організації;
	SI-03c.01[01]	налаштовано механізми захисту від шкідливого коду на виконання періодичних сканувань системи **<SI-03_ODP[02]**

	частота>;
SI-03c.01[02]	налаштовано механізми захисту від шкідливого коду на виконання сканування файлів із зовнішніх джерел у режимі реального часу за адресою **<SI-03_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** під час завантаження, відкриття або виконання файлів відповідно до політики організації;
SI-03c.02[01]	налаштовані механізми захисту від зловмисного коду на реакцію на виявлення зловмисного коду;
SI-03c.02[02]	налаштовано механізми захисту від зловмисного коду на надсилання сповіщень **<SI-03_ODP[06] персоналу або ролям>** у відповідь на виявлення зловмисного коду;
SI-03d.	вирішується проблема отримання хибних спрацьовувань під час виявлення та усунення шкідливого коду і пов'язаний з цим потенційний вплив на доступність системи.

ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ:

Дослідження: [ВИБІР: Політика цілісності системи та інформації; політика та процедури управління конфігурацією; процедури, що стосуються захисту від шкідливого коду; механізми захисту від зловмисного коду; записи оновлень захисту від шкідливого коду; проєктна документація системи; налаштування конфігурації системи та відповідна документація; сканувати результати від шкідливих механізмів захисту коду; запис дій, ініційованих механізмами захисту від зловмисного коду у відповідь на виявлення шкідливого коду; записи аудиту системи; інші відповідні документи або записи].

Співбесіда: [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який встановлює, налаштовує та, або підтримує інформаційну систему; персонал організації, відповідальний за захист від шкідливого коду; персонал організації, відповідальний за управління конфігурацією].

Перевірка: [ВИБІР: Процеси організації для використання, оновлення та налаштування механізмів захисту від зловмисного коду; організаційний процес вирішення помилкових спрацьовувань та наслідків потенційного впливу; автоматизовані механізми, що підтримують та, або впроваджують використання, оновлення та налаштування механізмів захисту від шкідливого коду; автоматизовані механізми, що підтримують та, або реалізують сканування шкідливого коду та подальші дії].

SI-3(1)	**ЗАХИСТ ВІД ШКІДЛИВОГО КОДУ - ЦЕНТРАЛІЗОВАНЕ УПРАВЛІННЯ**
	[Вилучено: включено до PL-9].

SI-3(2)	**ЗАХИСТ ВІД ШКІДЛИВОГО КОДУ - АВТОМАТИЧНІ ОНОВЛЕННЯ**
	[Вилучено: включено до SI-03].

SI-3(3)	**ЗАХИСТ ВІД ШКІДЛИВОГО КОДУ - НЕПРИВІЛЕЙОВАНІ КОРИСТУВАЧІ**
	[Вилучено: включено до AC-6(10)].

SI-3(4)	ЗАХИСТ ВІД ШКІДЛИВОГО КОДУ - ОНОВЛЕННЯ ТІЛЬКИ ПРИВІЛЕЙОВАНИМИ КОРИСТУВАЧАМИ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-03(04)	оновлюються механізми захисту від шкідливого коду лише за вказівкою привілейованого користувача.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються захисту від шкідливого коду; проєктна документація системи; механізми захисту від зловмисного коду; записи оновлень захисту шкідливого коду; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; розробники системи; персонал організації, який встановлює, налаштовує та, або підтримує інформаційну систему; персонал організації, відповідальний за захист від зловмисного коду]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують можливості захисту від зловмисного коду].	

SI-3(5)	ЗАХИСТ ВІД ШКІДЛИВОГО КОДУ - ПОРТАТИВНІ ПРИСТРОЇ ЗБЕРІГАННЯ ДАНИХ
	[Вилучено: включено до MP-7].

SI-3(6)	ЗАХИСТ ВІД ШКІДЛИВОГО КОДУ - ТЕСТУВАННЯ ТА ВЕРИФІКАЦІЯ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-03(06)_ODP	**визначено періодичність тестування механізмів захисту від зловмисного коду;**
	SI-03(06)(a)	перевіряються механізми захисту від шкідливого коду **<SI-03(06)_ODP частота>** шляхом введення в систему відомого доброякісного коду;
	SI-03(06)(b)[01]	відбувається виявлення (доброякісний тест) коду;
	SI-03(06)(b)[02]	відбувається відповідне звітування про інцидент.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються захисту від шкідливого коду; проєктна документація системи; налаштування конфігурації системи та відповідна документація; тестові справи; записи, що містять докази тестових справ, виконаних на механізмах захисту від шкідливого коду; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який	

	відповідає за інформаційну безпеку; персонал організації, який встановлює, налаштовує та, або підтримує інформаційну систему; персонал організації, відповідальний за захист від зловмисного коду]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або впроваджують тестування та перевірку можливостей захисту від шкідливого коду].

SI-3(7)	**ЗАХИСТ ВІД ШКІДЛИВОГО КОДУ - ВИЯВЛЕННЯ БЕЗ ПІДПИСУ**
	[Вилучено: включено до SI-3].

SI-3(8)	**ЗАХИСТ ВІД ШКІДЛИВОГО КОДУ - ВИЯВЛЕННЯ НЕАВТОРИЗОВАНИХ КОМАНД**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-03(08)_ODP[01]	**визначено апаратні компоненти системи, для яких неавторизовані команди операційної системи мають бути виявлені через інтерфейс прикладного програмування ядра;**
	SI-03(08)_ODP[02]	**визначено неавторизовані команди операційної системи, які потрібно виявити;**
	SI-03(08)_ODP[03]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {видати попередження; перевірити виконання команди; заборонити виконання команди};**
	SI-03(08)(a)	виявлено **<SI-03(08) _ODP[01] неавторизовані команди операційної системи>** через інтерфейс прикладного програмування ядра на **<SI-03(08) _ODP[02] апаратних компонентах системи>**;
	SI-03(08)(b)	виконується **<SI-03(08)_ODP[03] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(S)>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються захисту від шкідливого коду; проєктна документація системи; механізми захисту від зловмисного коду; попереджувальні повідомлення, що надсилаються при виявленні несанкціонованого виконання команди операційної системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; розробники системи; персонал організації, який встановлює, налаштовує та, або підтримує інформаційну систему; персонал організації, відповідальний за захист від зловмисного коду]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують можливості захисту від шкідливого коду; автоматизовані механізми, що підтримують та, або реалізують виявлення несанкціонованих команд	

	операційної системи через інтерфейс програмування ядра].

SI-3(9)	**ЗАХИСТ ВІД ШКІДЛИВОГО КОДУ - АВТЕНТИФІКАЦІЯ ВІДДАЛЕНИХ КОМАНД**
	[Вилучено: включено до AC-17(10)].

SI-3(10)	**ЗАХИСТ ВІД ШКІДЛИВОГО КОДУ - АНАЛІЗ ШКІДЛИВОГО КОДУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-03(10)_ODP	**визначені інструменти та методи, які будуть використовуватися для аналізу характеристик та поведінки шкідливого коду;**
	SI-03(10)(a)	використовуються **<SI-03(10)_ODP інструменти та методи>** для аналізу характеристик та поведінки шкідливого коду;
	SI-03(10)(b)[01]	включені результати аналізу шкідливого коду в організаційні процеси реагування на інциденти;
	SI-03(10)(b)[02]	включені результати аналізу шкідливого коду в організаційні процеси виправлення недоліків
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються захисту від шкідливого коду; процедури, що стосуються реагування на події; процедури, що стосуються усунення недоліків; проєктна документація системи; механізми, засоби та методи захисту від зловмисного коду; налаштування конфігурації системи та відповідна документація; результати аналізу шкідливого коду; записи подій щодо усунення недоліків, отриманих в результаті аналізу шкідливого коду; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який встановлює, налаштовує та, або підтримує інформаційну систему; персонал організації, відповідальний за захист від шкідливого коду; персонал організації, відповідальний за усунення недоліків; персонал організації, відповідальний за реагування на події, управління ними]. **Перевірка:** [ВИБІР: Організаційний процес реагування на інциденти; організаційний процес усунення недоліків; автоматизовані механізми, що підтримують та, або реалізують можливості захисту від зловмисного коду; інструменти та методи аналізу характеристик та поведінки шкідливого коду].	

SI-4	**МОНІТОРИНГ СИСТЕМИ**
	МЕТА ОЦІНКИ: Визначити, чи:

	SI-04_ODP[01]	**визначені цілі моніторингу для виявлення атак та індикатори потенційних атак на систему;**
	SI-04_ODP[02]	**визначені методи та способи, що використовуються для виявлення несанкціонованого використання системи;**
	SI-04_ODP[03]	**визначена інформація про моніторинг системи, яка повинна надаватися персоналу або ролям;**
	SI-04_ODP[04]	**визначено персонал або ролі, яким має надаватися інформація про моніторинг системи;**
	SI-04_ODP[05]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {за потребою; <SI-04_ODP[06] частота>};**
	SI-04_ODP[06]	**визначено періодичність моніторингу системи для персоналу або ролей (якщо вибрано);**
	SI-04a.01	проводиться моніторинг системи для виявлення атак та індикаторів потенційних атак відповідно до **<SI-04_ODP[01] цілі моніторингу>**;
	SI-04a.02[01]	здійснюється моніторинг системи для виявлення несанкціонованих локальних підключень;
	SI-04a.02[02]	здійснюється моніторинг системи на предмет виявлення несанкціонованих мережевих підключень;
	SI-04a.02[03]	здійснюється моніторинг системи для виявлення несанкціонованих віддалених підключень;
	SI-04b.	виявлено несанкціоноване використання системи за допомогою **<SI-04_ODP[02] прийомів та методів>**;
	SI-04c.01	задіяні внутрішні можливості моніторингу, чи стратегічно розгорнуті пристрої моніторингу в системі для збору важливої інформації, визначеної організацією;
	SI-04c.02	задіюються внутрішні можливості моніторингу, чи встановлюються пристрої моніторингу в окремих місцях системи для відстеження конкретних типів транзакцій, що становлять інтерес для організації;
	SI-04d.[01]	аналізуються виявлені події;
	SI-04d.[02]	аналізуються виявлені аномалії;
	SI-04e.	коригується рівень діяльності з моніторингу системи при зміні ризиків для діяльності та активів організації, окремих осіб, інших організацій або держави;
	SI-04f.	отримано юридичний висновок щодо діяльності з моніторингу системи;
	SI-04g.	надається **<SI-04_ODP[03] інформація про моніторинг системи> <SI-04_ODP[04] персоналу або ролям> <SI-04_ODP[05] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ:	

	Дослідження: [ВИБІР: Стратегія постійного моніторингу; політика цілісності системи та інформації; процедури, що стосуються засобів та методів моніторингу системи; схема об'єкта; проєктна документація системи; документація засобів і методів моніторингу системи; місця в системі, де розміщені пристрої моніторингу; налаштування конфігурації системи та відповідна документація; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, що встановлює, налаштовує та, або підтримує інформаційну систему; персонал організації, відповідальний за моніторинг системи]. **Перевірка:** [ВИБІР: Процеси організації для моніторингу системи; автоматизовані механізми, що підтримують та, або впроваджують можливості моніторингу системи].

SI-4(1)	**МОНІТОРИНГ СИСТЕМИ - ЗАГАЛЬНОСИСТЕМНА СИСТЕМА ВИЯВЛЕННЯ ВТОРГНЕНЬ (IDS)**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-04(01)[01]	підключені окремі засоби виявлення вторгнень до загальносистемної системи виявлення вторгнень;
	SI-04(01)[02]	об'єднані окремі інструменти виявлення вторгнень у загальносистемну систему виявлення вторгнень.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ’ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються засобів та методів моніторингу системи; проєктна документація системи; документація засобів і методів моніторингу системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який встановлює, налаштовує та, або підтримує інформаційну систему; персонал організації, відповідальний за моніторинг системи; персонал організації, відповідальний за реагування, управління інцидентами]. **Перевірка:** [ВИБІР: Процеси організації для аналізу подій майже у реальному часі; організаційні процеси моніторингу системи; автоматизовані механізми підтримки та, або впровадження моніторингу системи; автоматизовані механізми, інструменти, що підтримують та, або здійснюють аналіз подій].	

SI-4(2)	**МОНІТОРИНГ СИСТЕМИ - АВТОМАТИЗОВАНІ ЗАСОБИ ТА МЕХАНІЗМИ АНАЛІЗУ В РЕАЛЬНОМУ ЧАСІ**
	МЕТА ОЦІНКИ: Визначити, чи:

	SI-04(02)	застосовуються автоматизовані інструменти та механізми для підтримки аналізу подій у режимі, близькому до реального часу.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються засобів та методів моніторингу системи; проєктна документація системи; документація засобів і методів моніторингу системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який встановлює, налаштовує та, або підтримує інформаційну систему; персонал організації, відповідальний за моніторинг системи; персонал організації, відповідальний за реагування, управління інцидентами]. **Перевірка:** [ВИБІР: Процеси організації для аналізу подій майже у реальному часі; організаційні процеси моніторингу системи; автоматизовані механізми підтримки та, або впровадження моніторингу системи; автоматизовані механізми, інструменти, що підтримують та, або здійснюють аналіз подій].	

SI-4(3)	**МОНІТОРИНГ СИСТЕМИ - АВТОМАТИЗОВАНІ ЗАСОБИ ТА МЕХАНІЗМИ ІНТЕГРАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-04(03)[01]	використовуються автоматизовані інструменти та механізми для інтеграції інструментів та механізмів виявлення вторгнень у механізми контролю доступу;
	SI-04(03)[02]	використовуються автоматизовані інструменти та механізми для інтеграції інструментів та механізмів виявлення вторгнень у механізми контролю потоків.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються засобів та методів моніторингу системи; проєктна документація системи; документація засобів і методів моніторингу системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який встановлює, налаштовує та, або підтримує інформаційну систему; персонал організації, відповідальний за моніторинг системи; персонал організації, відповідальний за реагування, управління інцидентами]. **Перевірка:** [ВИБІР: Процеси організації для аналізу подій майже у реальному часі; організаційні процеси моніторингу системи; автоматизовані механізми підтримки та, або впровадження моніторингу системи; автоматизовані	

	механізми, інструменти, що підтримують та, або здійснюють аналіз подій].

SI-4(4)	**МОНІТОРИНГ СИСТЕМИ - ТРАФІК ВХІДНИХ І ВИХІДНИХ КОМУНІКАЦІЙ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-04(04)_ODP[01]	**визначено періодичність моніторингу вхідного комунікаційного трафіку на предмет виявлення незвичних або несанкціонованих дій чи умов;**
	SI-04(04)_ODP[02]	**визначені незвичайні або несанкціоновані дії або умови, які необхідно контролювати у вхідному трафіку зв'язку;**
	SI-04(04)_ODP[03]	**визначено періодичність моніторингу вихідного комунікаційного трафіку на предмет виявлення незвичних або несанкціонованих дій чи умов;**
	SI-04(04)_ODP[04]	**визначені незвичайні або несанкціоновані дії або умови, які необхідно контролювати у вихідному трафіку зв'язку;**
	SI-04(04)(a)[01]	визначені критерії незвичної або несанкціонованої діяльності або умови для вхідного трафіку зв'язку;
	SI-04(04)(a)[02]	визначені критерії незвичайної або несанкціонованої діяльності або умови для вихідного трафіку зв'язку;
	SI-04(04)(b)[01]	здійснюється моніторинг вхідного комунікаційного трафіку **<SI-04(04)_ODP[01] частота>** на предмет **<SI-04(04)_ODP[02] незвичних або несанкціонованих дій або умов>**;
	SI-04(04)(b)[02]	контролюється вихідний трафік зв'язку **<SI-04(04)_ODP[03] частота>** на предмет **<SI-04(04)_ODP[04] незвичних або несанкціонованих дій або умов>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються засобів та методів моніторингу системи; проєктна документація системи; документація засобів і методів моніторингу системи; налаштування конфігурації системи та відповідна документація; протоколи системи; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який встановлює, налаштовує та, або підтримує інформаційну систему; персонал організації, відповідальний за моніторинг системи; персонал організації, відповідальний за систему виявлення вторгнень]. **Перевірка:** [ВИБІР: Процеси організації для виявлення вторгнень, моніторинг системи; автоматизовані механізми, що підтримують та, або впроваджують можливість виявлення вторгнень, моніторинг системи; автоматизовані механізми, що підтримують та, або впроваджують моніторинг вхідного,	

	вихідного комунікаційного трафіку].

SI-4(5)	**МОНІТОРИНГ СИСТЕМИ - СИСТЕМНІ СПОВІЩЕННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-04(05)_ODP[01]	**визначено персонал або ролі, які мають бути сповіщені у разі виявлення ознак компрометації або потенційної компрометації;**
	SI-04(05)_ODP[02]	**визначені компромісні індикатори;**
	SI-04(05)	відбувається оповіщення **<SI-04(05) _ODP[01] персоналу або ролей>** при виникненні згенерованих системою **<SI-04(05) _ODP[02] індикаторів компрометації>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються засобів та методів моніторингу системи; документація засобів і методів моніторингу системи; налаштування конфігурації системи та відповідна документація; попередження, сповіщення, що генеруються на основі показників компрометації; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; розробники системи ; персонал організації, який встановлює, налаштовує та, або підтримує інформаційну систему; персонал організації, відповідальний за моніторинг системи; персонал організації, відповідальний за систему виявлення вторгнень]. **Перевірка:** [ВИБІР: Процеси організації для виявлення вторгнень, моніторинг системи; автоматизовані механізми, що підтримують та, або впроваджують можливість виявлення вторгнень, моніторингу системи; автоматизовані механізми, що підтримують та, або впроваджують попередження щодо показників компрометації].	

SI-4(6)	**МОНІТОРИНГ СИСТЕМИ - ЗАБОРОНА ДЛЯ НЕПРИВІЛЕЙОВАНИХ КОРИСТУВАЧІВ**
	[Вилучено: включено до AC-6(10)].

SI-4(7)	**МОНІТОРИНГ СИСТЕМИ - АВТОМАТИЧНЕ РЕАГУВАННЯ НА ПІДОЗРІЛІ ПОДІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-04(07)_ODP[01]	**визначено персонал з реагування на інциденти (ідентифікований за іменем та/або за роллю), який має бути повідомлений про виявлені підозрілі події;**

	SI-04(07)_ODP[02]	**визначені найменш руйнівні дії для припинення підозрілих подій;**
	SI-04(07)(a)	повідомляється персонал **<SI-04(07)_ODP[01] з реагування на інциденти>** про виявлені підозрілі події;
	SI-04(07)(b)	вживаються **<SI-04(07)_ODP[02] найменш руйнівні дії>** при виявленні підозрілих подій.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються засобів та методів моніторингу системи; проєктна документація системи; документація засобів і методів моніторингу системи; налаштування конфігурації системи та відповідна документація; попередження, повідомлення, що генеруються на основі виявлених підозрілих подій; записи дій, здійснених для припинення підозрілих подій; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; розробники системи; персонал організації, який встановлює, налаштовує та, або підтримує інформаційну систему; персонал організації, відповідальний за моніторинг системи; персонал організації, відповідальний за систему виявлення вторгнень]. **Перевірка:** [ВИБІР: Процеси організації для виявлення вторгнень, моніторинг системи; автоматизовані механізми, що підтримують та, або впроваджують можливість виявлення вторгнень, моніторингу системи; автоматизовані механізми підтримки та, або впровадження повідомлень персоналу реагування на інциденти; автоматизовані механізми, що підтримують та, або здійснюють дії щодо припинення підозрілих подій].	

SI-4(8)	**МОНІТОРИНГ СИСТЕМИ - ЗАХИСТ ІНФОРМАЦІЇ МОНІТОРИНГУ**
	[Вилучено: включено до SI-4].

SI-4(9)	**МОНІТОРИНГ СИСТЕМИ - ТЕСТУВАННЯ ЗАСОБІВ І МЕХАНІЗМІВ МОНІТОРИНГУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-04(09)_ODP	**визначена періодичність тестування інструментів і механізмів моніторингу вторгнень;**
	SI-04(09)	тестуються інструменти та механізми моніторингу вторгнень **<SI-04(09)_ ODP періодичність>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження: [**ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються тестування інструментів та механізмів моніторингу системи; документація, що підтверджує тестування засобів контролю за вторгненням; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який	

	відповідає за інформаційну безпеку; персонал організації, що встановлює, налаштовує та, або підтримує інформаційну систему; персонал організації, відповідальний за моніторинг системи; персонал організації, відповідальний за систему виявлення вторгнень]. **Перевірка:** [ВИБІР: Процеси організації для виявлення вторгнень, моніторинг системи; автоматизовані механізми, що підтримують та, або реалізують можливість виявлення вторгнень, моніторингу системи; автоматизовані механізми, що підтримують та, або впроваджують тестування засобів контролю за вторгненням].

