ЗАТВЕРДЖЕНО

Наказ Адміністрації
Державної служби
спеціального зв’язку та
захисту інформації України
__ _____ 2023 року № ___

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ
щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами

І. Загальні положення

1. Методичні рекомендації щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами (далі – Рекомендації) розроблено відповідно до підпункту 1 частини другої та пункту 3 частини третьої статті 8 Закону України «Про основні засади забезпечення кібербезпеки України», абзаців другого та п’ятого частини першої статті 3, пунктів 85, 86 та 88 частини першої статті 14 Закону України «Про Державну службу спеціального зв’язку та захисту інформації України», пунктів 45 Плану реалізації Стратегії кібербезпеки України, схваленого рішенням Ради національної безпеки і оборони України від 30 грудня 2021 року «Про План реалізації Стратегії кібербезпеки України», введеним в дію Указом Президента України від 01 лютого 2022 року № 37, пункту 12 Загальних вимог до кіберзахисту об’єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 року № 518, та абзацу другого підпункту 1 пункту 3 Положення про Адміністрацію Державної служби спеціального зв’язку та захисту інформації України, затвердженого постановою Кабінету Міністрів України від 03 вересня 2014 року № 411.

2. Рекомендації не є нормативно-правовим актом, мають інформаційний та рекомендаційний характер, не встановлюють правових норм і є добровільними для використання.

ІІ. Терміни та визначення понять

У цих Рекомендаціях терміни вживаються в такому значенні:

вимога безпеки — твердження, яке виражає конкретну потребу в безпеці

інформації (активу), включно із супутніми обмеженнями та умовами. Вимога безпеки, що висувається до інформації, інформаційної (автоматизованої) системи чи організації, може походити з різних джерел, серед яких, наприклад, закони, нормативно-правові акти Кабінету Міністрів України, нормативні документи, міжнародні, національні та галузеві стандарти, накази, директиви, правила (політики), положення, а також потреби конкретної організації;

відкрита інформація — інформація, яка може міститися на загальнодоступних ресурсах і до якої висуваються вимоги збереження цілісності та доступності;

вразливість — недолік, яким можна скористатися, уможливлюючи неавторизований доступ до систем або дозволяючи користувачам мати доступ до більших привілеїв ніж авторизовані;

електронна комунікаційна система — сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання та/або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб;

життєвий цикл інформації — етапи, через які проходить інформація, наприклад: створення або збір, обробка, поширення, використання, зберігання і розпорядження, включно зі знищенням і видаленням;

заходи захисту інформації (заходи безпеки) — заходи або контрзаходи, передбачені для впровадження в ІС або організації з метою захисту конфіденційності, цілісності та доступності інформації, що циркулює в ІС;

інформаційна (автоматизована) система - організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів;

інформаційно-комунікаційна система – сукупність інформаційних та електронних комунікаційних систем, які у процесі обробки інформації діють як єдине ціле;

інцидент — подія, яка теоретично або фактично загрожує конфіденційності та/або цілісності та/або доступності інформації або інформаційної (автоматизованої) системи, або являє собою порушення чи неминучу загрозу порушення закону, політики безпеки, процедур безпеки або прийнятних правил використання;

компонент системи — дискретний ідентифікований актив інформаційних технологій, який являє собою функціональний блок системи й може містити апаратне та/або програмне забезпечення;

критична інформація (критичні дані) — інформація з обмеженим доступом, яка не містить ознак державної таємниці, порушення конфіденційності та/або цілісності та/або доступності якої може мати негативні наслідки (негативний вплив) для власника інформації та/або ІС, у якій циркулює така інформація;

ланцюг довіри, ланцюг постачання — певний рівень довіри під час взаємодії в ланцюгу постачання, коли кожен учасник відносин «споживач-

постачальник» забезпечує належний захист своїх компонентів продуктів, систем і послуг;

наглядовий контроль та збір даних (Supervisory Control and Data Acquisition, SCADA) – загальна назва для комп'ютеризованої системи, яка здатна збирати й обробляти дані та застосовувати оперативний контроль на великих відстанях; типові види використання включають системи передачі та розподілу електроенергії та трубопроводи;

операційні технології — технології автоматизації технологічних процесів, промислових виробництв і підприємств на основі сучасних цифрових технологій та електронних комунікацій;

організація – орган державної влади, підприємство, установа, організація будь-якої форми власності, юридична та/або фізична особа, якому/якій на правах власності, оренди або на інших законних підставах належить ОТ/АСУ ТП або який/яка відповідає за його поточне функціонування;

патчі — додаткові фрагменти коду, розроблені для вирішення певних проблем або недоліків у існуючому програмному забезпеченні;

план заходів захисту інформації — документ або сукупність документів системного рівня, які детально описують заходи захисту, вибрані для інформаційної (автоматизованої) системи з метою задоволення відповідних вимог безпеки й управління ризиками, детально описують залучені способи/ролі управління, методології та показники, які використовуватимуться для оцінювання заходів захисту інформації;

політика безпеки інформації — документ або сукупність документів системного рівня, які містять набір вимог, правил, обмежень, рекомендацій, що регламентують порядок інформаційної діяльності в ІС і спрямовані на досягнення і підтримку стану інформаційної безпеки системи та організації в цілому;

постачальник електронних комунікаційних послуг – суб'єкт господарювання, який фактично надає та/або має право надавати електронні комунікаційні послуги на власних мережах та/або на мережах інших постачальників електронних комунікаційних послуг.

приватність – безпека персональних даних;

профіль безпеки (ПБ) — набір заходів захисту, які застосовуються до інформації або ІС для задоволення вимог чинної нормативної бази, а також спрямовані на захист потреб з метою управління ризиками безпеки;

роль — визначена сукупність правил, які встановлюють рамки взаємодії між користувачем та інформаційною системою;

таємна інформація — інформація, що охоплює відомості у сфері оборони, економіки, науки й техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України;

управління доступом на основі ролей — набір дозволів доступу, який цифрова ідентичність отримує на основі явного або неявного припущення про певну роль;

mesh-мережі (сітчаста мережа) — топологія комп'ютерної мережі, в якій кожен вузол (називається вузлом меш) передає дані мережею і виступає в ролі комутатора. Всі вузли співпрацюють у розподілі даних в мережі, тобто кожен вузол бере участь у передачі даних.

Інші терміни в цих Рекомендаціях вживаються у значенні, наведеному в нормативно-правових актах та нормативних документах України.

III. Скорочення

У цих Рекомендаціях наведено такі скорочення:

АС – автоматизована система;

ОТ/АСУ ТП – автоматизована система управління технологічними процесами;

ДБЖ – джерело безперебійного живлення;

ЕОТ –електронна обчислювальна техніка;

ЗОТ – засіб обчислювальної техніки;

ІС – інформаційна (автоматизована) система;

КБ – категорія безпеки;

КС – комп'ютерна система;

НД – нормативний документ;

НСД – несанкціонований доступ;

ОКІ – об’єкт критичної інфраструктури;

ОС – обчислювальна система;

ОТ – операційні технології;

ПАВ – план аварійного відновлення;

ПББ – план безперервності бізнесу;

ПД – персональні дані;

ПЗ – програмне забезпечення;

ПЛК — Програмований логічний контролер;

СУІБ – система управління інформаційною безпекою;

ТЗІ – технічний захист інформації;

ЦП – центральний процесор;

ЦТВ – цільова точка відновлення;

ЦЧВ – цільовий час відновлення;

CSF (Cybersecurity Framework) Supply Chain Risk Management — управління ризиками ланцюга постачання кібербезпеки;

CSMS (Cyber Security Management System) — система управління кібербезпекою;

FAT (Factory Acceptance Tests) — заводські приймальні випробування;

FIPP (Fair Information Practice Principles) — принципи чесної інформаційної практики;

FIPS (Federal Information Processing Standards) — федеральні (США) стандарти обробки інформації.