SI-4(10)	**МОНІТОРИНГ СИСТЕМИ - ВИДИМІСТЬ ЗАШИФРОВАНИХ КОМУНІКАЦІЙ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-04(10)_ODP[01]	**визначений зашифрований трафік зв'язку, який повинен бути видимим для інструментів і механізмів моніторингу системи**
	SI-04(10)_ODP[02]	**визначені засоби моніторингу системи та механізми доступу до зашифрованого трафіку зв'язку;**
	SI-04(10)	передбачено, щоб **<SI-04(10) _ODP[01] зашифрований трафік зв'язку>** був видимим для **<SI-04(10) _ODP[02] засобів та механізмів моніторингу системи>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються засобів та методів моніторингу системи; проєктна документація системи; документація засобів і методів моніторингу системи; налаштування конфігурації системи та відповідна документація; протоколи системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який встановлює, налаштовує та, або підтримує інформаційну систему; персонал організації, відповідальний за моніторинг системи; персонал організації, відповідальний за систему виявлення вторгнень]. **Перевірка:** [ВИБІР: Процеси організації для виявлення вторгнень, моніторинг системи; автоматизовані механізми, що підтримують та, або впроваджують можливість виявлення вторгнень, моніторингу системи; автоматизовані механізми, що підтримують та, або реалізують видимість зашифрованого комунікаційного трафіку для інструментів моніторингу].	

SI-4(11)	**МОНІТОРИНГ СИСТЕМИ - АНАЛІЗ АНОМАЛІЙ ТРАФІКУ КОМУНІКАЦІЙ**
	МЕТА ОЦІНКИ:

	Визначити, чи:	
	SI-04(11)_ODP	**визначені внутрішні точки в системі, в яких необхідно аналізувати комунікаційний трафік;**
	SI-04(11)[01]	аналізується вихідний комунікаційний трафік на зовнішніх інтерфейсах системи для виявлення аномалій;
	SI-04(11)[02]	аналізується вихідний трафік зв'язку в **<SI-04(11)_ODP внутрішніх точках>** для виявлення аномалій.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються засобів та методів моніторингу системи; проєктна документація системи; документація засобів і методів моніторингу системи; налаштування конфігурації системи та відповідна документація; перелік невідповідних або незвичних дій (із наслідками для безпеки), які викликають оповіщення; попередження, повідомлення, що надаються працівникам служби безпеки; журнали або записи моніторингу системи; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; розробники системи; персонал організації, який встановлює, налаштовує та, або підтримує інформаційну систему; персонал організації, відповідальний за моніторинг системи; персонал організації, відповідальний за систему виявлення вторгнень]. **Перевірка:** [ВИБІР: Процеси організації для виявлення вторгнень, моніторинг системи; автоматизовані механізми, що підтримують та, або впроваджують можливість виявлення вторгнень, моніторингу системи; автоматизовані механізми, що підтримують та, або впроваджують автоматизовані оповіщення персоналу служби безпеки].	

SI-4(12)	**МОНІТОРИНГ СИСТЕМИ - СТВОРЕНІ ОРГАНІЗАЦІЄЮ АВТОМАТИЗОВАНІ СПОВІЩЕННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-04(12)_ODP[01]	**визначено персонал або ролі, які мають бути сповіщені, коли з'являються ознаки невідповідної або незвичної діяльності, що має вплив на безпеку або конфіденційність;**
	SI-04(12)_ODP[02]	**визначені автоматизовані механізми, що використовуються для оповіщення персоналу або ролей;**
	SI-04(12)_ODP[03]	**є дії, які викликають оповіщення персоналу, або визначені;**
	SI-04(12)	оповіщається **<SI-04(12) _ODP[01] персонал або ролі>** за допомогою **<SI-04(12) _ODP[02] автоматизованих механізмів>**, коли **<SI-04(12) _ODP[03] дії, що викликають оповіщення>** вказують на невідповідну або незвичну

		діяльність, що має вплив на безпеку або приватне життя.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються засобів та методів моніторингу системи; проєктна документація системи; документація засобів і методів моніторингу системи; налаштування конфігурації системи та відповідна документація; перелік невідповідних або незвичних дій (із наслідками для безпеки), які викликають оповіщення; попередження, повідомлення, що надаються працівникам служби безпеки; журнали або записи моніторингу системи; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; розробники системи; персонал організації, який встановлює, налаштовує та, або підтримує інформаційну систему; персонал організації, відповідальний за моніторинг системи; персонал організації, відповідальний за систему виявлення вторгнень]. **Перевірка:** [ВИБІР: Процеси організації для виявлення вторгнень, моніторинг системи; автоматизовані механізми, що підтримують та, або впроваджують можливість виявлення вторгнень, моніторингу системи; автоматизовані механізми, що підтримують та, або впроваджують автоматизовані оповіщення персоналу служби безпеки].	

SI-4(13)	**МОНІТОРИНГ СИСТЕМИ - АНАЛІЗ ТРАФІКУ ТА ШАБЛОНІВ ПОДІЙ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-04(13)(a)[01]	аналізується трафік для системи;
	SI-04(13)(a)[02]	проаналізовано патерни подій для системи;
	SI-04(13)(b)[01]	розроблені профілі, що представляють загальний трафік;
	SI-04(13)(b)[02]	розроблені профілі, що представляють патерни подій;
	SI-04(13)(c)[01]	використовуються профілі трафіку при налаштуванні пристроїв системного моніторингу;
	SI-04(13)(c)[02]	використовуються профілі подій при налаштуванні пристроїв системного моніторингу
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються засобів та методів моніторингу системи; проєктна документація системи; документація засобів і методів моніторингу системи; налаштування конфігурації системи та відповідна документація; перелік невідповідних або незвичних дій (із наслідками для безпеки), які викликають оповіщення; попередження, повідомлення, що надаються працівникам служби безпеки; журнали або записи моніторингу системи; записи аудиту системи; інші відповідні документи або записи].	

	Співбесіда: [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; розробники системи; персонал організації, який встановлює, налаштовує та, або підтримує інформаційну систему; персонал організації, відповідальний за моніторинг системи; персонал організації, відповідальний за систему виявлення вторгнень]. **Перевірка:** [ВИБІР: Процеси організації для виявлення вторгнень, моніторинг системи; автоматизовані механізми, що підтримують та, або впроваджують можливість виявлення вторгнень, моніторингу системи; автоматизовані механізми, що підтримують та, або впроваджують автоматизовані оповіщення персоналу служби безпеки].

SI-4(14)	**МОНІТОРИНГ СИСТЕМИ - ВИЯВЛЕННЯ БЕЗДРОТОВОГО ВТОРГНЕННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-04(14)[01]	використовується система виявлення бездротових вторгнень для виявлення несанкціонованих бездротових пристроїв;
	SI-04(14)[02]	використовується бездротова система виявлення вторгнень для виявлення спроб атак на систему;
	SI-04(14)[03]	використовується бездротова система виявлення вторгнень для виявлення потенційних компрометації або порушень в системі.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються засобів та методів моніторингу системи; проєктна документація системи; документація засобів і методів моніторингу системи; налаштування конфігурації системи та відповідна документація; протоколи системи; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, відповідальний за інформаційну безпеку; персонал організації, що встановлює, налаштовує та, або підтримує інформаційну систему; персонал організації, відповідальний за моніторинг системи; персонал організації, відповідальний за систему виявлення вторгнень]. **Перевірка:** [ВИБІР: Процеси організації для виявлення вторгнень; автоматизовані механізми, що підтримують та, або реалізують можливість бездротового виявлення вторгнень].	

SI-4(15)	**МОНІТОРИНГ СИСТЕМИ - ПЕРЕХІД ВІД БЕЗДРОТОВОГО ЗВ'ЯЗКУ ДО ПРОВІДНИХ МЕРЕЖ**
	МЕТА ОЦІНКИ: Визначити, чи:

	SI-04(15)	використовується система виявлення вторгнень для моніторингу трафіку бездротового зв'язку при переході від бездротової до дротової мережі.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються засобів та методів моніторингу системи; проєктна документація системи; документація засобів і методів моніторингу системи; налаштування конфігурації системи та відповідна документація; протоколи системи; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, відповідальний за інформаційну безпеку; персонал організації, що встановлює, налаштовує та, або підтримує інформаційну систему; персонал організації, відповідальний за моніторинг системи; персонал організації, відповідальний за систему виявлення вторгнень]. **Перевірка:** [ВИБІР: Процеси організації для виявлення вторгнень; автоматизовані механізми, що підтримують та, або реалізують можливість бездротового виявлення вторгнень].	

SI-4(16)	**МОНІТОРИНГ СИСТЕМИ - ЗІСТАВЛЕННЯ ІНФОРМАЦІЇ МОНІТОРИНГУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-04(16)	співвідноситься інформація з інструментів моніторингу та механізмів, що застосовуються в системі.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються засобів та методів моніторингу системи; проєктна документація системи; документація засобів і методів моніторингу системи; налаштування конфігурації системи та відповідна документація; журнали або записи кореляції подій; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який встановлює, налаштовує та, або підтримує інформаційну систему; персонал організації, відповідальний за моніторинг системи; персонал організації, відповідальний за систему виявлення вторгнень]. **Перевірка:** [ВИБІР: Процеси організації для виявлення вторгнень, моніторинг системи; автоматизовані механізми, що підтримують та, або впроваджують можливість виявлення вторгнень, моніторингу системи; автоматизовані механізми, що підтримують та, або впроваджують співвідношення інформації з інструментів моніторингу].	

SI-4(17)	**МОНІТОРИНГ СИСТЕМИ - ІНТЕГРОВАНА СИТУАЦІЙНА ОБІЗНАНІСТЬ**

	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-04(17)	співвідноситься інформація, отримана в результаті моніторингу фізичної, кібернетичної діяльності та діяльності ланцюга поставок, з метою досягнення інтегрованої, загальноорганізаційної ситуаційної обізнаності.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються засобів та методів моніторингу системи; проєктна документація системи; документація засобів і методів моніторингу системи; налаштування конфігурації системи та відповідна документація; журнали кореляції подій або записи, що є результатом фізичної, кібердіяльності та діяльності ланцюжка постачання; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який встановлює, налаштовує та, або підтримує інформаційну систему; персонал організації, відповідальний за моніторинг системи; персонал організації, відповідальний за систему виявлення вторгнень]. **Перевірка:** [ВИБІР: Процеси організації для виявлення вторгнень, моніторинг системи; автоматизовані механізми, що підтримують та, або реалізують можливість виявлення вторгнень, моніторингу системи; автоматизовані механізми, що підтримують та, або впроваджують співвідношення інформації з інструментів моніторингу].	

SI-4(18)	**МОНІТОРИНГ СИСТЕМИ - АНАЛІЗ ТРАФІКУ ТА ПРИХОВАНОЇ ЕКСФІЛЬТРАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-04(18)_ODP	**визначені внутрішні точки в системі, в яких необхідно аналізувати комунікаційний трафік;**
	SI-04(18)[01]	аналізується вихідний комунікаційний трафік на зовнішніх по відношенню до системи інтерфейсах для виявлення прихованого витоку інформації;
	SI-04(18)[02]	аналізується вихідний трафік зв'язку в **<SI-04(18)_ODP внутрішніх точках>** для виявлення прихованого витоку інформації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються засобів та методів моніторингу системи; проєктна документація системи; схема мережі; документація засобів і методів моніторингу системи; налаштування конфігурації системи та відповідна документація; журнали або записи моніторингу системи; записи аудиту системи; інші відповідні документи	

	або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, який встановлює, налаштовує та, або підтримує інформаційну систему; персонал організації, відповідальний за моніторинг системи; персонал організації, відповідальний за систему виявлення вторгнень]. **Перевірка:** [ВИБІР: Процеси організації для виявлення вторгнень, моніторинг системи; автоматизовані механізми, що підтримують та, або реалізують можливість виявлення вторгнень, моніторингу системи; автоматизовані механізми підтримки та, або реалізації аналізу вихідного комунікаційного трафіку].

SI-4(19)	**МОНІТОРИНГ СИСТЕМИ - ОСОБИ, ЯКІ ПРЕДСТАВЛЯЮТЬ БІЛЬШИЙ РИЗИК**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-04(19)_ODP[01]	**потрібен додатковий моніторинг осіб, які були визначені як такі, що становлять підвищений рівень ризику;**
	SI-04(19)_ODP[02]	**визначені джерела, які ідентифікують осіб, що становлять підвищений рівень ризику;**
	SI-04(19)	здійснюється <**SI-04(19) _ODP[01] додатковий моніторинг**> щодо осіб, які були ідентифіковані джерелами <**SI-04(19) _ODP[02] як такі, що становлять підвищений рівень ризику**>.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються моніторингу системи; проєктна документація системи; перелік осіб, які були визнані такими, що становлять підвищений рівень ризику; документація засобів і методів моніторингу системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, що встановлює, налаштовує та, або підтримує інформаційну систему; персонал організації, відповідальний за моніторинг системи]. **Перевірка:** [ВИБІР: Процеси організації для моніторингу системи; автоматизовані механізми, що підтримують та, або впроваджують можливості моніторингу системи].	

SI-4(20)	**МОНІТОРИНГ СИСТЕМИ - ПРИВІЛЕЙОВАНІ КОРИСТУВАЧІ**
	МЕТА ОЦІНКИ:

	Визначити, чи:	
	SI-04(20)_ODP	**визначено додатковий моніторинг привілейованих користувачів;**
	SI-04(20)	реалізовано **<SI-04(20)_ODP додатковий моніторинг>** привілейованих користувачів.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються моніторингу системи; проєктна документація системи; перелік осіб, які були визнані такими, що становлять підвищений рівень ризику; документація засобів і методів моніторингу системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; персонал організації, що встановлює, налаштовує та, або підтримує інформаційну систему; персонал організації, відповідальний за моніторинг системи]. **Перевірка:** [ВИБІР: Процеси організації для моніторингу системи; автоматизовані механізми, що підтримують та, або впроваджують можливості моніторингу системи].	

SI-4(21)	**МОНІТОРИНГ СИСТЕМИ - ВИПРОБУВАЛЬНІ ТЕРМІНИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-04(21)_ODP[01]	**потрібно здійснювати додатковий моніторинг за особами під час випробувального терміну;**
	SI-04(21)_ODP[02]	изначено випробувальний термін для фізичних осіб;
	SI-04(21)	здійснюється **<SI-04(21) _ODP[01] додатковий моніторинг>** осіб під час **<SI-04(21) _ODP[02] випробувального терміну>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються моніторингу системи; проєктна документація системи; документація засобів і методів моніторингу системи; налаштування конфігурації системи та відповідна документація; журнали або записи моніторингу системи; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, відповідальний за інформаційну безпеку; персонал організації, який встановлює, налаштовує та, або підтримує інформаційну систему; персонал організації, відповідальний за моніторинг системи]. **Перевірка:** [ВИБІР: Процеси організації для моніторингу системи; автоматизовані механізми, що підтримують та, або впроваджують можливості	

	моніторингу системи].

SI-4(22)	**МОНІТОРИНГ СИСТЕМИ - НЕСАНКЦІОНОВАНІ ПОСЛУГИ МЕРЕЖІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-04(22)_ODP[01]	**визначені процеси авторизації або затвердження послуги мережі;**
	SI-04(22)_ODP[02]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {audit; alert <SI-04(22)_ODP[03] персонал або ролі>};**
	SI-04(22)_ODP[03]	**визначено персонал або ролі, які повинні бути сповіщені при виявленні послуги мережі, які не були дозволені або схвалені в рамках процесів авторизації або затвердження (якщо вибрано);**
	SI-04(22)(a)	виявлено послуги мережі, які не було авторизовано або схвалено відповідно до **<SI-04(22)_ODP[01] процесів авторизації або схвалення>**;
	SI-04(22)(b)	ініціюється **<SI-04(22)_ODP[02] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** при виявленні послуги мережі, які не були дозволені або схвалені процесами авторизації або схвалення.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються моніторингу системи; проєктна документація системи; документація засобів і методів моніторингу системи; налаштування конфігурації системи та відповідна документація; журнали або записи моніторингу системи; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, відповідальний за інформаційну безпеку; персонал організації, який встановлює, налаштовує та, або підтримує інформаційну систему; персонал організації, відповідальний за моніторинг системи]. **Перевірка:** [ВИБІР: Процеси організації для моніторингу системи; автоматизовані механізми, що підтримують та, або впроваджують можливості моніторингу системи].	

SI-4(23)	**МОНІТОРИНГ СИСТЕМИ - ПРИСТРОЇ НА ОСНОВІ ХОСТА**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-04(23)_ODP[01]	**визначені механізми моніторингу на базі хоста, які мають бути впроваджені на компонентах системи;**

	SI-04(23)_ODP[02]	**визначені компоненти системи, в яких має бути впроваджений моніторинг на основі хостів;**
	SI-04(23)	реалізовано **<SI-04(23) _ODP[01] механізми моніторингу на основі хостів>** на **<SI-04(23) _ODP[02] компоненти системи>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються засобів та методів моніторингу системи; проєктна документація системи; механізми моніторингу на основі хоста; документація засобів і методів моніторингу системи; налаштування конфігурації системи та відповідна документація; перелік компонентів системи, що вимагають моніторингу на основі хоста; журнали або записи моніторингу системи; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, відповідальний за інформаційну безпеку; персонал організації, який встановлює, налаштовує та, або підтримує інформаційну систему; персонал організації, відповідальний за моніторинг хостів системи]. **Перевірка:** [ВИБІР: Процеси організації для моніторингу системи; автоматизовані механізми, що підтримують та, або впроваджують можливість моніторингу на основі хоста].	

SI-4(24)	**МОНІТОРИНГ СИСТЕМИ - ІНДИКАТОРИ КОМПРОМЕТАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-04(24)_ODP[01]	**визначені джерела, які надають індикатори компрометації;**
	SI-04(24)_ODP[02]	**визначено персонал або ролі, на які поширюватимуться індикатори компрометації;**
	SI-04(24)[01]	виявлено індикатори компрометації, надані **<SI-04(24)_ODP[01] джерелами>**;
	SI-04(24)[02]	збираються індикатори компрометації, що надаються **<SI-04(24)_ODP[01] джерелами>**;
	SI-04(24)[03]	індикатори компрометації, надані **<SI-04(24) _ODP[01] джерелами>**, поширюються на **<SI-04(24) _ODP[02] персонал або ролі>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються засобів та методів моніторингу системи; проєктна документація системи; механізми моніторингу на основі хоста; документація засобів і методів моніторингу системи; налаштування конфігурації системи та відповідна документація; перелік компонентів системи, що вимагають моніторингу на основі хоста; журнали або записи моніторингу системи; записи аудиту системи;	

	інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, відповідальний за інформаційну безпеку; персонал організації, який встановлює, налаштовує та, або підтримує інформаційну систему; персонал організації, відповідальний за моніторинг хостів системи]. **Перевірка:** [ВИБІР: Процеси організації для моніторингу системи; автоматизовані механізми, що підтримують та, або впроваджують можливість моніторингу на основі хоста].

SI-4(25)	**МОНІТОРИНГ СИСТЕМИ - АНАЛІЗ МЕРЕЖЕВОГО ТРАФІКУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-04(25)[01]	забезпечується видимість мережевого трафіку на зовнішніх системних інтерфейсах для оптимізації ефективності пристроїв моніторингу;
	SI-04(25)[02]	забезпечено видимість мережевого трафіку на ключових внутрішніх інтерфейсах системи для оптимізації ефективності пристроїв моніторингу.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються моніторингу системи; проєктна документація системи; документація засобів і методів моніторингу системи; налаштування конфігурації системи та відповідна документація; журнали або записи моніторингу системи; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; розробник системи; персонал організації, що встановлює, налаштовує та, або підтримує інформаційну систему; персонал організації, відповідальний за моніторинг хостів системи]. **Перевірка:** [ВИБІР: Процеси організації для моніторингу системи; організаційні процеси для виявлення, збору, розподілу та використання ознак компрометації; автоматизовані механізми, що підтримують та, або впроваджують можливості моніторингу системи; автоматизовані механізми, що підтримують та, або впроваджують виявлення, збір, розподіл та використання ознак компрометації].	