FMEA (Failure Mode and Effects Analysis) — аналіз режиму відмови та наслідків;

HMI (Human Machine Interface) — людино-машинний інтерфейс;

HSE (Health, Safety and Environmental) — управління HSE (охорона здоров'я, безпека та навколишнє середовище);

HVAC (Heating, Ventilation, & AirConditioning) – опалення, вентиляція та кондиціонування;

ID — ідентифікатор;

IDS (Intrusion Detection System) – система виявлення вторгнень;

IP (Internet Protocol) — міжмережевий протокол;

NVD (National Vulnerability Database) — національна база даних вразливостей;

PHA (Preliminary Hazard Analysis) – аналіз технологічних небезпек;

PIV (Personal Identity Verification) – підтвердження ідентифікації особи;

PLC (Programmable Logic Controller) – програмований логічний контролер;

RBAC (Role-Based Access Control) – контроль доступу на основі ролей;

SAT (Site Acceptance Tests) — приймальні випробування на місці;

SBOM (Software Bill Of Materials) — перелік матеріалів для програмного забезпечення;

TCP/IP (Transmission Control Protocol/ Internet Protocol) — протокол керування передаванням/міжмережевий протокол;

VPN (Virtual Private Network) – віртуальна приватна мережа.

IV. Вимоги до кіберзахисту автоматизованих систем управління технологічними процесами

1. Функціональні профілі захищеності ОТ/АСУ ТП

1.1. Класифікація заходів кіберзахисту

У цих Рекомендаціях функціональні профілі захищеності наведено згідно з класифікацією (таксономією) заходів кіберзахисту та Методичними рекомендаціями щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури, затвердженими наказом Адміністрації Держспецзв'язку від 06 жовтня 2021 року № 601.

1.2. Клас заходів «Ідентифікація ризиків» (ID)

Таблиця 1 – Заходи кіберзахисту категорії ID.AM

Заходи кіберзахисту	
Захід кіберзахисту	Опис
1	2
ID.AM-1. Фізичне обладнання та системи на ОТ/АСУ ТП ідентифіковано та задокументовано.	Організації рекомендовано провести інвентаризацію всіх кіберфізичних пристроїв та носіїв інформації, що використовуються в ОТ/АСУ ТП, включаючи перелік систем, до яких вони належать, їхні функцій, способи ідентифікації пристроїв та іншу інформацію, яку організація вважає необхідною для опису характеру ризику.
ID.AM-2. Програмне забезпечення, що використовується ОТ/АСУ ТП для надання життєво важливих послуг та функцій, ідентифіковано та задокументовано.	Організації рекомендовано провести інвентаризацію програмного забезпечення ОТ/АСУ ТП, включаючи вбудоване програмне забезпечення окремих пристроїв, перелік систем, до яких вони належать, їхні функцій, номери версій, іншу інформацію, яку організація вважає необхідною для ідентифікування програмного забезпечення та опису характеру ризику.
ID.AM-3. Електронні комунікації та потоки даних ОТ/АСУ ТП ідентифіковано та задокументовано.	Організації рекомендовано визначити дані, якими ОТ/АСУ ТП обмінюється з іншими системами, наявні правила та процедури інформаційного обміну, технічні засоби, інтерфейси та протоколи електронних комунікацій, іншу інформацію, що сприятиме визначенню характеру ризику.
ID.AM-4. Зовнішні інформаційні та інформаційно-комунікаційні системи, промислові системи, які взаємодіють з інформаційно-комунікаційними та іншими системами ОТ/АСУ ТП обліковано.	До ресурсів системи захисту поза службовими приміщеннями має бути застосований захист з урахуванням різних ризиків роботи поза службовими приміщеннями організації.

1	2
ID.AM-5. Критичність активів (обладнання, устаткування, даних, програмного забезпечення) ОТ/АСУ ТП визначено відповідно до оцінки їх впливу на надання життєво важливих послуг та функцій ОТ/АСУ ТП.	Організації рекомендовано розробити критерії та призначити клас пріоритету для зниження ризику кожної логічної групи управління.
ID.AM-6. Обов'язки штатного персоналу ОТ/АСУ ТП та персоналу партнерів організації (наприклад – постачальників, клієнтів тощо) щодо забезпечення кібербезпеки визначено та закріплено у відповідних документах.	Необхідно чітко визначити види відповідальності всередині організації для виконання завдань забезпечення інформаційної безпеки та вжиття відповідних заходів з фізичної безпеки.

Таблиця 2 – Заходи кіберзахисту категорії ID.BE

Захід кіберзахисту	Опис
1	2
ID.BE-1. Роль ОТ/АСУ ТП у ланцюгу постачання товарів і послуг визначено та повідомлено всім постачальникам організації.	Угоди з постачальниками мають містити вимоги стосовно адресації ризиків інформаційної безпеки, пов’язаних з ланцюгом постачання продуктів і послуг інформаційно-комунікаційних технологій та електронних комунікацій. Організації рекомендовано регулярно проводити моніторинг, перегляд та аудит отримання послуг постачальника продуктів та послуг інформаційно-комунікаційних технологій та електронних комунікацій. Зміни в наданні послуг постачальника продуктів та послуг інформаційно-комунікаційних технологій та електронних комунікацій, зокрема й підтримування та вдосконалювання наявних політик інформаційної безпеки, процедур і заходів безпеки, мають вноситися з урахуванням критичності залучених бізнес-систем і процесів та переоцінки ризиків.

1	2
ID.BE-2. Місце та роль ОТ/АСУ ТП в системі надання життєво важливих послуг та функцій сектору (підсектору) критичної інфраструктури визначено і повідомлено всім постачальникам організації.	Організації рекомендовано вирішувати питання інформаційної безпеки при розробці документації та оновленні плану захисту критичної інфраструктури та ключових ресурсів.
ID.BE-3. Пріоритетність цілей, завдань і заходів щодо забезпечення кібербезпеки надання життєво важливих послуг та функцій встановлено та повідомлено.	Організації рекомендовано розробити розширене економічне обґрунтування як основу для своєї роботи з управління кібербезпекою ОТ/АСУ ТП, в якому розглядається специфіка залежності організації від ОТ/АСУ ТП.
ID.BE-4. Залежності та найважливіші процеси для забезпечення надання життєво важливих послуг та функцій встановлено.	Організації рекомендовано бути захищеній від аварійних відімкнень живлення та інших порушень, внаслідок аварій засобів життєзабезпечення. Електронна комунікаційна мережа передачі даних або підтримки інформаційних послуг рекомендовано бути захищеними від перехоплювання, взаємного впливу чи пошкоджень. Для забезпечення потрібної продуктивності системи необхідно проводити моніторинг та регулювати використання ресурсів і проєктувати вимоги до майбутньої потужності.
ID.BE-5. Вимоги до стійкості ОТ/АСУ ТП щодо забезпечення надання життєво важливих послуг та функцій встановлено.	Необхідно розробити й застосовувати фізичний захист від пошкодження внаслідок природних катаклізмів, акцій громадської непокори та аварій. Організації рекомендовано визначити свої вимоги щодо інформаційної безпеки та безперервності управління інформаційною безпекою в надзвичайних ситуаціях, наприклад, під час кризи чи катастрофи. Організації рекомендовано розробити, задокументувати,

1	2
	реалізувати та підтримувати процеси, процедури та заходи безпеки для гарантування необхідного рівня безперервності щодо інформаційної безпеки під час надзвичайної ситуації. Обладнання оброблення інформації слід впровадити з резервуванням, достатнім для того, щоб відповідати вимогам доступності.