SI-5	**ПОПЕРЕДЖЕННЯ, РЕКОМЕНДАЦІЇ ТА ДИРЕКТИВИ З БЕЗПЕКИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-05_ODP[01]	**визначені зовнішні організації, від яких необхідно постійно отримувати оповіщення, поради та директиви щодо безпеки системи;**
	SI-05_ODP[02]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ**

		ПАРАМЕТРІВ: {<SI-05_ODP[03] персонал або ролі>; <SI-05_ODP[04] елементи>; <SI-05_ODP[05] зовнішні організації>};
	SI-05_ODP[03]	**визначено персонал або ролі, до яких мають бути доведені попередження, поради та директиви з безпеки (якщо визначено);**
	SI-05_ODP[04]	**визначені елементи в організації, до яких мають надсилатися оповіщення, поради та директиви з безпеки (якщо вони були обрані);**
	SI-05_ODP[05]	**визначені зовнішні організації, до яких мають надсилатися попередження, поради та директиви з питань безпеки (якщо вони були обрані);**
	SI-05a.	отримуються попередження, поради та директиви з безпеки системи від **<SI-05_ODP[01] зовнішніх організацій>** на постійній основі;
	SI-05b.	генеруються внутрішні сповіщення, поради та директиви з безпеки, якщо це вважається необхідним;
	SI-05c.	поширюються попередження, поради та директиви безпеки на **<SI-05_ODP[02] ВИБІРКОВЕ ЗНАЧЕННЯ(Я) ПАРАМЕТРА(ів)>**;
	SI-05d.	впроваджуються директиви з безпеки відповідно до встановлених часових рамок, або чи повідомляється організація, що їх видала, про ступінь невідповідності.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються попереджень, рекомендацій та вказівок щодо безпеки; записи попереджень щодо безпеки; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який несе відповідальність за попередження та консультування; персонал організації, що впроваджує, експлуатує, підтримує та використовує інформаційну систему; персонал організації, організаційні елементи та, або зовнішні організації, яким слід поширювати попередження, рекомендації та директиви; адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для визначення, приймання, генерування, розповсюдження та дотримання сповіщень про безпеку, рекомендацій та директив; автоматизовані механізми, що підтримують та, або впроваджують визначення, отримання, генерування та розповсюдження попереджень, рекомендацій та директив безпеки; автоматизовані механізми, що підтримують та, або впроваджують директиви безпеки].	

SI-5(1)	**ПОПЕРЕДЖЕННЯ, РЕКОМЕНДАЦІЇ ТА ДИРЕКТИВИ З БЕЗПЕКИ - АВТОМАТИЧНІ ПОПЕРЕДЖЕННЯ ТА РЕКОМЕНДАЦІЇ**
	МЕТА ОЦІНКИ: Визначити, чи:

	SI-05(01)_ODP	**визначені зовнішні організації, від яких необхідно постійно отримувати оповіщення, поради та директиви щодо безпеки системи;**
	SI-05(01)	отримуються попередження, поради та директиви щодо безпеки системи від **<SI-05_ODP[01] зовнішніх організацій>** на постійній основі;
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються попереджень, рекомендацій та вказівок щодо безпеки; проєктна документація системи; налаштування конфігурації системи та відповідна документація; автоматизовані механізми підтримки розповсюдження попереджувальної та рекомендаційної інформації щодо безпеки; записи попереджень та рекомендацій щодо безпеки; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який несе відповідальність за попередження та консультування; персонал організації, що впроваджує, експлуатує, підтримує та використовує інформаційну систему; персонал організації, організаційні елементи та, або зовнішні організації, яким слід поширювати попередження та рекомендації; адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для визначення, приймання, генерування та розповсюдження попереджень та рекомендацій щодо безпеки; автоматизовані механізми, що підтримують та, або впроваджують розповсюдження попереджень та рекомендацій щодо безпеки].	

SI-5(1)	**ПОПЕРЕДЖЕННЯ, РЕКОМЕНДАЦІЇ ТА ДИРЕКТИВИ З БЕЗПЕКИ - АВТОМАТИЧНІ ПОПЕРЕДЖЕННЯ ТА РЕКОМЕНДАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-05(01)_ODP	**визначені автоматизовані механізми, які використовуються для трансляції попередження та рекомендації інформації про безпеку в організації;**
	SI-05(01)	використовуються **<SI-05(01)_ODP автоматизовані механізми>** для трансляції попередження та рекомендації інформації з питань безпеки по всій організації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються попереджень, рекомендацій та вказівок щодо безпеки; проєктна документація системи; налаштування конфігурації системи та відповідна документація; автоматизовані механізми підтримки розповсюдження попереджувальної та рекомендаційної інформації щодо безпеки; записи попереджень та рекомендацій щодо безпеки; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який несе відповідальність за	

	попередження та консультування; персонал організації, що впроваджує, експлуатує, підтримує та використовує інформаційну систему; персонал організації, організаційні елементи та, або зовнішні організації, яким слід поширювати попередження та рекомендації; адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для визначення, приймання, генерування та розповсюдження попереджень та рекомендацій щодо безпеки; автоматизовані механізми, що підтримують та, або впроваджують розповсюдження попереджень та рекомендацій щодо безпеки].

SI-6	**ПЕРЕВІРКА ФУНКЦІЙ БЕЗПЕКИ ТА ПРИВАТНОСТІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-06_ODP[01]	**визначені функції безпеки, які необхідно перевірити на коректність роботи;**
	SI-06_ODP[02]	**визначені функції приватності, які потрібно перевіряти на коректність роботи;**
	SI-06_ODP[03]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {<SI-06_ODP[04] перехідні стани системи>; за командою користувача з відповідним привілеєм; <SI-06_ODP[05] частота>};**
	SI-06_ODP[04]	**визначені перехідні стани системи, що вимагають перевірки функцій безпеки та конфіденційності; (якщо вибрано)**
	SI-06_ODP[05]	**визначена періодичність перевірки правильності роботи функцій безпеки та приватності; (якщо вибрано)**
	SI-06_ODP[06]	**визначено персонал або ролі, які мають бути сповіщені про невдалу перевірку безпеки та приватності;**
	SI-06_ODP[07]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {вимкнути систему; перезапустити систему; <SI-06_ODP[08] альтернативна дія (дії)>};**
	SI-06_ODP[08]	**визначені альтернативні дії, які необхідно виконати при виявленні аномалій (якщо вони були обрані);**
	SI-06a.[01]	**<SI-06_ODP[01] функції безпеки>** перевірено на коректну роботу;
	SI-06a.[02]	правильно працюють **<SI-06_ODP[02] функції приватності>**;
	SI-06b.[01]	перевіряються **<SI-06_ODP[01] функції безпеки> <SI-06_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>**;
	SI-06b.[02]	перевіряються **<SI-06_ODP[02] функції приватності> <SI-06_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>**;
	SI-06c.[01]	сповіщається **<SI-06_ODP[06] персонал або ролі>** про невдалі тести перевірки безпеки;

	SI-06c.[02]	сповіщається **<SI-06_ODP[06] персонал або ролі>** про невдалі тести перевірки приватності;
	SI-06d.	ініційовано **<SI-06_ODP[07] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** при виявленні аномалій.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються перевірки функції безпеки; проєктна документація системи; налаштування конфігурації системи та відповідна документація; попередження, повідомлення про невдалі тести перевірки безпеки; перелік станів переходу системи, що вимагають перевірки функціональності безпеки; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за перевірку функцій безпеки; персонал організації, що впроваджує, експлуатує та підтримує інформаційну систему; адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку; розробник системи]. **Перевірка:** [ВИБІР: Процеси організації для перевірки функції захисту; автоматизовані механізми, що підтримують та, або реалізують можливість перевірки функції безпеки].	

SI-6(1)	**ПЕРЕВІРКА БЕЗПЕКИ ТА ФУНКЦІЙ ПРИВАТНОСТІ - СПОВІЩЕННЯ ПРО НЕУСПІШНЕ ПРОХОДЖЕННЯ ТЕСТІВ З БЕЗПЕКИ**
	[Вилучено: включено до SI-6].

SI-6(2)	**ПЕРЕВІРКА БЕЗПЕКИ ТА ФУНКЦІЙ ПРИВАТНОСТІ - АВТОМАТИЗОВАНА ПІДТРИМКА РОЗПОДІЛЕНОГО ТЕСТУВАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-06(02)[01]	впроваджені автоматизовані механізми для підтримки розподіленого тестуванням функцій безпеки;
	SI-06(02)[02]	проваджені автоматизовані механізми для підтримки розподіленого тестуванням функцій приватності.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються перевірки функції безпеки; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за перевірку функцій безпеки; персонал організації, що впроваджує, експлуатує та підтримує інформаційну систему; адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для перевірки функції захисту; автоматизовані механізми, що підтримують та, або впроваджують управління розподіленим тестуванням безпеки].	

SI-6(3)	**ПЕРЕВІРКА БЕЗПЕКИ ТА ФУНКЦІЙ ПРИВАТНОСТІ - ПОВІДОМЛЕННЯ ПРО РЕЗУЛЬТАТИ ПЕРЕВІРКИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-06(03)_ODP	**визначено персонал або ролі, призначені для отримання результатів перевірки функцій безпеки та приватності;**
	SI-06(03)[01]	повідомляються результати перевірки функцій безпеки **<SI-06(03)_ODP персоналу або ролям>**;
	SI-06(02)[02]	повідомляються результати перевірки функції конфіденційності **<SI-06(03)_ODP персоналу або ролям>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються перевірки функції безпеки; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, який відповідає за перевірку функцій безпеки; персонал організації, що впроваджує, експлуатує та підтримує інформаційну систему; адміністратори системи, мережі; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для перевірки функції захисту; автоматизовані механізми, що підтримують та, або впроваджують управління розподіленим тестуванням безпеки].	

SI-7	**ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-07_ODP[01]	**визначено програмне забезпечення, яке потребує застосування засобів перевірки цілісності для виявлення несанкціонованих змін;**
	SI-07_ODP[02]	**визначено прошивку, яка потребує застосування інструментів перевірки цілісності для виявлення несанкціонованих змін;**
	SI-07_ODP[03]	**визначена інформація, яка потребує застосування засобів перевірки цілісності для виявлення несанкціонованих змін;**
	SI-07_ODP[04]	**визначені дії, яких слід вжити при виявленні несанкціонованих змін у програмному забезпеченні;**
	SI-07_ODP[05]	**визначені дії, яких слід вжити при виявленні несанкціонованих змін у прошивці;**

	SI-07_ODP[06]	**визначені дії, яких слід вжити при виявленні несанкціонованих змін до інформації;**
	SI-07a.[01]	використовуються засоби перевірки цілісності для виявлення несанкціонованих змін у **<SI-07_ODP[01] програмному забезпеченні>**;
	SI-07a.[02]	використовуються засоби перевірки цілісності для виявлення несанкціонованих змін у **<SI-07_ODP[02] мікропрограмі>**;
	SI-07a.[03]	використовуються засоби перевірки цілісності для виявлення несанкціонованих змін до **<SI-07_ODP[03] інформації>**;
	SI-07b.[01]	виконуються **<SI-07_ODP[04] дії>** при виявленні несанкціонованих змін у програмному забезпеченні;
	SI-07b.[02]	виконуються **<SI-07_ODP[05] дії>** при виявленні несанкціонованих змін у прошивці;
	SI-07b.[03]	виконуються **<SI-07_ODP[06] дії>** при виявленні несанкціонованих змін в інформації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються цілісності програмного забезпечення, вбудованого програмного забезпечення та інформації; проєктна документація системи; налаштування конфігурації системи та відповідна документація; засоби перевірки цілісності та відповідна документація; записи, генеровані, ініційовані засобами перевірки цілісності щодо несанкціонованих змін програмного забезпечення, вбудованого програмного забезпечення та інформації; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за програмне забезпечення, програмне забезпечення та, або цілісність інформації; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи, мережі]. **Перевірка:** [ВИБІР: Програмне забезпечення, вбудоване програмне забезпечення та засоби перевірки цілісності інформації].	

SI-7(1)	**ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - ПЕРЕВІРКА ЦІЛІСНОСТІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-07(01)_ODP[01]	**визначено програмне забезпечення, для якого має бути виконана перевірка цілісності;**
	SI-07(01)_ODP[02]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {при запуску; при <SI-07(01)_ODP[03] перехідних станах або подіях, пов'язаних з безпекою>; <SI-07(01)_ODP[04] частота>};**

	SI-07(01)_ODP[03]	**визначені транзитні стани або події, пов'язані з безпекою, що вимагають перевірки цілісності (у програмному забезпеченні) (якщо вибрано);**
	SI-07(01)_ODP[04]	**визначено частоту, з якою слід виконувати перевірку цілісності (на програмному забезпеченні) (якщо вибрано);**
	SI-07(01)_ODP[05]	**визначено прошивку, для якої потрібно виконати перевірку цілісності;**
	SI-07(01)_ODP[06]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {при запуску; при <SI-07(01)_ODP[07] перехідних станах або подіях, що стосуються безпеки>; <SI-07(01)_ODP[08] частота>};**
	SI-07(01)_ODP[07]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {при запуску; при <SI-07(01)_ODP[07] перехідних станах або подіях, пов'язаних з безпекою>; <SI-07(01)_ODP[08] частота>};**
	SI-07(01)_ODP[08]	**визначено частоту, з якою слід виконувати перевірку цілісності (у прошивці) (якщо вибрано);**
	SI-07(01)_ODP[09]	**визначена інформація, щодо якої необхідно виконати перевірку цілісності;**
	SI-07(01)_ODP[10]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {при запуску; при <SI-07(01)_ODP[11] перехідних станах або подіях, пов'язаних з безпекою>; <SI-07(01)_ODP[12] частота>};**
	SI-07(01)_ODP[11]	**визначено перехідні стани або події, пов'язані з безпекою, що вимагають перевірки цілісності (інформації) (якщо вибрано);**
	SI-07(01)_ODP[12]	**визначено періодичність перевірки цілісності (інформації) (якщо вибрано);**
	SI-07(01)[01]	виконується перевірка цілісності **<SI-07(01) _ODP[01] програмного забезпечення> <SI-07(01) _ODP[02] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>;**
	SI-07(01)[02]	виконується перевірка цілісності **<SI-07(01) _ODP[05] прошивки> <SI-07(01) _ODP[06] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>;**
	SI-07(01)[03]	виконується перевірка цілісності **<SI-07(01) _ODP[09] інформації> <SI-07(01) _ODP[10] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються програмного забезпечення, вбудованого програмного забезпечення та цілісності інформації; проєктна документація системи; налаштування конфігурації системи та відповідна документація; засоби перевірки цілісності та	

	відповідна документація; записи сканування цілісності; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за програмне забезпечення, програмне забезпечення та, або цілісність інформації; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи]. **Перевірка:** [ВИБІР: Програмне забезпечення, вбудоване програмне забезпечення та засоби перевірки цілісності інформації].

SI-7(1)	**ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - ПЕРЕВІРКА ЦІЛІСНОСТІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-07(01)_ODP[01]	**визначено програмне забезпечення, для якого має бути виконана перевірка цілісності;**
	SI-07(01)_ODP[02]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {при запуску; при <SI-07(01)_ODP[03] перехідних станах або подіях, пов'язаних з безпекою>; <SI-07(01)_ODP[04] частота>};**
	SI-07(01)_ODP[03]	**визначені транзитні стани або події, пов'язані з безпекою, що вимагають перевірки цілісності (у програмному забезпеченні) (якщо вибрано);**
	SI-07(01)_ODP[04]	**визначено частоту, з якою слід виконувати перевірку цілісності (на програмному забезпеченні) (якщо вибрано);**
	SI-07(01)_ODP[05]	**визначено прошивку, для якої потрібно виконати перевірку цілісності;**
	SI-07(01)_ODP[06]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {при запуску; при <SI-07(01)_ODP[07] перехідних станах або подіях, пов'язаних з безпекою>; <SI-07(01)_ODP[08] частота>};**
	SI-07(01)_ODP[07]	**визначено перехідні стани або події, пов'язані з безпекою, що вимагають перевірки цілісності (на прошивці) (якщо вибрано);**
	SI-07(01)_ODP[08]	**визначено частоту, з якою слід виконувати перевірку цілісності (у прошивці) (якщо вибрано);**
	SI-07(01)_ODP[09]	**визначена інформація, щодо якої необхідно виконати перевірку цілісності;**
	SI-07(01)_ODP[10]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {при запуску; при <SI-07(01)_ODP[11] перехідних станах або подіях, пов'язаних з безпекою>; <SI-**

		07(01)_ODP[12] частота>};
	SI-07(01)_ODP[11]	**визначені перехідні стани або події, пов'язані з безпекою, що вимагають перевірки цілісності (інформації) (якщо вибрано);**
	SI-07(01)_ODP[12]	**визначено періодичність перевірки цілісності (інформації) (якщо вибрано);**
	SI-07(01)[01]	виконується перевірка цілісності **<SI-07(01) _ODP[01] програмного забезпечення> <SI-07(01) _ODP[02] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>**;
	SI-07(01)[02]	виконується перевірка цілісності **<SI-07(01) _ODP[05] прошивки> <SI-07(01) _ODP[06] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>**;
	SI-07(01)[03]	виконується перевірка цілісності **<SI-07(01) _ODP[09] інформації> <SI-07(01) _ODP[10] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються програмного забезпечення, вбудованого програмного забезпечення та цілісності інформації; проєктна документація системи; налаштування конфігурації системи та відповідна документація; засоби перевірки цілісності та відповідна документація; записи сканування цілісності; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за програмне забезпечення, програмне забезпечення та, або цілісність інформації; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи]. **Перевірка:** [ВИБІР: Програмне забезпечення, вбудоване програмне забезпечення та засоби перевірки цілісності інформації].	

SI-7(2)	**ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - АВТОМАТИЧНІ СПОВІЩЕННЯ ПРО ПОРУШЕННЯ ЦІЛІСНОСТІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-07(02)_ODP	**визначено персонал або ролі, яким необхідно повідомляти про виявлення розбіжностей під час перевірки цілісності;**
	SI-07(02)	застосовуються автоматизовані інструменти, які надають повідомлення **<SI-07(02)_ODP персоналу або ролям>** при виявленні розбіжностей під час перевірки цілісності.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються програмного забезпечення, вбудованого програмного забезпечення та	

	цілісності інформації; проєктна документація системи; налаштування конфігурації системи та відповідна документація; засоби перевірки цілісності та відповідна документація; записи сканування цілісності; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за програмне забезпечення, програмне забезпечення та, або цілісність інформації; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи]. **Перевірка:** [ВИБІР: Програмне забезпечення, вбудоване програмне забезпечення та засоби перевірки цілісності інформації].

SI-7(3)	**ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - ІНСТРУМЕНТИ ЦІЛІСНОСТІ З ЦЕНТРАЛІЗОВАНИМ УПРАВЛІННЯМ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-07(03)	застосовуються інструменти цілісності з централізованим управлінням.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються програмного забезпечення, вбудоване програмне забезпечення та цілісності інформації; проєктна документація системи; налаштування конфігурації системи та відповідна документація; засоби перевірки цілісності та відповідна документація; записи сканування цілісності; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за центральне управління засобами перевірки цілісності; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або впроваджують центральне управління засобами перевірки цілісності].	

SI-7(4)	**ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ – ПАКУВАННЯ З ІНДИКАЦІЄЮ ОЗНАК ЇЇ НЕСАНКЦІОНОВАНОГО РОЗКРИТТЯ**
	[Вилучено: включено до SA-12].

SI-7(5)	**ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - АВТОМАТИЧНІ ВІДПОВІДІ ПРО ПОРУШЕННЯ ЦІЛІСНОСТІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-	**вибрано одне або декілька з наступних ЗНАЧЕНЬ**

	07(05)_ODP[01]	**ПАРАМЕТРІВ: {вимкнути систему; перезапустити систему; застосувати елементи <SI-07(05)_ODP[02] контролю>};**
	SI-07(05)_ODP[02]	**визначені засоби контролю, які будуть автоматично застосовуватися при виявленні порушень цілісності (якщо вибрано);**
	SI-07(05)	виконуються **<SI-07(05)_ODP[01] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(S)>** автоматично при виявленні порушень цілісності.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються програмного забезпечення, вбудоване програмне забезпечення та цілісності інформації; проєктна документація системи; налаштування конфігурації системи та відповідна документація; засоби перевірки цілісності та відповідна документація; записи сканування цілісності; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за центральне управління засобами перевірки цілісності; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або впроваджують центральне управління засобами перевірки цілісності].	

SI-7(6)	**ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - КРИПТОГРАФІЧНИЙ ЗАХИСТ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-07(06)[01]	впроваджені криптографічні механізми для виявлення несанкціонованих змін у програмному забезпеченні;
	SI-07(06)[02]	реалізовані криптографічні механізми для виявлення несанкціонованих змін у прошивці;
	SI-07(06)[03]	впроваджені криптографічні механізми для виявлення несанкціонованих змін інформації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються програмного забезпечення, вбудоване програмне забезпечення та цілісності інформації; проєктна документація системи; налаштування конфігурації системи та відповідна документація; криптографічні механізми та супутня документація; записи виявлених несанкціонованих змін програмного забезпечення, вбудоване програмне забезпечення та інформації; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за програмне забезпечення, вбудоване програмне забезпечення та, або цілісність інформації;	

	персонал організації, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи]. **Перевірка:** [ВИБІР: Програмне забезпечення, вбудоване програмне забезпечення та засоби перевірки цілісності інформації; криптографічні механізми, що реалізують програмне забезпечення, вбудоване програмне забезпечення та цілісність інформації].