Таблиця 3 – Заходи кіберзахисту категорії ID.GV

Захід кіберзахисту	Опис
1	2
ID.GV-1. Правила (політики) кібербезпеки ОТ/АСУ ТП встановлено та задокументовано.	Політика системи управління інформаційною безпекою (СУІБ): отримання дозволу керівництва на впровадження СУІБ; визначення методу вимірювання ефективності обраних засобів контролю; загальні вимоги до документації. Контроль документації; перевірка СУІБ керівництвом.
ID.GV-2. Обов'язки щодо забезпечення кібербезпеки ОТ/АСУ ТП скоординовано та узгоджено з обов’язками персоналу ОТ/АСУ ТП та із зовнішніми партнерами.	Слід чітко визначити види відповідальності всередині організації для виконання завдань забезпечення інформаційної безпеки та вжиття відповідних заходів з фізичної безпеки.
ID.GV-3. Правові та нормативні вимоги щодо забезпечення кібербезпеки ОТ/АСУ ТП, у тому числі зобов'язання щодо захисту недоторканості особистого життя (приватності), усвідомлено та управління ними здійснюється.	Організації рекомендовано ознайомитися з чинним законодавством та змінами у законодавстві, що стосуються кібербезпеки.

1	2
ID.GV-4. Процеси управління безпекою та управління ризиками спрямовано на вирішення питання оброблення ризиків кібербезпеки.	Організації рекомендовано визначити підходи та методи аналізування ризиків, які визначають та розставляють у порядку пріоритету ризики, пов'язані із загрозами безпеці, вразливостями та наслідками матеріальних об'єктів ОТ/АСУ ТП. Розширене аналізування ризиків рекомендовано проводити з метою розуміння наслідків для фінансової сфери і сфери здоров’я та навколишнього середовища (HSE - Health, safety and environmental) у разі появи загрози доступності, цілісності або конфіденційності ОТ/АСУ ТП. Методика оцінювання ризиків, обрана організацією, має передбачати методи визначення пріоритетів вразливостей, виявлених під час детального аналізу. Організації рекомендовано провести детальне аналізування ризиків, включаючи вразливості, виявлені під час детального аналізу. Результати оцінювання фізичних ризиків, ризиків HSE та ризиків, пов'язаних із кібербезпекою, слід об'єднати для розуміння загального ризику для матеріальних об'єктів. Персоналу, що відповідає за управління ризиками, розробку ОТ/АСУ ТП, системне адміністрування/обслуговування та інші завдання, що впливають на систему управління кібербезпекою (CSMS - Cyber security management system), слід пройти навчання з досягнення цілей безпеки та промислових операцій, пов'язаних з такими завданнями.

1	2
	Політики та процедури кібербезпеки, спрямовані на управління ризиками для ОТ/АСУ ТП, мають відповідати або бути продовженням політик, створених в рамках інших систем управління ризиками.

Таблиця 4 – Заходи кіберзахисту категорії ID.RA

Захід кіберзахисту	Опис
1	2
ID.RA-1. Вразливості активів ОТ/АСУ ТП проаналізовано, ідентифіковано та задокументовано.	Організації рекомендовано виконати детальний аналіз вразливостей своїх окремих логічних ОТ/АСУ ТП, сфера охоплення якого залежить від результатів розширеного аналізу ризиків та пріоритету предмета ОТ/АСУ ТП відносно таких ризиків. Організації рекомендовано провести детальний аналіз ризиків, включаючи вразливості, виявлені під час детального аналізу. Оцінювання ризиків слід проводити на всіх етапах життєвого циклу технології, включаючи розробку, впровадження, зміни та виведення з експлуатації.
ID.RA-2. Інформацію про загрози безпеки та вразливості отримано з форумів обміну інформацією та офіційних джерел.	Організації рекомендовано провести детальний аналіз ризиків, включаючи вразливості, виявлені під час детального аналізу. Оцінювання ризиків слід проводити на всіх етапах життєвого циклу технології, включаючи розробку, впровадження, зміни та виведення з експлуатації.
ID.RA-3. Загрози кібербезпеки (модель загроз) як внутрішні, так і зовнішні визначено й задокументовано.	Організації рекомендовано провести детальний аналіз ризиків, включаючи вразливості, виявлені під час детального аналізу. Оцінювання ризиків слід проводити на всіх етапах життєвого циклу технології, включаючи розробку, впровадження, зміни та виведення з експлуатації.

1	2
ID.RA-4. Потенційні наслідки (рівень шкоди), які можуть завдати загрози в наслідок їх реалізації на безперервне надання життєво важливих послуг та функцій та ймовірності їх реалізації визначено.	Організації рекомендовано провести детальний аналіз ризиків, включаючи вразливості, виявлені під час детального аналізу. Оцінювання ризиків слід проводити на всіх етапах життєвого циклу технології, включаючи розробку, впровадження, зміни та виведення з експлуатації.
ID.RA-5. Для визначення ризику застосовуються дані щодо загроз, вразливостей, їх ймовірностей та рівня шкоди використання для визначення ризику кібербезпеки.	Слід отримувати своєчасну інформацію щодо технічних вразливостей інформаційних (автоматизованих) систем, які використовуються, оцінювати загрози, організації таким вразливостям і вживати належних заходів, щоб урахувати пов’язаний з цим ризик.
ID.RA-6. Заходи реагування на ризик кібербезпеки визначено та їх пріоритетність встановлено.	Організація впроваджує процес для забезпечення того, щоб плани дій та етапи для програми безпеки та пов’язаних організаційних інформаційних (автоматизованих) систем: розроблялися та підтримувалися; задокументовувалися заходи з інформаційної безпеки, щоб адекватно реагувати на ризики для організаційних операцій та активів, окремих осіб, інших організацій та країни; переглядалися плани дій та етапи на відповідність стратегії управління ризиками організації та пріоритетам дій щодо реагування на ризики в масштабі всієї організації. Організація розробляє комплексну стратегію управління ризиками для організаційних операцій та активів, окремих осіб, інших організацій та країн, пов'язаних з експлуатацією та використанням інформаційних (автоматизованих) систем. Організація послідовно реалізує стратегію управління ризиками та переглядає й оновлює стратегію управління ризиками або у разі потреби для вирішення організаційних змін.

Таблиця 5 – Заходи кіберзахисту категорії ID.RM

Захід кіберзахисту	Опис
1	2
ID.RM-1. Процеси управління ризиками визначено, узгоджено із партнерами організації та управляються.	Виявнення ризиків. Аналізування та оцінювання ризиків. Виявлення та оцінювання варіантів зменшення ризиків. Вибір цілей і засобів контролю для зменшення ризику. Отримання дозволу керівництва на передбачувані залишкові ризики. Складання положення щодо застосовності. Реалізація плану зменшення ризиків. Упровадження засобів контролю. Визначення методу вимірювання ефективності обраних засобів контролю. Процедури впровадження і засоби контролю для визначення і реагування на події в сфері безпеки. Надання ресурсів.
ID.RM-2. Допустимий рівень ризику кібербезпеки визначено та чітко виражено.	Організації рекомендовано визначити та документально оформити своє розуміння допустимості ризиків як основи для розробки політики безпеки інформації та проведення роботи з управління ризиками.
ID.RM-3. Визначення допустимого рівня ризику ґрунтується на ролі ОТ/АСУ ТП як складової частини сектору критичної інфраструктури та аналізі ризиків, притаманних відповідному сектору критичної інфраструктури.	Організація вирішує питання інформаційної безпеки при розробці, документації та оновленні плану захисту критичної інфраструктури та ключових ресурсів. Організація розробляє комплексну стратегію управління ризиками для організаційних операцій та активів, окремих осіб, інших організацій та країни, пов'язаних з експлуатацією та використанням інформаційних (автоматизованих) систем;

1	2
	послідовно реалізує стратегію управління ризиками по всій організації; переглядає та оновлює стратегію управління ризиками або у разі потреби для вирішення організаційних змін. Організація визначає місію/бізнес-процеси з урахуванням інформаційної безпеки та ризику для організаційних операцій, організаційних активів, окремих осіб, інших організацій та країни; і визначає потреби в захисті інформації, що випливають із визначеної місії/бізнес-процесів, і переглядає процеси, доки не будуть досягнуті достатні потреби захисту. Організація визначає важливі компоненти та функції інформаційної (автоматизованої) системи, виконуючи аналіз критичності для визначених організацією інформаційних (автоматизованих) систем, компонентів інформаційної (автоматизованої) системи або послуг інформаційної (автоматизованої) системи, у точці прийняття рішення, визначеної організацією в життєвому циклі розробки системи.

Таблиця 6 – Заходи кіберзахисту категорії ID.SC

Захід кіберзахисту	Опис
1	2
ID.SC-1. Процеси управління ризиками кібербезпеки системи постачання визначено, узгоджено з партнерами організації та управляються.	Виявлення ризиків. Аналізування та оцінювання ризиків. Виявлення та оцінювання варіантів зменшення ризиків. Вибір цілей і засобів контролю для зменшення ризику. Отримання дозволу керівництва на передбачувані залишкові ризики. Складання положення щодо застосовності. Реалізація плану зменшення

1	2
	ризиків. Упровадження засобів контролю. Визначення методу вимірювання ефективності обраних засобів контролю. Процедури впровадження і засоби контролю для визначення і реагування на події в сфері безпеки. Надання ресурсів.
ID.SC-2. Постачальники (розпорядники) інформаційних систем, товарів і послуг для ОТ/АСУ ТП ідентифіковано, рівень їх критичності оцінено у відповідності до політики управління ризиками кібербезпеки з урахуванням ризиків, притаманних системі постачання.	Організації рекомендовано визначити підходи та методи аналізування ризиків, які визначають та розставляють у порядку пріоритету ризики, пов'язані із загрозами безпеці, вразливостями та наслідками для матеріальних об'єктів ОТ/АСУ ТП. Організації рекомендовано надати особам, які беруть участь в оцінюванні ризиків, відповідну інформацію, включаючи навчання методиці, до початку оцінювання ризиків. Розширене аналізування ризиків слід проводити для розуміння наслідків для фінансової сфери і сфери здоров’я та навколишнього середовища (HSE - Health, safety and environmental) у разі появи загрози доступності, цілісності або конфіденційності ОТ/АСУ ТП. Організації рекомендовано визначити різні ОТ/АСУ ТП, зібрати дані про пристрої, щоб можна було описати під час детального аналізу. Організації рекомендовано провести детальне аналізування ризиків, включаючи вразливості, виявлені під час детального аналізу. Організації рекомендовано визначити періодичність проведення повторного аналізування ризиків та вразливостей, а також критерії початку аналізування, залежно від змін технології, організації чи промислової експлуатації.

1	2
	Оцінювання ризиків слід проводити на всіх етапах життєвого циклу технології, включаючи розробку, впровадження, зміни та виведення з експлуатації. Для всіх об'єктів, що становлять ОТ/АСУ ТП, слід вести актуальні записи щодо аналізування вразливостей.
ID.SC-3. Постачальники товарів і послуг та партнери відповідно до договору можуть впроваджувати заходи, спрямовані на досягнення мети політики інформаційної безпеки/кібербезпеки ОТ/АСУ ТП та плану управління ризиками постачання.	У політики та процедури кібербезпеки для середовища ОТ/АСУ ТП слід включати вимоги щодо відповідності. Політики та процедури кібербезпеки слід переглядати на постійній основі, слід проводити їх оцінювання, що підтверджує, що вони виконуються та підтримуються в актуальному стані відповідно до вимог, що гарантує їхню відповідність вимогам.
ID.SC-5. З постачальниками здійснюється планування та тестування реагування за відповідними політиками реагування на кіберінциденти та відновлення стану кібербезпеки.	Привілеї доступу, надані обліковими записами, рекомендовано встановлювати відповідно до політики організації щодо авторизації. У політиці безпеки авторизації слід встановити правила, що визначають привілеї доступу, підтверджені для облікових записів для персоналу з різними посадовими функціями. Така політика має бути оформлена документально та застосовуватися щодо всього персоналу після процедури аутентифікації.

1.3. Клас заходів «Захист» (PR)

Таблиця 7 – Заходи кіберзахисту категорії PR.AC

Захід кіберзахисту	Опис
1	2
PR.AC-1. Ідентифікатори та дані автентифікації для авторизованих користувачів, адміністраторів та процесів призначаються, верифікуються, адмініструються, відкликаються (скасовуються) та перевіряються.	Привілеї доступу, надані обліковими записами, слід встановлювати відповідно до політики організації щодо авторизації. У політиці безпеки авторизації слід встановити правила, що визначають привілеї доступу, підтверджені для облікових записів для персоналу з різними посадовими функціями. Таку політику слід оформити документально та застосовувати щодо всього персоналу після процедури аутентифікації.
PR.AC-2. Фізичний доступ до ОТ/АСУ ТПІ захищений та управляється.	Для забезпечення захищеності від неавторизованого доступу та захисту об'єктів слід встановити один або кілька периметрів фізичної безпеки. Слід встановити процедури контролю та оповіщення у випадках виникнення загрози для фізичної безпеки або для захисту від зовнішніх впливів.
PR.AC-3. Здійснюється контроль та управління віддаленого доступу.	Організації рекомендовано розробити політику, яка регулює дистанційний вхід у систему одним користувачем та/або через дистанційне з'єднання (наприклад, міжзадачні з'єднання) із системами управління, в яких визначалися б відповідні повідомлення системи про невдалі спроби входу та закінчення періодів неактивності.

1	2
PR.AC-4. Права доступу встановлено із застосуванням принципів мінімальних привілеїв і розподілу обов'язків.	Облікові записи з доступом слід визначати посадовими функціями для керування доступом до відповідної інформації або систем для такої посадової функції користувача. Під час визначення посадових функцій слід враховувати наслідки для безпеки.
PR.AC-5. Цілісність електронної комунікаційної мережі захищено (наприклад, сегментація мережі).	Робочі процедури та обов’язки. Планування та приймання системи. Управління безпекою електронної комунікаційної мережі. Контроль доступу до мережі.
PR.AC-7. Автентифікація користувачів, адміністраторів, пристроїв та інших активів здійснюється (наприклад, методами однофакторної, багатофакторної автентифікації) відповідно до встановленого ризику порушення безпеки.	Організації рекомендовано розробити стратегії або підходи до аутентифікації, що дозволяє визначати метод(и) аутентифікації для їхнього подальшого застосування. Усі користувачі повинні проходити автентифікацію перед використанням додатка, що запитується, крім випадків, коли передбачені компенсуючі комбінації технологій контролю входу та адміністративних практик. Практики строгої автентифікації (наприклад, з вимогою ввести надійний пароль) рекомендовано застосовувати до всіх облікових записів для системних адміністраторів та конфігурації програм. У журналах реєстрації слід вести запис всіх спроб доступу до найважливіших систем, такі журнали варто перевіряти щодо вдалих і невдалих спроб доступу. Організація може реалізовувати схему аутентифікації з відповідним рівнем суворості для точного визначення дистанційного інтерактивного користувача. Організації рекомендовано розробити політику, яка регулює дистанційний вхід у систему одним

1	2
	користувачем та/або через дистанційне з'єднання (наприклад, міжзадачні з'єднання) із системами управління, в яких визначалися б відповідні повідомлення системи про невдалі спроби входу та закінчення періодів неактивності. Після певної кількості невдалих спроб входу віддаленим користувачем система має деактивувати обліковий запис на певний термін. Після закінчення певного періоду неактивності віддалений користувач повинен пройти повторну автентифікацію для отримання повторного доступу до системи. У системах рекомендовано реалізовувати відповідні схеми аутентифікації для міжзадачних з'єднань між додатками та пристроями.