SI-7(7)	**ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - ІНТЕГРАЦІЯ ВИЯВЛЕННЯ І РЕАГУВАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-07(07)_ODP	**визначені зміни в системі, що мають відношення до безпеки;**
	SI-07(07)	виявлення **<SI-07(07)_ODP змін>** включено до можливості організації реагування на інциденти.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються програмного забезпечення, вбудоване програмне забезпечення та цілісності інформації; процедури, що стосуються реагування на події; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи реагування на події; записи інформаційного аудиту; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за програмне забезпечення, вбудоване програмне забезпечення та, або цілісність інформації; персонал організації, який відповідає за інформаційну безпеку; персонал організації, відповідальний за реагування на події]. **Перевірка:** [ВИБІР: Процеси організації для включення виявлення несанкціонованих змін, що стосуються безпеки, до можливостей реагування на аварії; програмне забезпечення, вбудоване програмне забезпечення та засоби перевірки цілісності інформації; автоматизовані механізми, що підтримують та, або впроваджують включення виявлення несанкціонованих змін, що стосуються безпеки, у можливості реагування на аварії].	

SI-7(8)	**ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - АУДИТ ВАЖЛИВИХ ПОДІЙ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-07(08)_ODP[01]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {створити запис аудиту; попередити поточного користувача; попередити <SI-07(08)_ODP[02]**

		персонал або ролі>; <SI-07(08)_ODP[03] інші дії>};
	SI-07(08)_ODP[02]	**визначено персонал або ролі, які мають бути сповіщені при виявленні потенційного порушення цілісності (якщо визначено);**
	SI-07(08)_ODP[03]	**визначені інші дії, яких слід вжити після виявлення потенційного порушення цілісності (якщо вибрано);**
	SI-07(08)[01]	передбачена можливість аудиту події при виявленні потенційного порушення цілісності;
	SI-07(08)[02]	ініціюється **<SI-07(08)_ODP[01] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** при виявленні потенційного порушення цілісності.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються програмного забезпечення, вбудованого програмного забезпечення та цілісності інформації; проєктна документація системи; налаштування конфігурації системи та відповідна документація; засоби перевірки цілісності та відповідна документація; записи сканування цілісності; записи реагування на аварії, перелік змін, що стосуються безпеки, в системі; автоматизовані інструменти, що підтримують попередження та сповіщення у разі виявлення несанкціонованих змін безпеки; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за програмне забезпечення, вбудоване програмне забезпечення та, або цілісність інформації; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи]. **Перевірка:** [ВИБІР: Програмне забезпечення, вбудоване програмне забезпечення та засоби перевірки цілісності інформації; автоматизовані механізми, що підтримують та, або реалізують можливість аудиту потенційних порушень цілісності; автоматизовані механізми, що підтримують та, або впроваджують попередження про потенційні порушення цілісності].	

SI-7(9)	**ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - ПЕРЕВІРКА ПРОЦЕСУ ЗАВАНТАЖЕННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-07(09)_ODP	**визначено компоненти системи, які потребують перевірки цілісності процесу завантаження;**
	SI-07(09)	перевіряється цілісність процесу завантаження **<SI-07(09)_ODP системних компонентів>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що	

	стосуються програмного забезпечення, вбудованого програмного забезпечення та цілісності інформації; проєктна документація системи; налаштування конфігурації системи та відповідна документація; засоби перевірки цілісності та відповідна документація; документація; записи сканувань перевірки цілісності; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за програмне забезпечення, вбудоване програмне забезпечення та, або цілісність інформації; персонал організації, який відповідає за інформаційну безпеку; розробник системи]. **Перевірка:** [ВИБІР: Програмне забезпечення, вбудоване програмне забезпечення та засоби перевірки цілісності інформації; автоматизовані механізми, що підтримують та, або впроваджують перевірку цілісності процесу завантаження].

SI-7(9)	**ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - ПЕРЕВІРКА ПРОЦЕСУ ЗАВАНТАЖЕННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-07(09)_ODP	**визначено компоненти системи, які потребують перевірки цілісності процесу завантаження;**
	SI-07(09)	перевіряється цілісність процесу завантаження **<SI-07(09)_ODP системних компонентів>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються програмного забезпечення, вбудованого програмного забезпечення та цілісності інформації; проєктна документація системи; налаштування конфігурації системи та відповідна документація; засоби перевірки цілісності та відповідна документація; документація; записи сканувань перевірки цілісності; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за програмне забезпечення, вбудоване програмне забезпечення та, або цілісність інформації; персонал організації, який відповідає за інформаційну безпеку; розробник системи]. **Перевірка:** [ВИБІР: Програмне забезпечення, вбудоване програмне забезпечення та засоби перевірки цілісності інформації; автоматизовані механізми, що підтримують та, або впроваджують перевірку цілісності процесу завантаження].	

SI-7(10)	**ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - ЗАХИСТ ЗАВАНТАЖУВАЛЬНОГО ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ**
	МЕТА ОЦІНКИ:

	Визначити, чи:	
	SI-07(10)_ODP[01]	**визначені механізми захисту цілісності завантажувальної прошивки в системних компонентах;**
	SI-07(10)_ODP[02]	**визначено компоненти системи, які потребують механізмів захисту цілісності завантажувальної прошивки;**
	SI-07(10)	реалізовано **<SI-07(10) _ODP[01] механізми>** для захисту цілісності завантажувальної прошивки у **<SI-07(10) _ODP[02] системних компонентах>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються програмного забезпечення, вбудованого програмного забезпечення та цілісності інформації; проєктна документація системи; налаштування конфігурації системи та відповідна документація; засоби перевірки цілісності та відповідна документація; записи сканувань перевірки цілісності; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за програмне забезпечення, вбудоване програмне забезпечення та, або цілісність інформації; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи]. **Перевірка:** [ВИБІР: Програмне забезпечення, вбудоване програмне забезпечення та засоби перевірки цілісності інформації; автоматизовані механізми підтримки та, або реалізації захисту цілісності завантажувального програмного забезпечення; захисні механізми, що забезпечують захист цілісності завантажувального програмного забезпечення].	

SI-7(11)	**ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - ОБМЕЖЕНЕ СЕРЕДОВИЩЕ З ОБМЕЖЕНИМИ ПРИВІЛЕЯМИ**
	[Вилучено: включено до CM-7(6)].

SI-7(12)	**ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - ПЕРЕВІРКА ЦІЛІСНОСТІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-07(12)_ODP	**визначено програмне забезпечення, встановлене користувачем, яке потребує перевірки цілісності перед виконанням;**
	SI-07(12)	перевіряється цілісність **<SI-07(12)_ODP програмне забезпечення, встановлене користувачем>** перед виконанням.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ:	

	Дослідження: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються програмного забезпечення, вбудованого програмного забезпечення та цілісності інформації; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи про перевірку цілісності; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за програмне забезпечення, вбудоване програмне забезпечення та, або цілісність інформації; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Програмне забезпечення, вбудоване програмне забезпечення та засоби перевірки цілісності інформації; автоматизовані механізми, що підтримують та, або здійснюють перевірку цілісності встановленого користувачем програмного забезпечення перед виконанням].

SI-7(13)	**ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - ВИКОНАННЯ КОДУ В ЗАХИЩЕНИХ СЕРЕДОВИЩАХ**
	[Вилучено: включено до СМ-7(7)].

SI-7(14)	**ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - ДВІЙКОВИЙ АБО МАШИННО-ВИКОНУВАНИЙ КОД**
	[Вилучено: включено до СМ-7(8)].

SI-7(15)	**ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - АВТЕНТИФІКАЦІЯ КОДУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-07(15)_ODP	**визначено компоненти програмного забезпечення або мікропрограми, які мають бути автентифіковані за допомогою криптографічних механізмів перед встановленням;**
	SI-07(15)	реалізовано криптографічні механізми для автентифікації **<SI-07(15)_ODP програмного забезпечення або компонентів мікропрограми>** перед інсталяцією.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються програмного забезпечення, вбудованого програмного забезпечення та цілісності інформації; проєктна документація системи; налаштування конфігурації системи та відповідна документація; криптографічні механізми та супутня документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за програмне забезпечення, вбудоване програмне забезпечення та, або цілісність інформації; персонал організації, який відповідає за інформаційну безпеку; адміністратори	

	системи, мережі; розробник системи]. **Перевірка:** [ВИБІР: Криптографічні механізми, що перевіряють автентичність програмного забезпечення, вбудованого програмного забезпечення перед установкою].

SI-7(16)	**ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ - ТЕРМІН ВИКОНАННЯ ПРОЦЕСУ БЕЗ НАГЛЯДУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-07(16)_ODP	**визначено максимальний період часу, протягом якого процеси можуть виконуватися без нагляду;**
	SI-07(16)	заборонено процесам виконуватися без нагляду довше, ніж **<SI-07(16)_ODP часовий період>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються цілісності програмного забезпечення та інформації; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за програмне забезпечення, вбудоване програмне забезпечення та, або цілісність інформації; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи]. **Перевірка:** [ВИБІР: Програмне забезпечення, вбудоване програмне забезпечення та засоби перевірки цілісності інформації; автоматизовані механізми, що підтримують та, або впроваджують обмеження часу на виконання процесу без нагляду].	

SI-7(17)	**ЦІЛІСНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ВБУДОВАНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ІНФОРМАЦІЇ – САМОЗАХИСТ ПРОГРАМ ВІД САМОВІЛЬНОГО ВИКОНАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-07(17)_ODP	**визначено елементи керування, які потрібно реалізувати для самозахисту програми під час виконання;**
	SC-07(17)	реалізовано **<SI-07(17)_ODP елементи керування>** для самозахисту програми під час виконання**.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика забезпечення системної та інформаційної цілісності; процедури забезпечення системної та інформаційної цілісності; процедури забезпечення програмної та інформаційної цілісності; проектна	

	документація системи; налаштування конфігурації системи та пов'язана з нею документація; перелік відомих вразливостей, усунутих інструментальними засобами виконання; план забезпечення безпеки системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за захист від спаму; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи]. **Перевірка:** [ВИБІР: Процеси організації для впровадження захисту від спаму; автоматизовані механізми, що підтримують та, або впроваджують захист від спаму].

SI-8	**ЗАХИСТ ВІД СПАМУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-08a.[01]	застосовуються механізми захисту від спаму в точках входу в систему для виявлення небажаних повідомлень;
	SI-08a.[02]	застосовуються механізми захисту від спаму в точках виходу з системи для виявлення небажаних повідомлень;
	SI-08a.[03]	застосовуються механізми захисту від спаму в точках входу в систему для реагування на небажані повідомлення;
	SI-08a.[04]	застосовуються механізми захисту від спаму в точках виходу з системи для реагування на небажані повідомлення;
	SI-08b.	оновлюються механізми захисту від спаму, коли з'являються нові випуски, відповідно до політики та процедур управління конфігурацією організації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; політика та процедури управління конфігурацією (CM-1); процедури, що стосуються захисту від спаму; механізми захисту від спаму; записи оновлення захисту від спаму; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за захист від спаму; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи]. **Перевірка:** [ВИБІР: Процеси організації для впровадження захисту від спаму; автоматизовані механізми, що підтримують та, або впроваджують захист від спаму].	

SI-8(1)	**ЗАХИСТ ВІД СПАМУ - ЦЕНТРАЛІЗОВАНЕ УПРАВЛІННЯ**
	[Вилучено: включено до PL-9].

SI-8(2)	ЗАХИСТ ВІД СПАМУ - АВТОМАТИЧНІ ОНОВЛЕННЯ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-08(02)_ODP	**визначено періодичність автоматичного оновлення механізмів захисту від спаму;**
	SI-08(02)	автоматично оновлюються механізми захисту від спаму **<SI-08(02)_ODP частота>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; політика та процедури управління конфігурацією (CM-1); процедури, що стосуються захисту від спаму; механізми захисту від спаму; записи оновлення захисту від спаму; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за захист від спаму; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи]. **Перевірка:** [ВИБІР: Процеси організації для впровадження захисту від спаму; автоматизовані механізми, що підтримують та, або впроваджують захист від спаму].	

SI-8(3)	ЗАХИСТ ВІД СПАМУ - БЕЗПЕРЕРВНЕ НАВЧАННЯ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-08(03)	впроваджені механізми захисту від спаму з можливістю навчання для більш ефективного визначення законого комунікаційного трафіку.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; політика та процедури управління конфігурацією (CM-1); процедури, що стосуються захисту від спаму; механізми захисту від спаму; записи оновлення захисту від спаму; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за захист від спаму; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи]. **Перевірка:** [ВИБІР: Процеси організації для впровадження захисту від спаму; автоматизовані механізми, що підтримують та, або впроваджують захист від спаму].	

SI-9	ОБМЕЖЕННЯ НА ВВЕДЕННЯ ІНФОРМАЦІЇ
	[Вилучено: включено до AC-2, AC-3, AC-5, AC-6].

SI-10	ПЕРЕВІРКА ВВОДУ ІНФОРМАЦІЇ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-10_ODP	**визначено вхідні дані до системи, які потребують перевірки достовірності;**
	SI-10	перевіряється дійсність синтаксису **<SI-10_ODP вхідної інформації>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; політика та процедури контролю доступу; політика та процедури розподілу обов'язків; процедури, що стосуються перевірки введення інформації; документація на автоматизовані засоби та програми для перевірки достовірності інформації; перелік введених даних, що вимагають перевірки дійсності; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за перевірку введення інформації; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або впроваджують перевірку дійсності на вході інформації].	

SI-10(1)	ПЕРЕВІРКА ВВОДУ ІНФОРМАЦІЇ - МОЖЛИВІСТЬ РУЧНОГО ПЕРЕВИЗНАЧЕННЯ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-10(01)_ODP	**визначено авторизованих осіб, які можуть користуватися можливістю ручного перевизначення;**
	SI-10(01)(a)	передбачена можливість ручного перевизначення для валідації **<SI-10_ODP інформаційних входів>**;
	SI-10(01)(b)	використання можливості ручного перевизначення обмежено лише **<SI-10(01)_ODP уповноваженими особами>**;
	SI-10(01)(c)	проводиться аудит використання можливості ручного перевизначення.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; політика та процедури контролю доступу; політика та процедури розподілу обов'язків; процедури, що стосуються перевірки введення інформації; проєктна документація системи; налаштування конфігурації системи та відповідна	

	документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за перевірку введення інформації; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи]. **Перевірка:** [ВИБІР: Процеси організації для використання можливостей ручного перевизначення; автоматизовані механізми, що підтримують та, або впроваджують можливість ручного перевизначення для перевірки вхідних даних; автоматизовані механізми, що підтримують та, або здійснюють аудит використання можливостей ручного перевизначення].

SI-10(2)	**ПЕРЕВІРКА ВВОДУ ІНФОРМАЦІЇ - ПЕРЕГЛЯД ТА УСУНЕННЯ ПОМИЛОК**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-10(02)_ODP[01]	**визначено період часу, протягом якого помилки перевірки вхідних даних мають бути переглянуті;**
	SI-10(02)_ODP[02]	**визначено період часу, протягом якого помилки валідації вхідних даних мають бути виправлені;**
	SI-10(02)[01]	переглядаються помилки валідації вхідних даних протягом **<SI-10(02)_ODP[01] часового періоду>**;
	SI-10(02)[02]	помилки валідації вводу вирішуються протягом **<SI-10(02)_ODP[02] часового проміжку>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; політика та процедури контролю доступу; політика та процедури розподілу обов'язків; процедури, що стосуються перевірки введення інформації; проєктна документація системи; налаштування конфігурації системи та відповідна документація; переглядати записи помилок перевірки введення інформації та результатів вирішення; журнали або записи помилок перевірки введення інформації; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за перевірку введення інформації; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи, мережі]. **Перевірка:** [ВИБІР: Процеси організації для перегляду та вирішення помилок перевірки вхідних даних; автоматизовані механізми, що підтримують та, або впроваджують перевірку та вирішення помилок перевірки вхідних даних].	

SI-10(3)	**ПЕРЕВІРКА ВВОДУ ІНФОРМАЦІЇ - ПЕРЕДБАЧУВАНА ПОВЕДІНКА**
	МЕТА ОЦІНКИ: Визначити, чи:

	SI-10(03)[01]	поводиться система передбачувано при отриманні невірних вхідних даних;
	SI-10(03)[02]	система поводиться задокументованим чином при отриманні недійсних вхідних даних.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються перевірки введення інформації; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за перевірку введення інформації; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують передбачувану поведінку при отриманні недійсних входів].	

SI-10(4)	**ПЕРЕВІРКА ВВОДУ ІНФОРМАЦІЇ - ЧАСОВІ ВЗАЄМОДІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-10(04)	враховується часова взаємодія між компонентами системи при визначенні відповідної реакції на невірні вхідні дані.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються перевірки введення інформації; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за перевірку введення інформації; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують передбачувану поведінку при отриманні недійсних входів].	

SI-10(5)	**ПЕРЕВІРКА ВВОДУ ІНФОРМАЦІЇ - ОБМЕЖЕННЯ ВХІДНИХ ДАНИХ ДОВІРЕНИМИ ДЖЕРЕЛАМИ І ЗАТВЕРДЖЕНИМИ ФОРМАТАМИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-10(05)_ODP[01]	**визначені довірені джерела, до яких слід обмежити використання інформаційних вхідних даних;**
	SI-10(05)_ODP[02]	**визначені формати, якими має бути обмежено використання інформаційних вхідних даних;**

	SI-10(05)	обмежено використання інформаційних вхідних даних **<SI-10(05)_ODP[01] довіреними джерелами>** та/або **<SI-10(05)_ODP[02] форматами>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються перевірки введення інформації; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за перевірку введення інформації; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи]. **Перевірка:** [ВИБІР: Автоматизовані механізми, що підтримують та, або реалізують передбачувану поведінку при отриманні недійсних входів].	

SI-10(6)	**ПЕРЕВІРКА ВВОДУ ІНФОРМАЦІЇ - ПРОФІЛАКТИКА ВВОДУ ДАНИХ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-10(06)	**визначено елементи керування, які потрібно реалізувати для самозахисту програми під час виконання;**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика цілісності системи та інформації; процедури цілісності системи та інформації; процедури перевірки вхідної інформації; проектна документація системи; налаштування конфігурації системи та відповідна документація; перелік довірених джерел вхідної інформації; перелік допустимих форматів для обмежень вхідної інформації; записи аудиту системи; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за захист від спаму; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи]. **Перевірка:** [ВИБІР: Процеси організації для впровадження захисту від спаму; автоматизовані механізми, що підтримують та, або впроваджують захист від спаму].	

SI-11	**ОБРОБКА ПОМИЛОК**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-11_ODP	**визначено персонал або ролі, яким слід повідомляти про повідомлення про помилки;**
	SI-11a.	генеруються повідомлення про помилки, які надають інформацію, необхідну для коригувальних дій, без розкриття інформації, яка може бути використана;

	SI-11b.	показувати повідомлення про помилки лише для **<SI-11_ODP персонал або ролі>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються обробки помилок системи; проєктна документація системи; налаштування конфігурації системи та відповідна документація; документація, що забезпечує структуру, зміст повідомлень про помилки; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за перевірку введення інформації; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи]. **Перевірка:** [ВИБІР: Процеси організації для обробки помилок; автоматизовані механізми, що підтримують та, або реалізують обробку помилок; автоматизовані механізми підтримки та, або реалізації управління повідомленнями про помилки].	

SI-12	**УПРАВЛІННЯ ТА ЗБЕРЕЖЕННЯ ІНФОРМАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-12[01]	здійснюється управління інформацією в системі відповідно до чинних законів, наказів, директив, положень, політик, стандартів, інструкцій та експлуатаційних вимог;
	SI-12[02]	зберігається інформація в системі відповідно до чинних законів, указів Президента, директив, положень, політик, стандартів, інструкцій та експлуатаційних вимог;
	SI-12[03]	управління інформацією, що виводиться з системи, здійснюється відповідно до чинних законів, указів Президента, директив, положень, політик, стандартів, інструкцій та операційних вимог;
	SI-12[04]	зберігається інформація, що виводиться з системи, відповідно до чинних законів, наказів, директив, положень, політик, стандартів, інструкцій та експлуатаційних вимог.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; федеральні закони, розпорядження, директиви, політика, положення, стандарти та експлуатаційні вимоги, що застосовуються до обробки та зберігання інформації; політика та процедури захисту засобів масової інформації; процедури, що стосуються обробки та збереження вихідних даних системи; записи про збереження інформації, інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за обробку та збереження інформації; персонал організації, який відповідає за інформаційну безпеку, адміністратори мережі]. **Перевірка:** [ВИБІР: Процеси організації для обробки та збереження інформації;	

	автоматизовані механізми, що підтримують та, або впроваджують обробку та збереження інформації].