Таблиця 8 – Заходи кіберзахисту категорії PR.AT

Захід кіберзахисту	Опис
1	2
PR.AT-1. Усі співробітники ОТ/АСУ ТП обізнані та пройшли підготовку з питань кібербезпеки.	Усьому персоналу (включаючи співробітників, працівників за контрактом та сторонні організації) рекомендовано проходити початкове та періодичне навчання з питань роботи з відповідними процесами безпеки та правильним використанням об'єктів обробки інформації.
PR.AT-2. Користувачі (адміністратори) з превагами доступу розуміють свої обов’язки з питань кібербезпеки.	Усьому персоналу (включаючи співробітників, працівників за контрактом та сторонні організації) рекомендовано проходити початкове та періодичне навчання з питань роботи з правильними процесами безпеки та правильного використання об'єктів обробки інформації. Усьому персоналу, що відповідає за управління ризиками, розробку

1	2
	ОТ/АСУ ТП, системне адміністрування або обслуговування та інші завдання, що впливають на систему управління кібербезпекою (CSMS), рекомендовано пройти навчання з досягнення цілей безпеки та промислових операцій, пов'язаних з такими завданнями.
PR.AT-3. Партнери організації розуміють свої обов’язки з питань кібербезпеки.	Усьому персоналу (включаючи співробітників, працівників за контрактом та сторонні організації) рекомендовано проходити початкове та періодичне навчання з питань роботи з відповідними процесами безпеки та правильним використанням об'єктів обробки інформації.
PR.AT-4. Керівництво ОТ/АСУ ТП розуміє свої обов’язки з питань кібербезпеки.	Усьому персоналу (включаючи співробітників, працівників за контрактом та сторонні організації) рекомендовано проходити початкове та періодичне навчання з питань роботи з відповідними процесами безпеки та правильним використанням об'єктів обробки інформації.
PR.AT-5. Персонал із забезпечення фізичної та інформаційної безпеки розуміє свої обов’язки.	Усьому персоналу (включаючи співробітників, працівників за контрактом та сторонні організації) рекомендовано проходити початкове та періодичне навчання з питань роботи з відповідними процесами безпеки та правильним використанням об'єктів обробки інформації.

Таблиця 9 – Заходи кіберзахисту категорії PR.DS

Захід кіберзахисту	Опис
1	2
PR.DS-1. Дані, що зберігаються, захищено.	Система управління має забезпечувати можливість виявлення, фіксації, протидії та повідомлення про неавторизовані зміни програмного забезпечення та інформації під час їх зберігання. Система управління повинна забезпечувати можливість захисту конфіденційності інформації, для якої підтримується явна авторизація проведення операції читання, з урахуванням інформації, що зберігається або передається.
PR.DS-2. Дані, що передаються, захищено.	Система управління повинна забезпечувати можливість захисту цілісності інформації, що передається. Система управління має забезпечувати можливість захисту цілісності сеансів. Система управління повинна відмовляти у використанні некоректних ID сеансу. Система управління повинна забезпечувати можливість захисту конфіденційності інформації, для якої підтримується явна авторизація з метою проведення операції читання, з урахуванням інформації, що зберігається або передається Система управління повинна забезпечувати можливість видалення всієї інформації, для якої підтримується явна авторизація з метою читання, з компонентів, які мають бути виведені з активного сервісу та/або експлуатації.
PR.DS-3.Управління активами здійснюється з дотриманням правил видалення, передачі та розміщення.	Рекомендовано встановити та перевірити процедури щодо додавання, видалення чи ліквідації всіх об'єктів.

1	2
	Для інформації ОТ/АСУ ТП рекомендовано розробити та підтримувати процес управління документацією протягом життєвого циклу.
PR.DS-4. Необхідні спроможності для забезпечення доступності активів створено і підтримуються.	Система управління повинна забезпечувати можливість функціонування в режимі обмеженої функціональності під час події DoS. Система управління повинна забезпечувати можливість обмеження використання ресурсів за допомогою функцій безпеки для запобігання виснаженню ресурсів.
PR.DS-5. Захист від витоку даних впроваджено.	Система управління повинна забезпечувати можливість моніторингу та управління електронними комунікаціями на межах зон для забезпечення секціонування, визначеного в моделі зон і трактів, що базується на ризиках.
PR.DS-6. Механізми перевірки цілісності використовуються для верифікації програмного забезпечення, програмно-апаратних засобів та цілісності інформації.	Система управління повинна забезпечувати можливість захисту цілісності інформації, що передається. Система управління повинна забезпечувати можливість підтримки верифікації передбачуваної дії функцій безпеки та повідомляти про виявлення аномалій у ході FAT, SAT та планового технічного обслуговування. Ці функції безпеки повинні включати всі ті функції, які необхідні для підтримання вимог безпеки. Система управління має забезпечувати можливість виявлення, фіксації, протидії та повідомлення про неавторизовані зміни програмного забезпечення та інформації під час їх зберігання. Система управління має забезпечувати можливість захисту цілісності сеансів. Система

1	2
	управління повинна відмовляти у використанні некоректних ID сеансів.
PR.DS-7. Середовища розробки та тестування відокремлені від виробничого середовища.	Засоби розроблення, тестування та експлуатації слід відокремити для зменшення ризиків несанкціонованого доступу чи змін в операційному середовищі.

Таблиця 10 – Заходи кіберзахисту категорії PR.IP

Захід кіберзахисту	Опис
1	2
PR.IP-1. Базова конфігурація інформаційно-комунікаційних систем/системуправління виробничими процесами створена й підтримується.	Слід розробити та впровадити систему управління змінами для середовища ОТ/АСУ ТП. Процес управління змінами виконується за процедурою розподілу посадових обов'язків, що дозволяє уникнути конфлікту інтересів. Заплановані зміни в ОТ/АСУ ТП слід вивчати з використанням чітко визначених критеріїв щодо їх потенційного впливу на ризики HSE та ризики для інформаційної безпеки особами, які мають технічні знання про промислову експлуатацію та систему ОТ/АСУ ТП.
PR.IP-2. Життєвий цикл розробки, експлуатації та управління системами (SDLC) впроваджено.	Заплановані зміни в ОТ/АСУ ТП слід вивчати з використанням чітко визначених критеріїв щодо їх потенційного впливу на ризики HSE та ризики для інформаційної безпеки особами, які мають технічні знання про промислову експлуатацію та систему ОТ/АСУ ТП.
PR.IP-3. Процеси (заходи) управління змінами конфігурації впроваджено.	Слід розробити та впровадити систему управління змінами для середовища ОТ/АСУ ТП. Процес управління змінами виконується за процедурою розподілу посадових обов'язків, що дозволяє уникнути конфлікту інтересів. Заплановані зміни в ОТ/АСУ ТП слід вивчати з