SI-12(1)	**УПРАВЛІННЯ ТА ЗБЕРЕЖЕННЯ ІНФОРМАЦІЇ - ОБМЕЖЕННЯ ЕЛЕМЕНТІВ ПЕРСОНАЛЬНИХ ДАНИХ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-12(01)_ODP	**визначені елементи персональних даних у життєвому циклі інформації;**
	SI-12(01)	обмежується обробка персональних даних у життєвому циклі інформації в життєвому циклі інформації, **<SI-12(01)_ODP елементами інформації, що ідентифікує особу>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; федеральні закони, розпорядження, директиви, політика, положення, стандарти та експлуатаційні вимоги, що застосовуються до обробки та зберігання інформації; політика та процедури захисту засобів масової інформації; процедури, що стосуються обробки та збереження вихідних даних системи; записи про збереження інформації, інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за обробку та збереження інформації; персонал організації, який відповідає за інформаційну безпеку, адміністратори мережі]. **Перевірка:** [ВИБІР: Процеси організації для обробки та збереження інформації; автоматизовані механізми, що підтримують та, або впроваджують обробку та збереження інформації].	

SI-12(2)	**УПРАВЛІННЯ ТА ЗБЕРЕЖЕННЯ ІНФОРМАЦІЇ - МІНІМІЗАЦІЯ ВИКОРИСТАННЯ ПЕРСОНАЛЬНИХ ДАНИХ ПІД ЧАС ТЕСТУВАННЯ, НАВЧАННЯ ТА ДОСЛІДЖЕННІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-12(02)_ODP[01]	**визначені методи, які використовуються для мінімізації використання персональних даних для досліджень;**
	SI-12(02)_ODP[02]	**визначені методи, які використовуються для мінімізації використання персональних даних для тестування;**
	SI-12(02)_ODP[03]	**визначені методи, які використовуються для мінімізації використання персональних даних для навчання;**
	SI-12(02)[01]	використовуються **<SI-12(02)_ODP[01] методи>** для мінімізації використання персональних даних для досліджень;

	SI-12(02)[02]	використовуються **<SI-12(02)_ODP[02] методи>** для мінімізації використання персональних даних для тестування;
	SI-12(02)[03]	застосовуються **<SI-12(02)_ODP[03] методи>** для мінімізації використання персональних даних для навчання.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; федеральні закони, розпорядження, директиви, політика, положення, стандарти та експлуатаційні вимоги, що застосовуються до обробки та зберігання інформації; політика та процедури захисту засобів масової інформації; процедури, що стосуються обробки та збереження вихідних даних системи; записи про збереження інформації, інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за обробку та збереження інформації; персонал організації, який відповідає за інформаційну безпеку, адміністратори мережі]. **Перевірка:** [ВИБІР: Процеси організації для обробки та збереження інформації; автоматизовані механізми, що підтримують та, або впроваджують обробку та збереження інформації].	

SI-12(3)	**УПРАВЛІННЯ ТА ЗБЕРЕЖЕННЯ ІНФОРМАЦІЇ - ВИДАЛЕННЯ ІНФОРМАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-12(03)_ODP[01]	**визначені методи, які використовуються для знищення інформації після закінчення терміну зберігання;**
	SI-12(03)_ODP[02]	**визначені методи, які використовуються для знищення інформації після закінчення терміну зберігання;**
	SI-12(03)_ODP[03]	**визначені методи, які використовуються для видалення інформації після закінчення терміну зберігання;**
	SI-12(03)[01]	використовуються **<SI-12(03)_ODP[01] методи>** для знищення інформації після закінчення терміну зберігання;
	SI-12(03)[02]	використовуються **<SI-12(03)_ODP[02] методи>** для знищення інформації після закінчення терміну зберігання;
	SI-12(03)[03]	використовуються **<SI-12(03)_ODP[03] методи>** для стирання інформації після закінчення періоду зберігання.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика цілісності системи та інформації; федеральні закони, розпорядження, директиви, політика, положення, стандарти та експлуатаційні вимоги, що застосовуються до обробки та зберігання інформації; політика та процедури захисту засобів масової інформації; процедури, що стосуються обробки та збереження вихідних даних системи; записи про збереження інформації, інші відповідні документи чи записи].	

	Співбесіда: [ВИБІР: Персонал організації, відповідальний за обробку та збереження інформації; персонал організації, який відповідає за інформаційну безпеку, адміністратори мережі]. Перевірка: [ВИБІР: Процеси організації для обробки та збереження інформації; автоматизовані механізми, що підтримують та, або впроваджують обробку та збереження інформації].

SI-13	**ПЕРЕДБАЧУВАНЕ ЗАПОБІГАННЯ ЗБОЇВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-13_ODP[01]	**визначені компоненти системи, для яких необхідно визначити середній час до збою (MTTF);**
	SI-13_ODP[02]	**визначені критерії заміни за середнім часом напрацювання до збою (MTTF), які будуть використовуватися для заміни активних і резервних компонентів;**
	SI-13a.	визначено середній час напрацювання до збою (MTTF) для **<SI-13_ODP[01] системних компонентів>** у конкретних умовах експлуатації;
	SI-13b.	передбачені замінні компоненти системи та засоби заміни активних і резервних компонентів відповідно до **<SI-13_ODP[02] критеріїв заміни середнього часу напрацювання на відмову (MTTF) >**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР З: Політика цілісності системи та інформації; процедури, що стосуються передбачуваного запобігання збоїв; проєктна документація системи; налаштування конфігурації системи та відповідна документація; перелік критеріїв заміщення MTTF; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР З: Персонал організації, відповідальний за визначення та діяльність MTTF; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи, мережі; персонал організації, відповідальний за планування на випадок непередбачених ситуацій]. **Перевірка:** [ВИБІР З: Процеси організації для управління MTTF].	

SI-13(1)	**ЗАПОБІГАННЯ ПЕРЕДБАЧУВАНИХ ЗБОЇВ - ВІДПОВІДАЛЬНІСТЬ ЗА ПЕРЕДАЧУ ФУНКЦІЙ КОМПОНЕНТІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-13(01)_ODP	**визначено частку або відсоток середнього часу напрацювання до збою, в межах якого обов'язки**

		компонента системи можуть бути передані компоненту, що замінює його;
	SI-13(01)	виводяться компоненти системи з експлуатації шляхом передачі обов'язків компонентів на запасні компоненти не пізніше, ніж **<SI-13(01)_ODP частка або відсоток>** середнього напрацювання на відмову.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР З: Політика цілісності системи та інформації; процедури, що стосуються передбачуваного запобігання збоїв; проєктна документація системи; налаштування конфігурації системи та відповідна документація; перелік критеріїв заміщення MTTF; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР З: Персонал організації, відповідальний за визначення та діяльність MTTF; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи, мережі; персонал організації, відповідальний за планування на випадок непередбачених ситуацій]. **Перевірка:** [ВИБІР З: Процеси організації для управління MTTF].	

SI-13(2)	**ЗАПОБІГАННЯ ПЕРЕДБАЧУВАНИХ ЗБОЇВ - ТЕРМІН ВИКОНАННЯ ПРОЦЕСУ БЕЗ НАГЛЯДУ**
	[Вилучено: включено до SI-7 (16)].

SI-13(3)	**ЗАПОБІГАННЯ ПЕРЕДБАЧУВАНИХ ЗБОЇВ - РУЧНА ПЕРЕДАЧА ФУНКЦІЙ КОМПОНЕНТІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-13(03)_ODP	**визначено відсоток середнього часу напрацювання на відмову для передач, які потрібно ініціювати вручну;**
	SI-13(03)	ініціюються вручну передачі між активним та резервним компонентами системи, коли використання активного компонента досягає **<SI-13(03)_ODP відсоток>** від середнього часу напрацювання до збою.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються передбачуваного запобігання відмов; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за діяльність MTTF; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи, мережі; персонал організації, відповідальний за планування на випадок непередбачених ситуацій]. **Перевірка:** [ВИБІР: Процеси організації для управління MTTF та проведення ручного перенесення між активними та резервними компонентами].	

SI-13(4)	**ЗАПОБІГАННЯ ПЕРЕДБАЧУВАНИХ ЗБОЇВ - ВСТАНОВЛЕННЯ РЕЗЕРВНИХ КОМПОНЕНТІВ ТА ОПОВІЩЕННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-13(04)_ODP[01]	**визначено період часу для встановлення резервних компонентів;**
	SI-13(04)_ODP[02]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {активувати <SI-13(04)_ODP[03] сигнал>; автоматично вимкнути систему; <SI-13(04)_ODP[04] дію>};**
	SI-13(04)_ODP[03]	**потрібно активувати сигнал при виявленні несправностей компонентів системи (якщо вибрано);**
	SI-13(04)_ODP[04]	**визначено дії, яких слід вжити при виявленні відмов компонентів системи (якщо вибрано);**
	SI-13(04)(a)	успішно і прозоро встановлюються резервні компоненти протягом **<SI-13(04)_ODP[01] часу>**, якщо виявлено збої у роботі системних компонентів;
	SI-13(04)(b)	виконується **<SI-13(04)_ODP[02] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА(S)>** у разі виявлення збоїв компонентів системи.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються передбачуваного запобігання відмов; проєктна документація системи; налаштування конфігурації системи та відповідна документація; перелік дій, які слід вжити після виявлення несправності компонента системи; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за діяльність MTTF; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи, мережі; персонал організації, відповідальний за планування на випадок непередбачених ситуацій]. **Перевірка:** [ВИБІР: Процеси організації для управління MTTF; автоматизовані механізми, що підтримують та, або впроваджують прозорий монтаж резервних компонентів; автоматизовані механізми, що підтримують та, або реалізують аварійні сигнали або вимкнення системи у разі виявлення несправностей компонентів].	

SI-13(5)	**ЗАПОБІГАННЯ ПЕРЕДБАЧУВАНИХ ЗБОЇВ - МОЖЛИВІСТЬ АВАРІЙНОГО ПЕРЕМИКАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	

	SI-13(05)_ODP[01]	**вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {реальний час; близький до реального часу};**
	SI-13(05)_ODP[02]	**була визначена можливість обходу відмови для системи;**
	SI-13(05)	передбачено для системи <SI-13(05) _ODP[01] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА> <SI-13(05) _ODP[02] можливість обходу відмови>.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються передбачуваного запобігання відмов; проєктна документація системи; налаштування конфігурації системи та відповідна документація; документація, що описує можливість відмови, передбачена для системи; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за можливість відмови; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи, мережі; персонал організації, відповідальний за планування на випадок непередбачених ситуацій]. **Перевірка:** [ВИБІР: Процеси організації для управління відмовостійкими можливостями; автоматизовані механізми, що підтримують та, або реалізують можливість відмови].	

SI-14	**НЕСТІЙКІСТЬ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-14_ODP[01]	**визначені непостійні компоненти системи та сервіси, які необхідно застосовувати;**
	SI-14_ODP[02]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {по закінченні сеансу використання; <SI-14_ODP[03] частота>};**
	SI-14_ODP[03]	**визначено частоту завершення роботи непостійних компонентів і сервісів, які ініціюються у відомому стані (якщо вибрано);**
	SI-14[01]	реалізовано непостійні <SI-14_ODP[01] компоненти системи та сервіси>, які ініціюються у відомому стані;
	SI-14[02]	припиняються непостійні **<SI-14_ODP[01] компоненти системи та служби> <SI-14_ODP[02] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються передбачуваного запобігання відмов; проєктна документація системи; налаштування конфігурації системи та відповідна документація;	

	документація, що описує можливість відмови, передбачена для системи; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за можливість відмови; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи, мережі; персонал організації, відповідальний за планування на випадок непередбачених ситуацій]. **Перевірка:** [ВИБІР: Процеси організації для управління відмовостійкими можливостями; автоматизовані механізми, що підтримують та, або реалізують можливість відмови].

SI-14(1)	**НЕСТІЙКІСТЬ - ОНОВЛЕННЯ З НАДІЙНИХ ДЖЕРЕЛ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-14(01)_ODP	**визначені надійні джерела для отримання програмного забезпечення та даних для оновлення системних компонентів і служб;**
	SI-14(01)	програмне забезпечення та дані, що використовуються під час оновлення системних компонентів та служб, отримані з **<SI-14(01)_ODP довірених джерел>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються непостійності компонентів системи; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за отримання оновлення компонентів та послуг із надійних джерел; персонал організації, який відповідає за інформаційну безпеку]. **Перевірка:** [ВИБІР: Процеси організації для визначення та отримання оновлення компонентів та послуг із надійних джерел; автоматизовані механізми, що підтримують та, або впроваджують оновлення компонентів та послуг].	

SI-14(2)	**НЕСТІЙКІСТЬ - НЕСТІЙКА ІНФОРМАЦІЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-14(02)_ODP[01]	**вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {оновлювати <SI-14(02)_ODP[02] інформацію> < SI-14(02)_ODP[03] частота>; генерувати < SI-14(02)_ODP[04] інформація> на вимогу};**
	SI-14(02)_ODP[02]	**визначено інформацію, яку потрібно оновити (якщо вибрано);**
	SI-	**визначено частоту оновлення інформації (якщо вибрано);**

	14(02)_ODP[03]	
	SI-14(02)_ODP[04]	**визначено інформацію, яку потрібно згенерувати (якщо вибрано);**
	SI-14(02)(a)	виконується **<SI-14(02)_ODP[01] ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>**;
	SI-14(02)(b)	видаляється інформація, коли вона більше не потрібна.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються фільтрації вихідної інформації; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за перевірку виводу інформації; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи]. **Перевірка:** [ВИБІР: Процеси організації для перевірки виводу інформації; автоматизовані механізми, що підтримують та, або здійснюють перевірку виводу інформації].	

SI-14(3)	**НЕСТІЙКІСТЬ - НЕСТІЙКІ ПІДКЛЮЧЕННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-14(03)_ODP	**вибрано одне з наступних ЗНАЧЕНЬ ПАРАМЕТРА: {завершення запиту; період невикористання};**
	SI-14(03)[01]	встановлюються з'єднання з системою на вимогу;
	SI-14(03)[02]	припиняються з'єднання з системою після **<SI-14(03)_ODP ВИБРАНЕ ЗНАЧЕННЯ ПАРАМЕТРА>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються фільтрації вихідної інформації; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за перевірку виводу інформації; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи]. **Перевірка:** [ВИБІР: Процеси організації для перевірки виводу інформації; автоматизовані механізми, що підтримують та, або здійснюють перевірку виводу інформації].	

SI-15	**ФІЛЬТРАЦІЯ ВИХІДНИХ ДАНИХ**

	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-15_ODP	**визначені програми та/або додатки, виведення інформації з яких потребує перевірки;**
	SI-15	перевіряється інформація, що виводиться з **<SI-15_ODP програмне забезпечення та/або додатки>**, щоб переконатися, що інформація відповідає очікуваному змісту.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються фільтрації вихідної інформації; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за перевірку виводу інформації; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи]. **Перевірка:** [ВИБІР: Процеси організації для перевірки виводу інформації; автоматизовані механізми, що підтримують та, або здійснюють перевірку виводу інформації].	

SI-16	**ЗАХИСТ ПАМ'ЯТІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-16_ODP	**визначено засоби контролю для захисту системної пам'яті від несанкціонованого виконання коду;**
	SI-16	реалізовано **<SI-16_ODP контроль>** для захисту системної пам'яті від несанкціонованого виконання коду.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються фільтрації вихідної інформації; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за перевірку виводу інформації; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи]. **Перевірка:** [ВИБІР: Процеси організації для перевірки виводу інформації; автоматизовані механізми, що підтримують та, або здійснюють перевірку виводу інформації].	

SI-17	**ВІДМОВОСТІЙКІ ПРОЦЕДУРИ**
	МЕТА ОЦІНКИ:

	Визначити, чи:	
	SI-17_ODP[01]	**визначені відмовостійкі процедури, пов'язані з умовами відмови;**
	SI-17_ODP[02]	**визначено перелік умов відмови, що вимагають відмовостійких процедур;**
	SI-17	реалізовано **<SI-17_ODP[01] процедури захисту від збоїв>** при виникненні **<SI-17_ODP[02] перелік умов збою>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються захисту пам'яті для системи; проєктна документація системи; налаштування конфігурації системи та відповідна документація; перелік засобів безпеки, що захищають пам'ять системи від несанкціонованого виконання коду; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за процедури захисту; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи]. **Перевірка:** [ВИБІР: Організаційні процедури захисту; автоматизовані механізми, що підтримують та, або впроваджують процедури захисту].	

SI-18	**ОПЕРАЦІЇ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ДАНИХ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-18_ODP[01]	**визначено періодичність перевірки точності персональну інформацію протягом життєвого циклу інформації;**
	SI-18_ODP[02]	**визначено періодичність перевірки актуальності персональної інформації протягом життєвого циклу інформації;**
	SI-18_ODP[03]	**визначено періодичність перевірки актуальності персональної інформації протягом життєвого циклу інформації;**
	SI-18_ODP[04]	**визначено періодичність перевірки повноти персональної інформації протягом життєвого циклу інформації;**
	SI-18a.[01]	перевіряється точність персональної інформації протягом життєвого циклу інформації **<SI-18_ODP[01] частота>**;
	SI-18a.[02]	перевіряється актуальність персональної інформації протягом життєвого циклу інформації **< SI-18_ODP[02] частота>**;
	SI-18a.[03]	перевіряється своєчасність персональної інформації протягом життєвого циклу інформації **<частота SI-18_ODP[03]>**;
	SI-18a.[04]	перевіряється повнота персональної інформації протягом життєвого циклу інформації **<SI-18_ODP[04] частота>**;

	SI-18b.	потрібно виправити або видалити неточну або застарілу персональну інформацію.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються захисту пам'яті для системи; проєктна документація системи; налаштування конфігурації системи та відповідна документація; перелік засобів безпеки, що захищають пам'ять системи від несанкціонованого видалення інформації; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за процедури захисту; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи]. **Перевірка:** [ВИБІР: Організаційні процедури захисту; автоматизовані механізми, що підтримують та, або впроваджують процедури захисту].	

SI-18(1)	**ОПЕРАЦІЇ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ДАНИХ - АВТОМАТИЧНА ПІДТРИМКА**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-18(01)_ODP	**визначені автоматизовані механізми, які використовуються для виправлення або видалення персональної інформації яка є неточною, застарілою, неправильно визначеною щодо впливу або неправильно деідентифікованою;**
	SI-18(01)	використовуються **<SI-18(01)_ODP автоматизовані механізми>** для виправлення або видалення персональної інформації яка є неточною, застарілою, неправильно визначеною щодо впливу або неправильно деідентифікованою.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються фільтрації вихідної інформації; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за перевірку виводу інформації; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи]. **Перевірка:** [ВИБІР: Процеси організації для перевірки виводу інформації; автоматизовані механізми, що підтримують та, або здійснюють перевірку виводу інформації].	

SI-18(2)	**ОПЕРАЦІЇ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ДАНИХ - ТЕГУВАННЯ ДАНИХ**
	МЕТА ОЦІНКИ:

	Визначити, чи:	
	SI-18(02)	використовуються мітки даних для автоматизації виправлення або видалення персональної інформації протягом життєвого циклу інформації в системах організації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються фільтрації вихідної інформації; проєктна документація системи; налаштування конфігурації системи та відповідна документація; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за маркування даних; персонал організації, відповідальний за інформаційну безпеку та конфіденційність]. **Перевірка:** [ВИБІР: Механізми тегування даних; автоматизовані механізми, що підтримують та/або реалізують тегування даних].	

SI-18(3)	**ОПЕРАЦІЇ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ДАНИХ - ЗБИРАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-18(03)	збирається персональна інформація безпосередньо від особи.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика цілісності системи та інформації; процедури цілісності системи та інформації; політика обробки персональних даних; документація з конфігурації системи; записи аудиту системи; користувацький інтерфейс, де збирається персональна інформація; план захисту інформації системи; план забезпечення конфіденційності; оцінка впливу на конфіденційність; документація з оцінки ризиків для конфіденційності; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за збір даних; персонал організації, відповідальний за інформаційну безпеку та конфіденційність]. **Перевірка:** [ВИБІР: Механізми збору даних; автоматизовані механізми, що підтримують та/або підтверджують збір даних безпосередньо від особи].	

SI-18(4)	**ОПЕРАЦІЇ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ДАНИХ - ІНДИВІДУАЛЬНІ ЗАПИТИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-18(04)	виправляється або видаляється персональну інформація на вимогу осіб або їхніх уповноважених представників.

	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика цілісності системи та інформації; процедури цілісності системи та інформації; політика обробки персональних даних; документація з конфігурації системи; записи аудиту системи; користувацький інтерфейс, де збирається персональна інформація; план захисту інформації системи; план забезпечення конфіденційності; оцінка впливу на конфіденційність; документація з оцінки ризиків для конфіденційності; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за збір даних; персонал організації, відповідальний за інформаційну безпеку та конфіденційність]. **Перевірка:** [ВИБІР: Механізми збору даних; автоматизовані механізми, що підтримують та/або підтверджують збір даних безпосередньо від особи].

SI-18(5)	**ОПЕРАЦІЇ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ДАНИХ - ПОВІДОМЛЕННЯ ПРО ВИПРАВЛЕННЯ ЧИ ВИДАЛЕННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-18(05)_ODP	**визначені одержувачі персональних даних, які повинні бути повідомлені про виправлення або видалення персональних даних;**
	SI-18(05)	**<SI-18(05)_ODP одержувачі>** та фізичні особи повідомляються про виправлення або видалення персональної інформації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика цілісності системи та інформації; процедури цілісності системи та інформації; політика обробки персональних даних; документація з конфігурації системи; записи аудиту системи; користувацький інтерфейс, де збирається персональна інформація; план захисту інформації системи; план забезпечення конфіденційності; оцінка впливу на конфіденційність; документація з оцінки ризиків для конфіденційності; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за збір даних; персонал організації, відповідальний за інформаційну безпеку та конфіденційність]. **Перевірка:** [ВИБІР: Механізми збору даних; автоматизовані механізми, що підтримують та/або підтверджують збір даних безпосередньо від особи].	

SI-19	**ДЕІДЕНТИФІКАЦІЯ**
	МЕТА ОЦІНКИ: Визначити, чи:

	SI-19_ODP[01]	**визначені елементи персональної інформації, які мають бути вилучені з наборів даних;**
	SI-19_ODP[02]	**визначено частоту, з якою слід оцінювати ефективність деідентифікації;**
	SI-19a.	вилучено **<SI-19_ODP[01] елементи>** з наборів даних;
	SI-19b.	оцінюється ефективність деідентифікації **<SI-19_ODP[02] частота>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються захисту пам'яті для системи; політики управління даними**;** проєктна документація системи; налаштування конфігурації системи та відповідна документація; перелік засобів безпеки, що захищають дані в системі; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за процедури захисту; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи]. **Перевірка:** [ВИБІР: Організаційні процедури захисту; автоматизовані механізми, що підтримують та, або впроваджують процедури захисту; механізми видалення персональних даних].	

SI-19(1)	**ДЕІДЕНТИФІКАЦІЯ - ЗБІР**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-19(01)	деідентифікується набір даних після збору шляхом відмови від збору персональної інформації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються захисту пам'яті для системи; політики управління даними**;** проєктна документація системи; налаштування конфігурації системи та відповідна документація; перелік засобів безпеки, що захищають дані в системі; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за процедури захисту; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи]. **Перевірка:** [ВИБІР: Організаційні процедури захисту; автоматизовані механізми, що підтримують та, або впроваджують процедури захисту; механізми видалення персональних даних].	

SI-19(2)	**ДЕІДЕНТИФІКАЦІЯ - АРХІВАЦІЯ**
	МЕТА ОЦІНКИ:

	Визначити, чи:	
	SI-19(02)	заборонено архівування елементів персональної інформації, якщо ці елементи в наборі даних не будуть потрібні після того, як набір даних буде заархівовано.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються захисту пам'яті для системи; політики управління даними**;** проєктна документація системи; налаштування конфігурації системи та відповідна документація; перелік засобів безпеки, що захищають дані в системі; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за процедури захисту; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи]. **Перевірка:** [ВИБІР: Організаційні процедури захисту; автоматизовані механізми, що підтримують та, або впроваджують процедури захисту; механізми видалення персональних даних].	

SI-19(3)	**ДЕІДЕНТИФІКАЦІЯ - ВИДАЛЕННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-19(03)	видаляються елементи персональної інформаціїз набору даних перед його оприлюдненням, якщо ці елементи в наборі даних не повинні бути частиною оприлюднення даних.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються захисту пам'яті для системи; політики управління даними**;** проєктна документація системи; налаштування конфігурації системи та відповідна документація; перелік засобів безпеки, що захищають дані в системі; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за процедури захисту; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи]. **Перевірка:** [ВИБІР: Організаційні процедури захисту; автоматизовані механізми, що підтримують та, або впроваджують процедури захисту; механізми видалення персональних даних].	

SI-19(4)	**ДЕІДЕНТИФІКАЦІЯ - ВИДАЛЕННЯ, МАСКУВАННЯ, ШИФРУВАННЯ, ХЕШУВАННЯ АБО ЗАМІНА ПРЯМИХ ІДЕНТИФІКАТОРІВ**
	МЕТА ОЦІНКИ: Визначити, чи:

	SI-19(04)	були прямі ідентифікатори в наборі даних видалені, замасковані, зашифровані, хешовані або замінені.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються захисту пам'яті для системи; політики управління даними**;** проєктна документація системи; налаштування конфігурації системи та відповідна документація; перелік засобів безпеки, що захищають дані в системі; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за процедури захисту; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи]. **Перевірка:** [ВИБІР: Організаційні процедури захисту; автоматизовані механізми, що підтримують та, або впроваджують процедури захисту; механізми збору та видалення персональних даних].	

SI-19(5)	**ДЕІДЕНТИФІКАЦІЯ - КОНТРОЛЬ СТАТИСТИЧНОГО РОЗКРИТТЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-19(05)[01]	не маніпулюють числовими даними так, щоб у результатах аналізу не можна було ідентифікувати жодну особу чи організацію;
	SI-19(05)[02]	не маніпулюють таблицями непередбачених обставин таким чином, щоб у результатах аналізу не можна було ідентифікувати жодну особу чи організацію;
	SI-19(05)[03]	не маніпулюють статистичними даними так, щоб за результатами аналізу не можна було ідентифікувати жодну особу чи організацію.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються захисту пам'яті для системи; політики управління даними**;** проєктна документація системи; налаштування конфігурації системи та відповідна документація; перелік засобів безпеки, що захищають дані в системі; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за процедури захисту; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи]. **Перевірка:** [ВИБІР: Організаційні процедури захисту; автоматизовані механізми, що підтримують та, або впроваджують процедури захисту; механізми збору та видалення персональних даних].	

SI-19(6)	**ДЕІДЕНТИФІКАЦІЯ - ДИФЕРЕНЦІЙОВАНА КОНФІДЕНЦІЙНІСТЬ**

	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-19(06)	запобігає розголошенню персональної інформації, додавання недетермінованого шуму до результатів математичних операцій до того, як результати будуть повідомлені.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються захисту пам'яті для системи; політики управління даними**;** проєктна документація системи; налаштування конфігурації системи та відповідна документація; перелік засобів безпеки, що захищають дані в системі; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за процедури захисту; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи]. **Перевірка:** [ВИБІР: Організаційні процедури захисту; автоматизовані механізми, що підтримують та, або впроваджують процедури захисту; механізми збору та видалення персональних даних].	

SI-19(7)	**ДЕІДЕНТИФІКАЦІЯ - ПЕРЕВІРЕНЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-19(07)[01]	виконується деідентифікація за допомогою перевірених алгоритмів;
	SI-19(07)[02]	виконується деідентифікація за допомогою програмного забезпечення, яке пройшло валідацію для реалізації алгоритмів.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються захисту пам'яті для системи; політики управління даними**;** проєктна документація системи; налаштування конфігурації системи та відповідна документація; перелік засобів безпеки, що захищають дані в системі; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за процедури захисту; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи]. **Перевірка:** [ВИБІР: Організаційні процедури захисту; автоматизовані механізми, що підтримують та, або впроваджують процедури захисту; механізми збору та видалення персональних даних].	

SI-19(8)	**ДЕІДЕНТИФІКАЦІЯ - МОТИВОВАНИЙ ПОРУШНИК**

	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-19(08)	виконується тест мотивованого зловмисника для деідентифікованого набору даних, щоб визначити, чи залишаються ідентифіковані дані або чи можна повторно ідентифікувати деідентифіковані дані.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження:** [ВИБІР: Політика цілісності системи та інформації; процедури, що стосуються захисту пам'яті для системи; політики управління даними**;** проєктна документація системи; налаштування конфігурації системи та відповідна документація; перелік засобів безпеки, що захищають дані в системі; записи аудиту системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за процедури захисту; персонал організації, який відповідає за інформаційну безпеку; адміністратори системи, мережі; розробник системи]. **Перевірка:** [ВИБІР: Організаційні процедури захисту; автоматизовані механізми, що підтримують та, або впроваджують процедури захисту; механізми збору та видалення персональних даних].	

SI-20	**ПСУВАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-20_ODP	**визначені системи або компоненти системи з даними або можливостями, що підлягають застосуванню;**
	SI-20	вбудовані дані або можливості в **<SI-20_ODP системи або компоненти системи>**, щоб визначити, чи були дані організації викрадені або неналежним чином видалені з організації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика цілісності системи та інформації; процедури цілісності системи та інформації; політика обробки персональних даних; процедури, що стосуються цілісності програмного забезпечення та інформації; проектна документація системи; налаштування конфігурації системи та пов'язана з нею документація; політика та процедури, що стосуються техніки обману в системі безпеки; план захисту інформації системи; план забезпечення конфіденційності; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за виявлення пошкоджених даних; персонал організації, відповідальний за інженерну безпеку систем; персонал організації, відповідальний за інформаційну безпеку та конфіденційність]. **Перевірка:** [ВИБІР: Автоматизовані механізми пост-інцидентного виявлення; приманки, пастки, принади та методи обману супротивників; механізми	

	виявлення та сповіщення].

SI-21	**ОНОВЛЕННЯ ІНФОРМАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-21_ODP[01]	**визначена інформація, яку потрібно оновити;**
	SI-21_ODP[02]	**визначені частоти, з якими потрібно оновлювати інформацію;**
	SI-21	**<SI-21_ODP[01] інформація >** оновлюється **<SI-21_ODP[02] частота >** або генерується на вимогу і видаляється, коли більше не потрібна.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика цілісності системи та інформації; процедури цілісності системи та інформації; політика обробки персональних даних; процедури, що стосуються цілісності програмного забезпечення та informa⌕on; проектна документація системи; налаштування конфігурації системи та відповідна документація; процедури оновлення інформації; перелік інформації, що підлягає оновленню; план захисту інформації системи; план забезпечення конфіденційності; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за оновлення інформації; персонал організації, відповідальний за інформаційну безпеку та конфіденційність; персонал організації, відповідальний за інженерну безпеку систем; розробники систем]. **Перевірка:** [ВИБІР: Механізми оновлення інформації; організаційні процеси для оновлення інформації].	

SI-22	**РІЗНОВИДИ ІНФОРМАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-22_ODP[01]	**визначені альтернативні джерела інформації для основних функцій та послуг;**
	SI-22_ODP[02]	**визначені основні функції та послуги, які потребують альтернативних джерел інформації;**
	SI-22_ODP[03]	**визначені системи або компоненти системи, які потребують альтернативного джерела інформації для виконання основних функцій або послуг;**
	SI-22a.	визначені **<SI-22_ODP[01] альтернативні джерела інформації>** для **<SI-22_ODP[02] основних функцій та послуг>;**

	SI-22b.	використовується альтернативне джерело інформації для виконання основних функцій або послуг у **<SI-22_ODP[03] системах або компонентах системи>**, коли первинне джерело інформації пошкоджене або недоступне.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика цілісності системи та інформації; процедури цілісності системи та інформації; політика обробки персональних даних; проектна документація системи; налаштування конфігурації системи та пов'язана з нею документація; перелік джерел інформації; план захисту інформації системи; план забезпечення конфіденційності; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за інформаційну безпеку та конфіденційність; персонал організації, відповідальний за інженерну безпеку систем; розробники систем]. **Перевірка:** [ВИБІР: Автоматизовані методи та механізми перетворення інформації з аналогового в цифрове середовище].	

SI-23	**ФРАГМЕНТАЦІЯ ІНФОРМАЦІЇ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SI-23_ODP[01]	**визначені обставини, які вимагають фрагментації інформації;**
	SI-23_ODP[02]	**визначена інформація, яка підлягає фрагментації;**
	SI-23_ODP[03]	**визначені системи або компоненти системи, між якими має бути розподілена фрагментована інформація;**
	SI-23a.	за **<SI-23_ODP[01] обставин>**, **<SI-23_ODP[02] інформація>** є фрагментованою;
	SI-23b.	за **<SI-23_ODP[01] обставин>** фрагментована інформація розподіляється між **<SI-23_ODP[03] системами або компонентами системи>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика цілісності системи та інформації; процедури цілісності системи та інформації; політика обробки персональних даних; процедури, що стосуються програмного забезпечення та цілісності інформації; проектна документація системи; налаштування конфігурації системи та відповідна документація; процедури ідентифікації інформації для фрагментації та розподілу між системами/компонентами системи; перелік розподіленої та фрагментованої інформації; перелік обставин, що вимагають фрагментації інформації; архітектура підприємства; архітектура безпеки системи; план захисту інформації системи; план забезпечення конфіденційності; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за інформаційну	

	безпеку та конфіденційність; персонал організації, відповідальний за інженерну безпеку систем; розробники систем, архітектори безпеки]. **Перевірка:** [ВИБІР: Процеси організації ідентифікації інформації для фрагментації та розподілу між системами/компонентами системи; автоматизовані механізми, що підтримують та/або здійснюють фрагментацію та розподіл інформації між системами/компонентами системи].

XIX. КЛАС ЗАХОДІВ ЗАХИСТУ SR — УПРАВЛІННЯ РИЗИКАМИ ЛАНЦЮГА

SR-1	**ПОЛІТИКА ТА ПРОЦЕДУРИ УПРАВЛІННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SR-01_ODP[01]	**визначено персонал або ролі, на які поширюється політика управління ризиками ланцюга постачання;**
	SR-01_ODP[02]	**визначено персонал або ролі, на які поширюються процедури управління ризиками ланцюга постачання;**
	SR-01_ODP[03]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {рівень організації; рівень завдань/бізнес-процесу; рівень системи};**
	SR-01_ODP[04]	**визначена посадова особа, відповідальна за розробку, документування та розповсюдження політики та процедур управління ризиками ланцюга постачання;**
	SR-01_ODP[05]	**визначена періодичність перегляду та оновлення поточної політики управління ризиками ланцюга постачання;**
	SR-01_ODP[06]	**є події, які вимагають перегляду та оновлення поточної політики управління ризиками ланцюга постачання;**
	SR-01_ODP[07]	**визначена періодичність перегляду та оновлення поточної процедури управління ризиками ланцюга постачання;**
	SR-01_ODP[08]	**визначені події, які вимагають перегляду та оновлення процедур управління ризиками ланцюга постачання;**
	SR-01a.[01]	розроблена та задокументована політика управління ризиками ланцюга постачання;
	SR-01a.[02]	поширюється політика управління ризиками ланцюга постачання на **<SR-01_ODP[01] персонал або ролі>**;
	SR-01a.[03]	розроблені та задокументовані процедури управління ризиками ланцюга поставок для сприяння впровадженню політики управління ризиками ланцюга поставок та відповідних контролів управління ризиками ланцюга постачання;
	SR-01a.[04]	поширюються процедури управління ризиками ланцюга постачання на **<SR-01_ODP[02] персонал або ролі>**.
	SR-01a.01(a)[01]	відповідає політика **<SR-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** управління ризиками ланцюга постачання поставленій меті;
	SR-01a.01(a)[02]	стосується політика управління ризиками ланцюга постачання **<SR-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** сфери застосування;
	SR-01a.01(a)[03]	**<SR-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ**

	ПАРАМЕТРА(ів)> політика управління ризиками ланцюга постачання враховує ролі;
SR-01a.01(a)[04]	стосується політика управління ризиками ланцюга постачання **<SR-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** розподілу обов'язків;
SR-01a.01(a)[05]	політика управління ризиками ланцюга постачання **<SR-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** враховує зобов'язання керівництва;
SR-01a.01(a)[06]	політика управління ризиками ланцюга постачання **<SR-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** передбачає координацію між організаційними одиницями;
SR-01a.01(a)[07]	стосується політика управління ризиками ланцюга постачання **<SR-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** комплаєнсу.
SR-01a.01(b)	відповідає **<SR-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** політика управління ризиками ланцюга постачання чинному законодавству, виконавчим наказам, директивам, положенням, політикам, стандартам та настановам;
SR-01b.	призначена **<SR-01_ODP[04] посадова особа>** для управління розробкою, документуванням та розповсюдженням політики та процедур управління ризиками ланцюга постачання;
SR-01c.01[01]	переглядається та оновлюється поточна політика управління ризиками ланцюга постачання **<SR-01_ODP[05] частота>**;
SR-01c.01[02]	переглядається та оновлюється поточна політика управління ризиками ланцюга постачання після **<SR-01_ODP[06] події>**;
SR-01c.02[01]	переглядаються та оновлюються поточні процедури управління ризиками ланцюга постачання **<SR-01_ODP[07] частота>**;
SR-01c.02[02]	переглядаються та оновлюються поточні процедури управління ризиками ланцюга постачання після **<SR-01_ODP[08] події>.**
ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика управління ризиками ланцюга постачання; процедури управління ризиками ланцюга постачання; план захисту інформації системи; план забезпечення конфіденційності; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за управління ризиками ланцюга постачання; персонал організації, відповідальний за інформаційну безпеку та конфіденційність; персонал організації, відповідальний за закупівлю; персонал організації, відповідальний за управління ризиками підприємства].	

SR-2	ПЛАН УПРАВЛІННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SR-02_ODP[01]	**визначені системи, компоненти системи або системні послуги, для яких розробляється план управління ризиками ланцюга постачання;**
	SR-02_ODP[02]	**визначено періодичність перегляду та оновлення плану управління ризиками ланцюга постачання;**
	SR-02a.[01]	розроблено план управління ризиками ланцюга постачання;
	SR-02a.[02]	враховує план управління ризиками ланцюга постачання ризики, пов'язані з дослідженнями та розробкою **<SR-02_ODP[01] систем, системних компонентів або системних послуг>**;
	SR-02a.[03]	враховує план управління ризиками ланцюга постачання ризики, пов'язані з проектуванням **<SR-02_ODP[01] систем, системних компонентів або системних послуг>**;
	SR-02a.[04]	враховує план управління ризиками ланцюга постачання ризики, пов'язані з виробництвом **<SR-02_ODP[01] систем, системних компонентів або системних послуг>**;
	SR-02a.[05]	враховує план управління ризиками ланцюга постачання ризики, пов'язані з придбанням **<SR-02_ODP[01] систем, системних компонентів або системних послуг>**;
	SR-02a.[06]	стосується політика управління ризиками ланцюга постачання **<SR-01_ODP[03] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** сфери застосування;
	SR-02a.[07]	враховує план управління ризиками ланцюга постачання ризики, пов'язані з інтеграцією **<SR-02_ODP[01] систем, системних компонентів або системних послуг>**;
	SR-02a.[08]	враховує план управління ризиками ланцюга постачання ризики, пов'язані з експлуатацією та обслуговуванням **<SR-02_ODP[01] систем, системних компонентів або системних послуг>**;
	SR-02a.[09]	враховує план управління ризиками ланцюга постачання ризики, пов'язані з утилізацією **<SR-02_ODP[01] систем, системних компонентів або системних послуг>**;
	SR-02b.	переглядається та оновлюється план управління ризиками ланцюга постачання **<SR-02_ODP[02] частота>** або в міру необхідності для реагування на загрози, організаційні зміни чи зміни в навколишньому середовищі;
	SR-02c.[01]	захищений план управління ризиками ланцюга постачання від несанкціонованого розголошення;
	SR-02c.[02]	захищений план управління ризиками ланцюга постачання від

		несанкціонованих змін.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика управління ризиками ланцюга постачання; процедури управління ризиками ланцюга постачання; план управління ризиками ланцюга постачання; політика придбання систем та послуг; процедури придбання систем та послуг; процедури захисту ланцюга постачання; процедури захисту плану управління ризиками ланцюга постачання від несанкціонованого розголошення та модифікації; процедури життєвого циклу розробки системи; процедури, що стосуються інтеграції вимог інформаційної безпеки та конфіденційності в процес придбання; документація щодо придбання; угоди про рівень обслуговування; контракти на придбання системи, системного компонента або системної послуги; перелік загроз ланцюга постачання; перелік заходів захисту від загроз ланцюга постачання; документація щодо життєвого циклу системи; міжорганізаційні угоди та процедури; план захисту інформації системи; план забезпечення конфіденційності; план програми забезпечення конфіденційності; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за закупівлю; персонал організації, відповідальний за інформаційну безпеку та конфіденційність; персонал організації, відповідальний за управління ризиками ланцюга постачання]. **Перевірка:** [ВИБІР: Процеси організації для визначення та документування життєвого циклу розвитку системи (SDLC); організаційні процеси для визначення ролей та обов'язків SDLC; організаційні процеси для інтеграції управління ризиками ланцюга поставок в SDLC; механізми підтримки та/або впровадження SDLC].	