1	2
	використанням чітко визначених критеріїв щодо їх потенційного впливу на ризики HSE та ризики для інформаційної безпеки особами, які мають технічні знання про промислову експлуатацію та систему ОТ/АСУ ТП.
PR.IP-4. Резервне копіювання інформації проводиться, підтримується та періодично тестується.	Рекомендовано створити, використовувати та підтверджувати відповідними перевірками процедуру резервування та відновлення систем та захисту резервних копій.
PR.IP-5. Правила (політика) та норми фізичної безпеки операційного середовища та обладнання організації (ОТ/АСУ ТП) виконуються.	Рекомендовано встановити політики та процедури безпеки, спрямовані на забезпечення фізичної безпеки та захисту від зовнішніх впливів у рамках захисту об'єктів. Для забезпечення захищеності від неавторизованого доступу та захисту об'єктів слід встановити один або кілька периметрів фізичної безпеки. На кожній межі слід передбачити відповідні засоби контролю доступу. Від співробітників вимагається виконання та примусове виконання встановлених процедур у рамках забезпечення фізичної безпеки. Усі лінії електронних комунікаційних мереж під контролем організації мають бути належним чином захищені від несанкціонованого втручання чи ушкодження.
PR.IP-6. Дані знищуються відповідно до політики безпеки.	Рекомендовано розробити політики та процедури, які детально описують процеси збереження, фізичного захисту та захисту цілісності, знищення та ліквідації всіх об'єктів залежно від їх класифікації, у тому числі письмові та електронні записи, обладнання та інші засоби, що містять дані, з урахуванням вимог законодавства.

1	2
PR.IP-7. Процеси кіберзахисту постійно вдосконалюються.	Рекомендовано призначити організацію для управління і координації вдосконаленнями та внесення змін до CSMS, використання встановленого методу внесення та реалізації змін. Керуюча організація повинна періодично оцінювати всю систему CSMS для забезпечення досягнення цілей безпеки. Організації рекомендовано створити перелік тригерних факторів із встановленими граничними значеннями для подальшого аналізування відповідних елементів CSMS та, можливо, внесення змін. Ці тригерні фактори повинні передбачати, як мінімум, факти серйозних інцидентів у системі безпеки, зміни у законодавстві та нормативних документах, зміни у ризиках та значні зміни у ОТ/АСУ ТП. Порогові значення мають базуватися на межах допустимості ризиків для організації. Організації рекомендовано визначити та проводити відповідні коригувальні та превентивні заходи, щоб модифікувати CSMS для виконання цілей безпеки. Аналізування меж допустимості ризиків для організації проводиться у разі значних змін в організації, технології, цілях діяльності і внутрішньої діяльності та у зовнішніх подіях, включаючи виявлені загрози та зміни у соціальній обстановці. Власникам системи управління рекомендовано проводити моніторинг галузі на предмет передових практик, що застосовуються в CSMS, для оцінки та пом'якшення ризиків, оцінювати їх застосовність.

1	2
	Організації рекомендовано ознайомитися із чинним законодавством та змінами у законодавстві, що стосуються кібербезпеки. Рекомендовано здійснювати активний пошук і доведення до відома керівництва пропозицій працівників у сфері безпеки щодо недоліків та потенціалу роботи системи безпеки.
PR.IP-9. Плани реагування (реагування на кіберінциденти та забезпечення безперервності бізнесу) і плани відновлення (відновлення після кіберінциденту та відновлення після аварії) наявні та управляються.	Плани безперервності рекомендовано розробляти та впроваджувати для того, щоб гарантувати можливість відновлення бізнес-процесів відповідно до цілей відновлення. Організації рекомендовано реалізувати план реагування на інциденти, в якому зазначити відповідальний персонал та заходи, які проводяться призначеними особами.
PR.IP-10. Плани реагування та відновлення тестуються.	План безперервності бізнесу рекомендовано перевіряти на постійній основі та оновлювати у разі потреби. Для перевірки програми реагування у робочому порядку мають бути проведені навчання.
PR.IP-12. План управління вразливостями розроблено й впроваджено.	Слід отримувати своєчасну інформацію щодо технічних вразливостей використовуваних інформаційних (автоматизованих) систем, оцінювати загрози організації таким вразливостям і вживати належних заходів, щоб урахувати пов’язаний з цим ризик. Керівники повинні регулярно перевіряти відповідність оброблення інформації та процедур у межах сфери їх відповідальності належним політикам, стандартам та іншим вимогам щодо безпеки.

Таблиця 11 – Заходи кіберзахисту категорії PR.MA

Захід кіберзахисту	Опис
1	2
PR.MA-1. Технічне обслуговування та ремонт активів ОТ/АСУ ТП виконуються та своєчасно документуються з використанням визначених та контрольованих засобів.	Усе обладнання, включаючи допоміжне обладнання для захисту від зовнішніх впливів, має підтримуватися у належному стані з метою забезпечення правильної роботи.
PR.MA-2. Дистанційне обслуговування активів ОТ/АСУ ТП схвалено, задокументовано та виконується в спосіб, що унеможливлює несанкціонований доступ.	Організація може реалізовувати схему аутентифікації з відповідним рівнем суворості для точного визначення дистанційного інтерактивного користувача. Організація повинна розробити політику, яка регулює дистанційний вхід у систему одним користувачем та/або через дистанційне з'єднання (наприклад, міжзадачні з'єднання) з системами управління, в яких визначалися б відповідні повідомлення системи про невдалі спроби входу та закінчення періодів неактивності. Після певної кількості невдалих спроб входу віддаленим користувачем система має деактивувати обліковий запис на певний термін.

Таблиця 12 – Заходи кіберзахисту категорії PR.PT

Захід кіберзахисту	Опис
1	2
PR.PT-1. Записи аудиту (журналів подій) визначено, задокументовано, впроваджено й перевірено відповідно до політик, правил, процедур з безпеки.	Рекомендовано встановити та перевірити процедури щодо додавання, видалення чи ліквідації всіх об'єктів. Рекомендовано виконувати періодичні перевірки щодо відповідності вимогам політики в галузі адміністрування облікових записів. Рекомендовано виконувати періодичні перевірки щодо відповідності інформації та політики управління документацією. У програмі аудиту має бути зазначена методика проведення аудиту. Підтвердження відповідності системи ОТ/АСУ ТП CSMS, CSMS має включати періодичні аудити системи ОТ/АСУ ТП для підтвердження того, що політика та процедури безпеки виконуються в належному порядку і для виконання цілей безпеки для конкретної зони. Має бути зазначено перелік документації та звітів, необхідних для створення журналу контролю.
PR.PT-2. Змінні носії захищено, а їх використання обмежено відповідно до правил, процедур з безпеки.	Система управління має забезпечувати можливість автоматичного висування конфігурованих обмежень на звернення, що передбачають заборону використання портативних та мобільних пристроїв; вимогу до авторизації, обумовленої контекстом; обмеження на передачу кодів і даних на(від) портативні та мобільні пристрої.

1	2
PR.PT-3. Контроль доступу до систем і активів здійснюється із застосуванням принципу мінімальних привілеїв.	Привілеї доступу, надані обліковими записами, рекомендовано встановлювати відповідно до політики організації щодо авторизації. Для всіх засобів контролю інформаційної безпеки вибір облікових записів доступу для окремих осіб на відміну від облікових записів для команди визначається з урахуванням загроз, ризиків та вразливостей. У цьому випадку враховуються ризики HSE окремих засобів контролю, зменшення ризиків з використанням сучасних засобів забезпечення фізичної безпеки, вимог до відповідальності та адміністративних/експлуатаційних потреб. Надання, зміна або припинення доступу здійснюються під контролем відповідного керівника. Рекомендовано вести реєстрацію всіх облікових записів доступу, включаючи докладні дані про особу та пристрої, авторизовані для використання облікового запису, їх дозволи та керівника, рішенням якого надаються дозволи. Облікові записи доступу тимчасово блокуються або видаляються, коли вони більше не потрібні (наприклад, при зміні посади). Усі встановлені облікові записи доступу рекомендовано постійно перевіряти, щоб гарантувати, що особа(и) та пристрої мають лише мінімально потрібні дозволи. Стандартні паролі для облікових записів доступу рекомендовано змінити до введення ОТ/АСУ ТП в експлуатацію. Рекомендовано виконувати періодичні перевірки щодо відповідності вимогам політики в

1	2
	галузі адміністрування облікових записів. Організації рекомендовано розробити стратегії або підходи до аутентифікації, що дозволяє визначати метод(и) аутентифікації для їхнього подальшого застосування. Усі користувачі мають проходити автентифікацію перед використанням додатка, що запитується, крім випадків, коли передбачено компенсуючі комбінації технологій контролю входу та адміністративних практик. Практики суворої автентифікації (наприклад, з вимогою ввести надійний пароль) рекомендовано застосовувати до всіх облікових записів для системних адміністраторів та конфігурації програм. У журналах реєстрації слід вести запис всіх спроб доступу до найважливіших систем. Такі журнали повинні перевірятися щодо вдалих і невдалих спроб доступу. Організація може реалізовувати схему аутентифікації з відповідним рівнем суворості для точного визначення дистанційного інтерактивного користувача. Організації рекомендовано розробити політику, яка регулює дистанційний вхід у систему одним користувачем та/або через дистанційне з'єднання (наприклад, міжзадачні з'єднання) із системами управління, в яких визначалися б відповідні повідомлення системи про невдалі спроби входу та закінчення періодів неактивності. Після певної кількості невдалих спроб входу віддаленим користувачем система має деактивувати обліковий запис на певний термін.

1	2
	Після закінчення певного періоду неактивності віддалений користувач повинен пройти повторну автентифікацію для отримання повторного доступу до системи. У системах рекомендовано реалізовувати відповідні схеми аутентифікації для міжзадачних з'єднань між додатками та пристроями. У політиці безпеки авторизації рекомендовано встановити правила, що визначають привілеї доступу, підтверджені для облікових записів для персоналу з різними посадовими функціями. Таку політику рекомендовано оформити документально та застосовувати щодо всього персоналу після процедури аутентифікації. Дозвіл на отримання доступу до пристроїв ОТ/АСУ ТП рекомендовано зробити логічним (правила, за якими надається або відхиляється доступ для користувачів залежно від їх посадових функцій), фізичним (замки, камери та інші засоби контролю, що обмежують доступ до активного пульта управління) або і тим, і іншим. Облікові записи з доступом рекомендовано визначати посадовими функціями для керування доступом до відповідної інформації або систем для такої посадової функції користувача. Під час визначення посадових функцій слід враховувати наслідки для безпеки. У середовищах, для яких потрібний особливий контроль, слід застосовувати множинні способи авторизації для обмеження доступу до ОТ/АСУ ТП.

1	2
PR.PT-4. Електронні комунікаційні мережі та мережі управління захищено.	Система управління має забезпечувати можливість захисту цілісності інформації, що передається. Система управління має виконувати валідацію синтаксичної структури та змісту будь-яких вхідних даних, які є вхідними даними управління технологічними процесами або вхідними даними, що безпосередньо впливають на роботу системи управління. Система управління має забезпечувати можливість захисту цілісності сеансів. Система управління повинна відмовляти у використанні некоректних ID сеансів. Система управління має забезпечувати можливість захисту конфіденційності інформації, для якої підтримується явна авторизація з метою здійснення операції читання, з урахуванням інформації, що зберігається або передається Якщо необхідна криптографія, то система управління має використовувати криптографічні алгоритми, довжину ключів та механізми для створення та управління ключами відповідно до загальноприйнятих практик і рекомендацій індустрії безпеки. Система управління має забезпечувати можливість логічного розмежування мереж систем управління щодо мереж, що не належать до систем управління, та логічного розмежування критично важливих мереж систем управління щодо інших мереж систем управління. Система управління має забезпечувати можливість моніторингу та управління електронними комунікаціями на межах зон для забезпечення секціонування,

1	2
	визначеного в моделі зон та трактів, що базується на ризиках. Система управління має забезпечувати можливість запобігання отриманню загально цільових повідомлень «абонент — абонент» користувачами або системами, які знаходяться за межами системи управління. Система управління має забезпечувати можливість функціонування в режимі обмеженої функціональності під час події DoS. Система управління має забезпечувати можливість її конфігурування відповідно до рекомендованих конфігурацій електронної комунікаційної мережі та безпеки, як описано в керівних документах, наданих постачальником системи управління. Система управління має забезпечувати інтерфейс для поточних параметрів конфігурації електронної комунікаційної мережі та безпеки.
PR.PT-5. Упровадження механізмів на ОТ/АСУ ТП для досягнення вимог до стійкості у разі надзвичайних ситуацій та інцидентів у кіберпросторі.	Організації рекомендовано розробити, задокументувати, реалізувати та підтримувати процеси, процедури та заходи безпеки для гарантування необхідного рівня безперервності щодо інформаційної безпеки під час надзвичайної ситуації. Обладнання оброблення інформації має бути впроваджено з резервуванням, достатнім для того, щоб відповідати вимогам доступності.

1.4. Клас заходів «Виявлення кіберінцидентів» (DE)

Таблиця 13 – Заходи кіберзахисту категорії DE.AE

Захід кіберзахисту	Опис
1	2
DE.AE-1. Еталони мережевих операцій та очікуваних потоків даних для користувачів і систем встановлені та управляються.	Організації рекомендовано створити перелік тригерних факторів зі встановленими граничними значеннями для подальшого аналізування відповідних елементів CSMS та, можливо, внесення змін. Ці тригерні фактори повинні включати, як мінімум, факти серйозних інцидентів у системі безпеки, зміни у законодавстві та нормативних документах, зміни у ризиках та значні зміни у ОТ/АСУ ТП. Порогові значення мають бути засновані на межах допустимості ризиків для організації. Привілеї доступу, надані обліковими записами, повинні встановлюватися відповідно до політики організації щодо авторизації. Для всіх засобів контролю інформаційної безпеки вибір облікових записів доступу для окремих осіб на відміну від облікових записів для команди визначається з урахуванням загроз, ризиків та вразливостей. У цьому випадку враховуються ризики HSE окремих засобів контролю, зменшення ризиків з використанням сучасних засобів забезпечення фізичної безпеки, вимог до відповідальності та адміністративних/експлуатаційних потреб. Надання, зміна або припинення доступу здійснюються під контролем відповідного керівника. Слід вести реєстрацію всіх облікових записів доступу, включаючи докладні дані про особу та пристрої, авторизовані для використання облікового запису, їх дозволи та керівника, рішенням якого надаються дозволи облікові записи доступу тимчасово блокуються або видаляються, коли вони більше не

1	2
	потрібні (наприклад, при зміні посади). Усі встановлені облікові записи доступу рекомендовано постійно перевіряти, щоб гарантувати, що особа(и) та пристрої мають лише мінімально потрібні дозволи. Стандартні паролі для облікових записів доступу рекомендовано змінювати до введення ОТ/АСУ ТП в експлуатацію. Рекомендовано виконувати періодичні перевірки щодо відповідності вимогам політики в галузі адміністрування облікових записів. Організації рекомендовано розробити стратегії або підходи до аутентифікації, що дозволяє визначати метод(и) аутентифікації для їхнього подальшого застосування. Усі користувачі повинні проходити автентифікацію перед використанням додатка, що запитується, крім випадків, коли передбачено компенсуючі комбінації технологій контролю входу та адміністративних практик. Практики суворої автентифікації (наприклад, з вимогою ввести надійний пароль) рекомендовано застосовувати до всіх облікових записів для системних адміністраторів та конфігурації програм. У журналах реєстрації слід вести запис всіх спроб доступу до найважливіших систем. Такі журнали повинні перевірятися щодо вдалих і невдалих спроб доступу. Організація може реалізовувати схему аутентифікації з відповідним рівнем суворості для точного визначення дистанційного інтерактивного користувача.