SR-2(1)	**СТВОРЕННЯ КОМАНДИ УПРАВЛІННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SR-02(01)_ODP[01]	**визначено персонал, ролі та обов'язки команди з управління ризиками ланцюга постачання;**
	SR-02(01)_ODP[02]	**визначені заходи з управління ризиками постачання;**
	SR-02(01)	створена команда з управління ризиками ланцюга постачання, що складається з **<SR-02(01)_ODP[01] персонал, ролі та обов'язки>** для керівництва та підтримки **<SR-02(01)_ODP[02] діяльності з управління ризиками ланцюга постачання>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика управління ризиками ланцюга постачання; процедури управління ризиками ланцюга постачання; статутна документація групи управління ризиками ланцюга постачання; стратегія управління ризиками	

	ланцюга постачання; план впровадження управління ризиками ланцюга постачання; процедури захисту ланцюга постачання; план захисту інформації системи; план забезпечення конфіденційності; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за закупівлю; персонал організації, відповідальний за інформаційну безпеку та конфіденційність; персонал організації, відповідальний за управління ризиками ланцюга постачання; персонал організації, відповідальний за управління ризиками підприємства; юрисконсульт; персонал організації, відповідальний за безперервність бізнесу].

SR-3	**КОНТРОЛЬ ЛАНЦЮГА ПОСТАЧАННЯ І ПРОЦЕСІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SR-03_ODP[01]	**визначено систему або компонент системи, який потребує процесу або процесів для виявлення та усунення слабких місць або недоліків;**
	SR-03_ODP[02]	**визначено персонал ланцюга поставок, з яким необхідно координувати процес або процеси виявлення та усунення слабких місць або недоліків в елементах і процесах ланцюга постачання;**
	SR-03_ODP[03]	**визначені засоби контролю ланцюга постачання, що застосовуються для захисту від ризиків ланцюга постачання для системи, системного компонента або системної послуги, а також для обмеження шкоди або наслідків від подій, пов'язаних з ланцюгом постачання;**
	SR-03_ODP[04]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {плани безпеки та конфіденційності; план управління ризиками ланцюга постачання; <SR-03_ODP[05] документ>};**
	SR-03_ODP[05]	**визначено документ, що ідентифікує обрані та впроваджені процеси та засоби контролю ланцюга постачання (якщо обрано);**
	SR-03a.[01]	запроваджено процес або процеси для виявлення та усунення слабких місць або недоліків в елементах та процесах ланцюга постачання;
	SR-03a.[02]	процес або процеси виявлення та усунення слабких місць або недоліків в елементах та процесах ланцюга постачання **<SR-03_ODP[01] системи або компонента системи>** координується/координуються з **<SR-03_ODP[02] персоналом ланцюга постачання>**;
	SR-03b.	застосовуються **<SR-03_ODP[03] засоби контролю ланцюга постачання>** для захисту від ризиків ланцюга постачання для системи, системного компонента або системної послуги, а також для обмеження шкоди або наслідків від подій,

		пов'язаних з ланцюгом постачання;
	SR-03c.	задокументовані обрані та впроваджені процеси та засоби контролю ланцюга постачання в **<SR-03_ODP[04] ЗНАЧЕННЯ ВИБІРКОВОГО ПАРАМЕТРА(ів)>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика управління ризиками ланцюга постачання; процедури управління ризиками ланцюга постачання; стратегія управління ризиками ланцюга постачання; план управління ризиками ланцюга постачання; документація з інвентаризації систем та критично важливих компонентів системи; політика придбання систем та послуг; процедури придбання систем та послуг; процедури інтеграції вимог інформаційної безпеки та конфіденційності в процес придбання; документація щодо подання пропозицій; документація щодо придбання (включаючи замовлення на придбання); угоди про рівень обслуговування; контракти на придбання систем або послуг; документація щодо реєстру ризиків; план захисту інформації системи; план конфіденційності; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за закупівлю; персонал організації, відповідальний за інформаційну безпеку та конфіденційність; персонал організації, відповідальний за управління ризиками ланцюга постачання]. **Перевірка:** [ВИБІР: Процеси організації для виявлення та усунення недоліків елементів і процесів ланцюга поставок].	

SR-3(1)	**КОНТРОЛЬ ЛАНЦЮГА ПОСТАЧАННЯ І ПРОЦЕСІВ - РІЗНІ БАЗИ ПОСТАЧАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SR-03_ODP[01]	**визначено систему або компонент системи, який потребує процесу або процесів для виявлення та усунення слабких місць або недоліків;**
	SR-03_ODP[02]	**визначено персонал ланцюга постачання, з яким необхідно координувати процес або процеси виявлення та усунення слабких місць або недоліків в елементах і процесах ланцюга поставок;**
	SR-03_ODP[03]	**визначені засоби контролю ланцюга постачання, що застосовуються для захисту від ризиків ланцюга постачання для системи, системного компонента або системної послуги, а також для обмеження шкоди або наслідків від подій, пов'язаних з ланцюгом постачання;**
	SR-03_ODP[04]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {плани безпеки та конфіденційності; план управління ризиками ланцюга постачання; <SR-03_ODP[05] документ>};**

	SR-03_ODP[05]	**визначено документ, що ідентифікує обрані та впроваджені процеси та засоби контролю ланцюга постачання (якщо обрано);**
	SR-03a.[01]	запроваджено процес або процеси для виявлення та усунення слабких місць або недоліків в елементах та процесах ланцюга постачання;
	SR-03a.[02]	процес або процеси виявлення та усунення слабких місць або недоліків в елементах та процесах ланцюга постачання **<SR-03_ODP[01] системи або компонента системи>** координується/координуються з **<SR-03_ODP[02] персоналом ланцюга постачання>**;
	SR-03b.	застосовуються **<SR-03_ODP[03] засоби контролю ланцюга постачання>** для захисту від ризиків ланцюга постачання для системи, системного компонента або системної послуги, а також для обмеження шкоди або наслідків від подій, пов'язаних з ланцюгом постачання;
	SR-03c.	задокументовані обрані та впроваджені процеси та засоби контролю ланцюга постачання в **<SR-03_ODP[04] ЗНАЧЕННЯ ВИБІРКОВОГО ПАРАМЕТРА(ів)>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика управління ризиками ланцюга постачання; процедури управління ризиками ланцюга постачання; стратегія управління ризиками ланцюга постачання; план управління ризиками ланцюга постачання; документація з інвентаризації систем та критично важливих компонентів системи; політика придбання систем та послуг; процедури придбання систем та послуг; процедури інтеграції вимог інформаційної безпеки та конфіденційності в процес придбання; документація щодо подання пропозицій; документація щодо придбання (включаючи замовлення на придбання); угоди про рівень обслуговування; контракти на придбання систем або послуг; документація щодо реєстру ризиків; план захисту інформації системи; план забезпечення конфіденційності; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за закупівлю; персонал організації, відповідальний за інформаційну безпеку та конфіденційність; персонал організації, відповідальний за управління ризиками ланцюга постачання]. **Перевірка:** [ВИБІР: Процеси організації для виявлення та усунення недоліків елементів і процесів ланцюга поставок].	

SR-3(2)	**КОНТРОЛЬ ЛАНЦЮГА ПОСТАЧАННЯ І ПРОЦЕСІВ - ОБМЕЖЕННЯ ШКОДИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SR-03(02)_ODP	**визначені засоби контролю для обмеження шкоди від потенційних супротивників ланцюга постачання;**

	SR-03(02)	застосовуються <**SR-03(02)_ODP контроль**> для обмеження шкоди від потенційних супротивників, які ідентифікують та націлюються на ланцюг постачання організації.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика та процедури управління ризиками ланцюга постачання; план управління ризиками ланцюга постачання; політика придбання систем та послуг; політика управління конфігурацією; процедури захисту ланцюга постачання; процедури інтеграції вимог інформаційної безпеки в процес придбання; процедури базової конфігурації системи; план управління конфігурацією; документація з проектування системи; архітектура системи та пов'язана з нею конфігураційна документація; тендерна документація; документація щодо придбання; контракти на придбання системи, системного компонента або системної послуги; оцінки загроз; оцінки вразливостей; перелік заходів безпеки, які необхідно вжити для захисту ланцюга постачання організації від потенційних загроз ланцюга постачання; план забезпечення безпеки системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за закупівлю; персонал організації, відповідальний за інформаційну безпеку та конфіденційність; персонал організації, відповідальний за управління ризиками ланцюга постачання]. **Перевірка:** [ВИБІР: Процеси організації визначення та застосування запобіжних заходів для обмеження шкоди з боку опонентів ланцюга постачання організації; механізми, що підтримують та/або реалізують визначення та застосування запобіжних заходів для захисту ланцюга постачання організації].	

SR-3(3)	**КОНТРОЛЬ ЛАНЦЮГА ПОСТАЧАННЯ І ПРОЦЕСІВ - ПЕРЕНЕСЕННЯ ЗАХОДІВ ЗАХИСТУ УПРАВЛІННЯ РИЗИКАМИ ЛАНЦЮГА ПОСТАЧАННЯ ДО СУБПІДРЯДНИКІВ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SR-03(03)	включені засоби контролю, передбачені в контрактах з основними підрядниками, також і в контрактах з субпідрядниками.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика та процедури управління ризиками ланцюга постачання; план управління ризиками ланцюга постачання; політика придбання систем та послуг; процедури захисту ланцюга постачання; документація щодо придбання; угоди про рівень обслуговування; контракти на придбання системи, системного компонента або системної послуги; міжорганізаційні угоди та процедури; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за закупівлю; персонал організації, відповідальний за інформаційну безпеку та конфіденційність; персонал організації, відповідальний за управління ризиками	

	ланцюга постачання]. **Перевірка:** [ВИБІР: Процеси організації для встановлення міжорганізаційних угод та процедур з суб'єктами ланцюга постачання].

SR-4	**ПОХОДЖЕННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SR-04_ODP	визначені системи, компоненти системи та пов'язані з ними дані, які потребують достовірного походження;
	SR-04[01]	задокументовано дійсне походження для **<SR-04_ODP систем, компонентів системи та пов'язаних з ними даних>**;
	SR-04[02]	відстежується дійсне походження для **<SR-04_ODP систем, компонентів системи та пов'язаних з ними даних>**;
	SR-04[03]	підтримується дійсне походження для **<SR-04_ODP систем, компонентів системи та пов'язаних з ними даних>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика та процедури управління ризиками ланцюга постачання; план управління ризиками ланцюга постачання; політика придбання систем та послуг; процедури захисту ланцюга постачання; документація щодо придбання; угоди про рівень обслуговування; контракти на придбання системи, системного компонента або системної послуги; міжорганізаційні угоди та процедури; план захисту інформації системи; інші відповідні документи або записи]. **півбесіда:** [ВИБІР: Персонал організації, відповідальний за закупівлю; персонал організації, відповідальний за інформаційну безпеку та конфіденційність; персонал організації, відповідальний за управління ризиками ланцюга постачання]. **Перевірка:** [ВИБІР: Процеси організації для визначення походження критично важливих систем та компонентів критично важливих систем; механізми, що використовуються для документування, моніторингу або підтримки походження].	

SR-4(1)	**ПОХОДЖЕННЯ - ІДЕНТИЧНІСТЬ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SR-04(01)_ODP	визначені елементи ланцюга постачання, процеси та персонал, пов'язані з системами та критично важливими компонентами системи, які потребують унікальної ідентифікації;
	SR-04(01)[01]	встановлена унікальна ідентифікація **<SR-04(01)_ODP елементів ланцюга постачання, процесів та персоналу>**;

	SR-04(01)[02]	підтримується унікальна ідентифікація **<SR-04(01)_ODP елементів ланцюга постачання, процесів та персоналу>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика та процедури управління ризиками ланцюга постачання; план управління ризиками ланцюга постачання; політика придбання систем та послуг; процедури захисту ланцюга постачання; процедури інтеграції вимог інформаційної безпеки в процес придбання; перелік елементів ланцюга постачання, процесів та суб'єктів (пов'язаних із системою, компонентом системи або системною послугою), які потребують впровадження унікальних ідентифікаційних процесів, процедур, інструментів, механізмів, обладнання, методів та/або конфігурацій; план захисту інформації системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за придбання систем та послуг; персонал організації, відповідальний за інформаційну безпеку; персонал організації, відповідальний за захист ланцюга постачання; персонал організації, відповідальний за встановлення та збереження унікальної ідентифікації елементів, процесів та суб'єктів ланцюга постачання]. **Перевірка:** [ВИБІР: Процеси організації визначення, встановлення та збереження унікальної ідентифікації елементів, процесів та учасників ланцюга поставок; механізми, що підтримують та/або реалізують визначення, встановлення та збереження унікальної ідентифікації елементів, процесів та учасників ланцюга поставок].	

SR-4(2)	**ПОХОДЖЕННЯ - УНІКАЛЬНА ІДЕНТИФІКАЦІЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SR-04(02)_ODP	**визначені системи та критичні компоненти системи, які потребують унікальної ідентифікації для відстеження в ланцюгу постачання;**
	SR-04(02)[01]	встановлена унікальна ідентифікація **<SR-04(02)_ODP систем та критичних системних компонентів>** для відстеження в ланцюгу постачання;
	SR-04(01)[02]	зберігається унікальна ідентифікація **<SR-04(02)_ODP систем та критично важливих системних компонентів>** для відстеження в ланцюгу постачання.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика та процедури управління ризиками ланцюга постачання; план управління ризиками ланцюга постачання; політика придбання систем та послуг; процедури захисту ланцюга постачання; процедури інтеграції вимог інформаційної безпеки в процес придбання; перелік елементів ланцюга постачання, процесів та суб'єктів (пов'язаних із системою, компонентом системи або системною послугою), які потребують впровадження унікальних ідентифікаційних процесів, процедур, інструментів, механізмів, обладнання, методів та/або конфігурацій; план захисту інформації системи; інші відповідні	

	документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за придбання систем та послуг; персонал організації, відповідальний за інформаційну безпеку; персонал організації, відповідальний за захист ланцюга постачання; персонал організації, відповідальний за встановлення та збереження унікальної ідентифікації елементів, процесів та суб'єктів ланцюга постачання]. **Перевірка:** [ВИБІР: Процеси організації визначення, встановлення та збереження унікальної ідентифікації елементів, процесів та учасників ланцюга поставок; механізми, що підтримують та/або реалізують визначення, встановлення та збереження унікальної ідентифікації елементів, процесів та учасників ланцюга поставок].

SR-4(3)	**ПОХОДЖЕННЯ - ПЕРЕВІРКА НА СПРАВЖНІСТЬ І ВІДСУТНІСТЬ ВНЕСЕННЯ ЗМІН**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SR-04(03)_ODP[01]	**визначені засоби контролю для підтвердження того, що отримана система або компонент системи є справжньою;**
	SR-04(03)_ODP[02]	**визначені засоби контролю для перевірки того, що отримана система або компонент системи не були змінені;**
	SR-04(03)[01]	застосовуються **<SR-04(03)_ODP[01] засоби контролю>** для перевірки того, що отримана система або компонент системи є справжніми;
	SR-04(03)[02]	застосовуються **<SR-04(03)_ODP[02] засоби контролю>** для перевірки того, що отриману систему або компонент системи не було змінено.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика та процедури управління ризиками ланцюга постачання; план управління ризиками ланцюга постачання; політика придбання систем та послуг; процедури, що стосуються захисту ланцюга постачання; процедури, що стосуються принципу проектування безпеки довірених компонентів, які використовуються у специфікації, проектуванні, розробці, впровадженні та модифікації системи; документація з проектування системи; процедури, що стосуються інтеграції вимог інформаційної безпеки в процес придбання; документація щодо подання пропозицій; документація щодо придбання; угоди про рівень обслуговування; контракти на придбання системи, системного компонента або системної послуги; доказова документація (включаючи відповідні конфігурації), яка вказує на те, що система або системний компонент є справжніми і не були змінені; план забезпечення безпеки системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за придбання систем та послуг; персонал організації, відповідальний за інформаційну безпеку; персонал організації, відповідальний за управління ризиками ланцюга	

	постачання]. **Перевірка:** [ВИБІР: Процеси організації для визначення та застосування гарантій валідації; механізми, що підтримують та/або реалізують визначення та застосування гарантій валідації; механізми, що підтримують застосування принципу проектування безпеки довірених компонентів у специфікації, проектуванні, розробці, впровадженні та модифікації системи].

SR-4(4)	**ПОХОДЖЕННЯ – ПЕРЕВІРКА ЛАНЦЮГА ЦІЛІСНОСТІ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SR-04(04)_ODP[01]	**визначені засоби контролю, що застосовуються для забезпечення цілісності системи та системних компонентів;**
	SR-04(04)_ODP[02]	**визначено метод аналізу, який необхідно провести для перевірки внутрішнього складу та походження критично важливих або необхідних для виконання місії технологій, продуктів та послуг для забезпечення цілісності системи та системних компонентів;**
	SR-04(04)[01]	застосовуються **<SR-04(04)_ODP[01] засоби контролю>** для забезпечення цілісності системи та її компонентів;
	SR-04(04)[02]	проводиться **<SR-04(04)_ODP[02] метод аналізу>** для забезпечення цілісності системи та компонентів системи.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика та процедури управління ризиками ланцюга постачання; план управління ризиками ланцюга постачання; політика придбання систем та послуг; процедури захисту ланцюга постачання; специфікація матеріалів для критично важливих систем або компонентів системи; документація acquisi℘on; теги ідентифікації програмного забезпечення; декларації виробника щодо атрибутів платформи (наприклад, серійні номери, перелік апаратних компонентів) та вимірювань (наприклад, хеші прошивки), які тісно пов'язані з самим апаратним забезпеченням; план захисту інформації системи; інші відповідні документи чи записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за придбання систем та послуг; персонал організації, відповідальний за інформаційну безпеку; персонал організації, відповідальний за управління ризиками ланцюга постачання]. **Перевірка:** [ВИБІР: Процеси організації ідентифікації родовідної інформації; організаційні процеси визначення та підтвердження цілісності внутрішнього складу критичних систем та компонентів критичних систем; механізми визначення та підтвердження цілісності внутрішнього складу критичних систем та компонентів критичних систем].	

SR-5	**СТРАТЕГІЇ ПРИДБАННЯ, ІНСТРУМЕНТИ І МЕТОДИ**

	МЕТА ОЦІНКИ: Визначити, чи:	
	SR-05_ODP	**визначені стратегії закупівель, контрактні інструменти та методи закупівель для захисту, виявлення та пом'якшення ризиків ланцюга постачання;**
	SR-05[01]	застосовуються **<SR-05_ODP стратегії, інструменти та методи>** для захисту від ризиків ланцюга постачання;
	SR-05[02]	застосовуються **<SR-05_ODP стратегії, інструменти та методи>** для виявлення ризиків ланцюга постачання;
	SR-05[03]	застосовуються **<SR-05_ODP стратегії, інструменти та методи>** для зменшення ризиків ланцюга постачання.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика управління ризиками ланцюга постачання; процедури управління ризиками ланцюга постачання; план управління ризиками ланцюга постачання; політика придбання систем та послуг; процедури придбання систем та послуг; процедури захисту ланцюга постачання; процедури інтеграції вимог інформаційної безпеки та конфіденційності в процес придбання; тендерна документація; документація щодо придбання (включаючи замовлення на придбання); угоди про рівень обслуговування; контракти на придбання систем, системних компонентів або послуг; документація щодо програм підготовки, навчання та підвищення обізнаності персоналу з питань ризиків ланцюга постачання; план захисту інформації системи; план забезпечення конфіденційності; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за закупівлю; персонал організації, відповідальний за інформаційну безпеку та конфіденційність; персонал організації, відповідальний за управління ризиками ланцюга постачання]. **Перевірка:** [ВИБІР: Процеси організації для визначення та застосування спеціальних стратегій закупівель, контрактних інструментів та методів закупівель; механізми, що підтримують та/або впроваджують визначення та застосування спеціальних стратегій закупівель, контрактних інструментів та методів закупівель].	

SR-5(1)	**СТРАТЕГІЇ ПРИДБАННЯ, ІНСТРУМЕНТИ І МЕТОДИ - НАЛЕЖНЕ ПОСТАЧАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SR-05(01)_ODP[01]	**визначені засоби контролю для забезпечення адекватного постачання критично важливих компонентів системи;**
	SR-05(01)_ODP[02]	**визначені критичні компоненти системи, які потребують адекватного постачання;**

	SR-05(01)	застосовуються **<SR-05(01)_ODP[01] засоби контролю>** для забезпечення адекватного постачання **<SR-05(01)_ODP[02] критично важливих компонентів системи>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика та процедури управління ризиками ланцюга постачання; стратегія управління ризиками ланцюга постачання; план управління ризиками ланцюга постачання; документи з планування на випадок надзвичайних ситуацій; інвентаризація критично важливих систем та компонентів системи; визначення адекватного постачання; політика придбання систем та послуг; процедури захисту ланцюга постачання; процедури інтеграції вимог інформаційної безпеки в процес придбання; процедури, що стосуються інтеграції стратегій придбання, контрактних інструментів та методів закупівель у процес придбання; документація щодо подання пропозицій; документація щодо придбання; угоди про рівень обслуговування; контракти на придбання систем або послуг; замовлення/вимоги на придбання системи, системного компонента або системної послуги від постачальників; план забезпечення безпеки системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за придбання систем та послуг; персонал організації, відповідальний за інформаційну безпеку; персонал організації, відповідальний за управління ризиками ланцюга постачання]. **Перевірка:** [ВИБІР: Процеси організації для визначення та застосування спеціальних стратегій закупівель, контрактних інструментів та методів закупівель; механізми, що підтримують та/або впроваджують визначення та застосування спеціальних стратегій закупівель, контрактних інструментів та методів закупівель].	

SR-5(1)	**СТРАТЕГІЇ ПРИДБАННЯ, ІНСТРУМЕНТИ І МЕТОДИ - НАЛЕЖНЕ ПОСТАЧАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SR-05(01)_ODP[01]	**визначені засоби контролю для забезпечення адекватного постачання критично важливих компонентів системи;**
	SR-05(01)_ODP[02]	**визначені критичні компоненти системи, які потребують адекватного постачання;**
	SR-05(01)	застосовуються **<SR-05(01)_ODP[01] засоби контролю>** для забезпечення адекватного постачання **<SR-05(01)_ODP[02] критично важливих компонентів системи>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика та процедури управління ризиками ланцюга постачання; стратегія управління ризиками ланцюга постачання; план управління ризиками ланцюга постачання; документи з планування на випадок надзвичайних ситуацій; інвентаризація критично важливих систем та компонентів системи;	

	визначення адекватного постачання; політика придбання систем та послуг; процедури захисту ланцюга постачання; процедури інтеграції вимог інформаційної безпеки в процес придбання; процедури, що стосуються інтеграції стратегій придбання, контрактних інструментів та методів закупівель у процес придбання; документація щодо подання пропозицій; документація щодо придбання; угоди про рівень обслуговування; контракти на придбання систем або послуг; замовлення/вимоги на придбання системи, системного компонента або системної послуги від постачальників; план забезпечення безпеки системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за придбання систем та послуг; персонал організації, відповідальний за інформаційну безпеку; персонал організації, відповідальний за управління ризиками ланцюга постачання]. **Перевірка:** [ВИБІР: Процеси організації для визначення та застосування спеціальних стратегій закупівель, контрактних інструментів та методів закупівель; механізми, що підтримують та/або впроваджують визначення та застосування спеціальних стратегій закупівель, контрактних інструментів та методів закупівель].

SR-5(2)	**СТРАТЕГІЇ ПРИДБАННЯ, ІНСТРУМЕНТИ І МЕТОДИ - ОЦІНКА ПЕРЕД ВІДБОРОМ, ПРИЙНЯТТЯ, МОДИФІКАЦІЯ ЧИ ОНОВЛЕННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SR-05(02)[01]	оцінюється система, компонент системи або послуги системи перед відбором;
	SR-05(02)[02]	оцінюється система, компонент системи або послуги системи перед прийняттям;
	SR-05(02)[03]	оцінюється система, компонент системи або послуги системи перед модифікацією;
	SR-05(02)[04]	оцінюється система, компонент системи або послуги системи перед оновленням.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: План захисту інформації системи; політика придбання систем та послуг; процедури захисту ланцюга постачання; процедури інтеграції вимог інформаційної безпеки в процес придбання; результати тестування та оцінки безпеки; результати оцінки вразливостей; результати тестування на проникнення; результати оцінки організаційних ризиків; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за придбання систем та послуг; персонал організації, відповідальний за інформаційну безпеку; персонал організації, відповідальний за захист ланцюга постачання]. **Перевірка:** [ВИБІР: Процеси організації проведення оцінювання перед відбором, прийняттям або оновленням; механізми, що підтримують та/або реалізують проведення оцінювання перед відбором, прийняттям або оновленням].	

SR-6	ОЦІНКА ПОСТАЧАЛЬНИКІВ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SR-06_ODP	**визначена періодичність оцінки та аналізу ризиків, пов'язаних з ланцюгом постачання, що стосуються постачальників або підрядників, а також систем, компонентів системи або системних послуг, які вони надають;**
	SR-06	оцінюються та аналізуються ризики, пов'язані з ланцюгом постачання, які стосуються постачальників або підрядників та систем, компонентів системи або системних послуг, які вони надають **< SR-06_ODP частота >.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика та процедури управління ризиками ланцюга постачання; стратегія управління ризиками ланцюга постачання; план управління ризиками ланцюга постачання; політика придбання систем та послуг; процедури захисту ланцюга постачання; процедури інтеграції вимог інформаційної безпеки в процес придбання; записи перевірок належної перевірки постачальника; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за придбання систем та послуг; персонал організації, відповідальний за інформаційну безпеку; персонал організації, відповідальний за захист ланцюга постачання].**Перевірка:** [ВИБІР: Процеси організації для проведення перевірок постачальників; механізми підтримки та/або впровадження перевірок постачальників].	

SR-6(1)	ОЦІНКА ПОСТАЧАЛЬНИКІВ - ТЕСТУВАННЯ ТА АНАЛІЗ	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SR-06(01)_ODP[01]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {організаційний аналіз; незалежний сторонній аналіз; організаційне тестування; незалежне стороннє тестування};**
	SR-06(01)_ODP[02]	**визначені елементи ланцюга поставок, процеси та учасники, які підлягають аналізу та тестуванню;**
	SR-06(01)	використовується **<SR-06(01) _ODP[01] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** на **<SR-06(01) _ODP[02] елементах ланцюга постачання, процесах та суб'єктах>**, пов'язаних із системою, системним компонентом або системною послугою.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ:	

	Дослідження: [ВИБІР: Політика та процедури управління ризиками ланцюга постачання; план управління ризиками ланцюга постачання; політика придбання систем та послуг; процедури захисту ланцюга постачання; докази проведення організаційного аналізу, незалежного стороннього аналізу, організаційного тестування на проникнення та/або незалежного стороннього тестування на проникнення; перелік елементів ланцюга постачання, процесів та суб'єктів (пов'язаних із системою, компонентом системи або системною послугою), що підлягають аналізу та/або тестуванню; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за придбання систем та послуг; персонал організації, відповідальний за інформаційну безпеку; персонал організації, відповідальний за управління ризиками ланцюга поставок; персонал організації, відповідальний за аналіз та/або тестування елементів, процесів та учасників ланцюга поставок]. **Перевірка:** [ВИБІР: Процеси організації для визначення та застосування методів аналізу/тестування елементів, процесів та учасників ланцюга поставок; механізми підтримки та/або впровадження аналізу/тестування елементів, процесів та учасників ланцюга поставок].

SR-7	**БЕЗПЕКА ОПЕРАЦІЙ ЛАНЦЮГА ПОСТАЧАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SR-07_ODP	**визначені заходи захисту операційної безпеки (OPSEC) для захисту інформації, пов'язаної з ланцюжком поставок, для системи, системного компонента або системної служби;**
	SR-07	застосовуються **<SR-07_ODP засоби управління OPSEC>** для захисту інформації, пов'язаної з ланцюжком постачання для системи, системного компонента або системної служби.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика та процедури управління ризиками ланцюга постачання; план управління ризиками ланцюга постачання; політика придбання систем та послуг; процедури захисту ланцюга постачання; докази проведення організаційного аналізу, незалежного стороннього аналізу, організаційного тестування на проникнення та/або незалежного стороннього тестування на проникнення; перелік елементів ланцюга постачання, процесів та суб'єктів (пов'язаних із системою, компонентом системи або системною послугою), що підлягають аналізу та/або тестуванню; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за придбання систем та послуг; персонал організації, відповідальний за інформаційну безпеку; персонал організації, відповідальний за управління ризиками ланцюга поставок; персонал організації, відповідальний за аналіз та/або тестування елементів, процесів та учасників ланцюга поставок]. **Перевірка:** [ВИБІР: Процеси організації для визначення та застосування методів аналізу/тестування елементів, процесів та учасників ланцюга поставок;	

	механізми підтримки та/або впровадження аналізу/тестування елементів, процесів та учасників ланцюга поставок].

SR-8	**ПОВІДОМЛЕННЯ ПРО ПОРУШЕННЯ ЛАНЦЮГА ПОСТАЧАННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SR-08_ODP[01]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРІВ: {повідомлення про порушення ланцюга постачання; <SR-08_ODP[02] результати оцінок або аудитів>};**
	SR-08_ODP[02]	**визначена інформація, для якої необхідно встановити угоди та процедури (якщо вибрано);**
	SR-08	встановлені угоди та процедури з суб'єктами, залученими до ланцюга постачання системи, компонентів системи або системної послуги для **<SR-08_ODP[01] ВИБІРКОВЕ ЗНАЧЕННЯ(Я) ПАРАМЕТРА(ів)>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика та процедури управління ризиками ланцюга постачання; план управління ризиками ланцюга постачання; політика придбання систем та послуг; процедури захисту ланцюга постачання; докази проведення організаційного аналізу, незалежного стороннього аналізу, організаційного тестування на проникнення та/або незалежного стороннього тестування на проникнення; перелік елементів ланцюга постачання, процесів та суб'єктів (пов'язаних із системою, компонентом системи або системною послугою), що підлягають аналізу та/або тестуванню; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за придбання систем та послуг; персонал організації, відповідальний за інформаційну безпеку; персонал організації, відповідальний за управління ризиками ланцюга постачання].	

SR-9	**ЗАХИСТ ВІД ЗЛОМУ ТА ВИЯВЛЕННЯ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SR-09	**реалізована програма захисту від несанкціонованого доступу для системи, компонента системи або системної служби.**
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика та процедури управління ризиками ланцюга постачання; план управління ризиками ланцюга постачання; політика придбання систем та послуг; процедури захисту ланцюга постачання; докази проведення організаційного аналізу, незалежного стороннього аналізу, організаційного	

	тестування на проникнення та/або незалежного стороннього тестування на проникнення; перелік елементів ланцюга постачання, процесів та суб'єктів (пов'язаних із системою, компонентом системи або системною послугою), що підлягають аналізу та/або тестуванню; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за програму захисту від несанкціонованого доступу; персонал організації, відповідальний за інформаційну безпеку; персонал організації, відповідальний за управління ризиками ланцюга постачання]. **Перевірка:** Процеси організації реалізації програми захисту від несанкціонованого доступу; механізми підтримки та/або реалізації програми захисту від несанкціонованого доступу].

SR-9(1)	**ЗАХИСТ ВІД ЗЛОМУ ТА ВИЯВЛЕННЯ - ЕТАПИ ЧИ СИСТЕМИ РОЗВИТКУ ЖИТТЄВОГО ЦИКЛУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SR-09(01)	застосовуються технології, інструменти та методи захисту від втручання протягом усього життєвого циклу розробки системи.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика та процедури управління ризиками ланцюга постачання; план управління ризиками ланцюга постачання; політика придбання систем та послуг; процедури захисту ланцюга постачання; докази проведення організаційного аналізу, незалежного стороннього аналізу, організаційного тестування на проникнення та/або незалежного стороннього тестування на проникнення; перелік елементів ланцюга постачання, процесів та суб'єктів (пов'язаних із системою, компонентом системи або системною послугою), що підлягають аналізу та/або тестуванню; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за програму захисту від несанкціонованого доступу; персонал організації, відповідальний за інформаційну безпеку; персонал організації, відповідальний за управління ризиками ланцюга постачання]. **Перевірка:** Процеси організації реалізації програми захисту від несанкціонованого доступу; механізми підтримки та/або реалізації програми захисту від несанкціонованого доступу].	

SR-10	**ПЕРЕВІРКА СИСТЕМИ І КОМПОНЕНТІВ СИСТЕМИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SR-10_ODP[01]	**визначені системи або компоненти системи, які**

		потребують перевірки;
	SR-10_ODP[02]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРА: {випадково; з частотою <SR-10_ODP[03]; за наявності <SR-10_ODP[04] вказівок на необхідність перевірки>};**
	SR-10_ODP[03]	**визначена періодичність проведення перевірок систем або компонентів системи (якщо вибрано);**
	SR-10_ODP[04]	**визначені ознаки необхідності перевірки систем або компонентів системи (якщо вони були обрані);**
	SR-10	перевіряються **<SR-10_ODP[01] системи або компоненти системи> <SR-10_ODP[02] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(ів)>** для виявлення несанкціонованого втручання.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика та процедури управління ризиками ланцюга постачання; план управління ризиками ланцюга постачання; політика придбання систем та послуг; процедури захисту ланцюга постачання; докази проведення організаційного аналізу, незалежного стороннього аналізу, організаційного тестування на проникнення та/або незалежного стороннього тестування на проникнення; перелік елементів ланцюга постачання, процесів та суб'єктів (пов'язаних із системою, компонентом системи або системною послугою), що підлягають аналізу та/або тестуванню; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за програму захисту від несанкціонованого доступу; персонал організації, відповідальний за інформаційну безпеку; персонал організації, відповідальний за управління ризиками ланцюга постачання]. **Перевірка:** Процеси організації реалізації програми захисту від несанкціонованого доступу; механізми підтримки та/або реалізації програми захисту від несанкціонованого доступу].	

SR-11	**АВТЕНТИЧНІСТЬ КОМПОНЕНТУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SR-11_ODP[01]	**вибрано одне або декілька з наступних ЗНАЧЕНЬ ПАРАМЕТРА: {джерело підробленого компонента; <SR-11_ODP[02] зовнішні підзвітні організації>; <SR-11_ODP[03] персонал або ролі>};**
	SR-11_ODP[02]	**визначені зовнішні підзвітні організації, яким слід повідомляти про підроблені компоненти системи (якщо вони були обрані);**
	SR-11_ODP[03]	**визначено персонал або ролі, яким слід повідомляти про підроблені компоненти системи (якщо визначено);**

	SR-11a.[01]	розроблено та впроваджено політику боротьби з підробками;
	SR-11a.[02]	розроблені та впроваджені процедури боротьби з підробками;
	SR-11a.[03]	включають процедури боротьби з підробками засоби для виявлення підроблених компонентів, що потрапляють до системи;
	SR-11a.[04]	включають процедури боротьби з підробками засоби запобігання потраплянню в систему підроблених компонентів;
	SR-11b.	повідомляється про підроблені компоненти системи в **<SR-11_ODP[01] ВИБІРКОВЕ ЗНАЧЕННЯ ПАРАМЕТРА(S)>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика та процедури управління ризиками ланцюга постачання; план управління ризиками ланцюга постачання; політика придбання систем та послуг; процедури захисту ланцюга постачання; докази проведення організаційного аналізу, незалежного стороннього аналізу, організаційного тестування на проникнення та/або незалежного стороннього тестування на проникнення; перелік елементів ланцюга постачання, процесів та суб'єктів (пов'язаних із системою, компонентом системи або системною послугою), що підлягають аналізу та/або тестуванню; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за програму захисту від несанкціонованого доступу; персонал організації, відповідальний за інформаційну безпеку; персонал організації, відповідальний за управління ризиками ланцюга постачання]. **Перевірка:** Процеси організації реалізації програми захисту від несанкціонованого доступу; механізми підтримки та/або реалізації програми захисту від несанкціонованого доступу].	

SR-11(1)	**АВТЕНТИЧНІСТЬ КОМПОНЕНТУ - ТРЕНУВАННЯ ПО БОРОТЬБІ З ПІДРОБКАМИ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SR-11(01)_ODP	**визначено персонал або ролі, які потребують підготовки для виявлення підроблених компонентів системи (включаючи апаратне, програмне та мікропрограмне забезпечення);**
	SR-11(01)	підготовлений **<SR-11(01)_ODP персонал або ролі>** до виявлення підроблених компонентів системи, включаючи апаратне, програмне та мікропрограмне забезпечення.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика та процедури управління ризиками ланцюга постачання; план управління ризиками ланцюга постачання; політика придбання	

	систем та послуг; процедури захисту ланцюга постачання; докази проведення організаційного аналізу, незалежного стороннього аналізу, організаційного тестування на проникнення та/або незалежного стороннього тестування на проникнення; перелік елементів ланцюга постачання, процесів та суб'єктів (пов'язаних із системою, компонентом системи або системною послугою), що підлягають аналізу та/або тестуванню; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Персонал організації, відповідальний за програму захисту від несанкціонованого доступу; персонал організації, відповідальний за інформаційну безпеку; персонал організації, відповідальний за управління ризиками ланцюга постачання]. **Перевірка:** Процеси організації реалізації програми захисту від несанкціонованого доступу; механізми підтримки та/або реалізації програми захисту від несанкціонованого доступу]. **Перевірка:** Процеси організації для навчання по боротьбі з підробками [Електронний ресурс].

SR-11(2)	**АВТЕНТИЧНІСТЬ КОМПОНЕНТУ - КОНТРОЛЬ КОНФІГУРАЦІЇ КОМПОНЕНТІВ, ЯКІ ПОТРЕБУЮТЬ СЕРВІСНОГО ОБСЛУГОВУВАННЯ І РЕМОНТУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SR-11(02)_ODP	**визначені компоненти системи, які потребують контролю конфігурації;**
	SR-11(02)[01]	підтримується контроль конфігурації над **<SR-11(02)_ODP системних компонентів>**, які очікують на обслуговування або ремонт;
	SR-11(02)[02]	підтримується контроль конфігурації над обслуговуваними або відремонтованими **<SR-11(02)_ODP системними компонентами>**, які очікують на повернення в експлуатацію.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика та процедури управління ризиками ланцюга постачання; план управління ризиками ланцюга постачання; політика придбання систем та послуг; процедури захисту ланцюга постачання; докази проведення організаційного аналізу, незалежного стороннього аналізу, організаційного тестування на проникнення та/або незалежного стороннього тестування на проникнення; перелік елементів ланцюга постачання, процесів та суб'єктів (пов'язаних із системою, компонентом системи або системною послугою), що підлягають аналізу та/або тестуванню; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Процеси організації реалізації програми захисту від несанкціонованого доступу; механізми підтримки та/або реалізації програми захисту від несанкціонованого доступу]. **Перевірка:** Процеси організації встановлення міжорганізаційних угод та	

	процедур з суб'єктами ланцюга поставок; процеси контролю організаційної конфігурації].

SR-11(3)	**АВТЕНТИЧНІСТЬ КОМПОНЕНТУ - СКАНУВАННЯ ДЛЯ ВИЯВЛЕННЯ ПІДРОБОК**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SR-11(03)	проводиться сканування на наявність підроблених компонентів системи **<SR-11(03)_ODP частота>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика та процедури управління ризиками ланцюга постачання; план управління ризиками ланцюга постачання; політика придбання систем та послуг; процедури захисту ланцюга постачання; докази проведення організаційного аналізу, незалежного стороннього аналізу, організаційного тестування на проникнення та/або незалежного стороннього тестування на проникнення; перелік елементів ланцюга постачання, процесів та суб'єктів (пов'язаних із системою, компонентом системи або системною послугою), що підлягають аналізу та/або тестуванню; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Процеси організації реалізації програми захисту від несанкціонованого доступу; механізми підтримки та/або реалізації програми захисту від несанкціонованого доступу]. **Перевірка:** Процеси організації встановлення міжорганізаційних угод та процедур з суб'єктами ланцюга поставок; процеси контролю організаційної конфігурації].	

SR-12	**УТИЛІЗАЦІЯ КОМПОНЕНТУ**	
	МЕТА ОЦІНКИ: Визначити, чи:	
	SR-12_ODP[01]	**визначені дані, документація, інструменти або компоненти системи, які підлягають утилізації;**
	SR-12_ODP[02]	**визначені методи та способи утилізації даних, документації, інструментів або компонентів системи;**
	SR-12	утилізуються **<SR-12_ODP[01] дані, документація, інструменти або компоненти системи>** з використанням **<SR-12_ODP[02] прийомів і методів>**.
	ПОТЕНЦІЙНІ МЕТОДИ ТА ОБ'ЄКТИ ОЦІНКИ: **Дослідження**: [ВИБІР: Політика та процедури управління ризиками ланцюга постачання; план управління ризиками ланцюга постачання; політика придбання систем та послуг; процедури захисту ланцюга постачання; докази проведення організаційного аналізу, незалежного стороннього аналізу, організаційного	

	тестування на проникнення та/або незалежного стороннього тестування на проникнення; перелік елементів ланцюга постачання, процесів та суб'єктів (пов'язаних із системою, компонентом системи або системною послугою), що підлягають аналізу та/або тестуванню; план захисту інформації системи; інші відповідні документи або записи]. **Співбесіда:** [ВИБІР: Процеси організації реалізації програми захисту від несанкціонованого доступу; механізми підтримки та/або реалізації програми захисту від несанкціонованого доступу]. **Перевірка:** Процеси організації встановлення міжорганізаційних угод та процедур з суб'єктами ланцюга поставок; процеси контролю організаційної конфігурації].