1	2
	Організації рекомендовано розробити політику, яка регулює дистанційний вхід у систему одним користувачем та/або через дистанційне з'єднання (наприклад, міжзадачні з'єднання) із системами управління, в яких визначалися б відповідні повідомлення системи про невдалі спроби входу та закінчення періодів неактивності. Після певної кількості невдалих спроб входу віддаленим користувачем система має деактивувати обліковий запис на певний термін. Після закінчення певного періоду неактивності віддалений користувач повинен пройти повторну автентифікацію для отримання повторного доступу до системи. У системах рекомендовано реалізовувати відповідні схеми аутентифікації для міжзадачних з'єднань між додатками та пристроями. У політиці безпеки авторизації рекомендовано встановити правила, що визначають привілеї доступу, підтверджені для облікових записів для персоналу з різними посадовими функціями. Таку політику слід оформити документально та застосовуватися щодо всього персоналу після процедури аутентифікації. Авторизація доступу до пристроїв ОТ/АСУ ТП може бути на логічному рівні (правила, за якими надається або відхиляється доступ для користувачів залежно від їх посадових функцій) або на фізичному (замки, камери та інші засоби контролю, що обмежують доступ до активного пульта управління), або змішаною.

1	2
	Облікові записи з доступом рекомендовано визначати посадовими функціями для керування доступом до відповідної інформації або систем для такої посадової функції користувача. Під час визначення посадових функцій слід враховувати наслідки для безпеки. У середовищах, для яких потрібний особливий контроль, необхідно застосовувати множинні способи авторизації для обмеження доступу до ОТ/АСУ ТП.
DE.AE-2. Існує практика аналізу виявлених подій.	При виявленні інциденту організації рекомендовано негайно відреагувати на нього відповідно до затверджених процедур. В організації мають існувати процедури виявлення невдалих та вдалих спроб порушення інформаційної безпеки. Інформація про виявлений інцидент має бути зафіксована із зазначенням інциденту, процедури реагування, висновків та будь-яких дій, вжитих для зміни CSMS після інциденту.
DE.AE-3. Дані про події збираються та корелюються з кількох джерел та датчиків.	Система управління має забезпечувати можливість доступу авторизованих фізичних осіб та/або інструментів до файлів реєстрації аудиту в режимі «тільки читання».

1	2
DE.AE-4. Існує процес визначення можливих впливів кіберінцидентів.	Організація: розробляє план дій у надзвичайних ситуаціях для інформаційної (автоматизованої) системи; розповсюджує копії плану на випадок надзвичайних ситуацій; координує заходи з планування на випадок надзвичайних ситуацій з ліквідації інцидентів; переглядає план дій у надзвичайних ситуаціях для інформаційної (автоматизованої) системи; оновлює план на випадок надзвичайних ситуацій, щоб вирішити зміни в організації, інформаційній системі або середовищі функціонування та проблеми, що виникли під час впровадження, виконання або тестування плану, на випадок непередбачених обставин; повідомляє про зміни плану на випадок надзвичайних ситуацій; захищає план дій у надзвичайних ситуаціях від несанкціонованого розкриття та модифікації. Організація реалізує можливість обробки інцидентів для інцидентів безпеки, що передбачає підготовку, виявлення та аналіз, стримування, ліквідацію та відновлення, координує заходи з ліквідації інцидентів з плануванням на випадок надзвичайних ситуацій і вносить навички, отримані з поточної діяльності з обробки інцидентів, у процедури реагування на інциденти, навчання та тестування, і впроваджує зміни, що виникли. Організація: проводить оцінку ризику, включаючи ймовірність і величину збитку від несанкціонованого доступу, використання, розкриття, порушення, модифікації або знищення інформаційної (автоматизованої)

1	2
	системи та інформації, яку вона обробляє, зберігає або передає; документує результати оцінки ризиків, переглядає результати оцінки ризиків, поширює результати оцінки ризиків; оновлює оцінку ризику або щоразу, коли відбуваються значні зміни в інформаційній системі або середовищі функціонування (включаючи виявлення нових загроз і вразливостей), або інші умови, які можуть вплинути на стан безпеки системи; контролює інформаційну систему; визначає несанкціоноване використання інформаційної (автоматизованої) системи; розгортає пристрої моніторингу; захищає інформацію, отриману за допомогою засобів моніторингу вторгнень, від несанкціонованого доступу, зміни та видалення. Підвищує рівень активності моніторингу інформаційної (автоматизованої) системи кожного разу, коли є ознаки підвищеного ризику для організаційних операцій та активів, окремих осіб, інших організацій чи країни на основі інформації правоохоронних органів, розвідувальної інформації чи інших надійних джерел інформації; одержує юридичний висновок щодо діяльності з моніторингу інформаційної (автоматизованої) системи відповідно до чинного законодавства, розпоряджень, директив, політик або нормативних актів.
DE.AE-5. Пороги оповіщення про кіберінциденти встановлено.	Організації рекомендовано визначити періодичність проведення повторного аналізування ризиків та вразливостей, а також критерії початку аналізування залежно від змін технології, організації чи промислової експлуатації.

Таблиця 14 – Заходи кіберзахисту категорії DE.CM

Захід кіберзахисту	Опис
1	2
DE.CM-1. Електронна комунікаційна мережа (ОТ/АСУ ТПІ) відстежується для виявлення потенційних кіберінцидентів.	Система управління має забезпечувати можливість безперервного моніторингу функціонування всіх механізмів безпеки за допомогою загальноприйнятих практик та рекомендацій індустрії безпеки для оперативного виявлення, опису та інформування про прогалини в безпеці.
DE.CM-2. Фізичне середовище відстежується для виявлення потенційних кіберінцидентів.	Рекомендовано встановити процедури контролю та оповіщення у випадках виникнення загрози для фізичної безпеки або захисту від зовнішніх впливів.
DE.CM-3. Активність персоналу відстежується для виявлення потенційних кіберінцидентів.	Система управління має забезпечувати можливість безперервного моніторингу функціонування всіх механізмів безпеки за допомогою загальноприйнятих практик та рекомендацій індустрії безпеки для оперативного виявлення, опису та інформування про прогалини в безпеці.
DE.CM-4. Шкідливий код виявляється.	Рекомендовано встановити, документально оформити та виконати процедуру управління антивірусною безпекою/захистом від шкідливих програм.

1	2
DE.CM-5. Несанкціонований програмний продукт виявлено.	Система управління має забезпечувати можливість висування обмежень на звернення з використанням технологій мобільного коду, виходячи з ризику заподіяння шкоди системі управління, і ці обмеження містять: заборону виконання мобільного коду; запит відповідної автентифікації та авторизації для джерела коду; обмеження передачі мобільного коду до системи керування та від неї; відстеження використання мобільного коду.
DE.CM-6. Активність зовнішнього постачальника товарів і послуг відстежується з метою виявлення потенційних кіберінцидентів.	Організації рекомендовано здійснювати нагляд над аутсорсинговим розробленням систем, а також його моніторинг. Організації рекомендовано регулярно проводити моніторинг, перегляд та аудит отримання послуг постачальника.
DE.CM-7. Моніторинг неавторизованого персоналу, з'єднань, пристроїв і програмного забезпечення здійснюється на постійній основі.	Інформаційна (автоматизована) система організації: забезпечує можливість створення записів аудиту для подій, які підлягають аудиту; дозволяє вибрати події, які підлягають аудиту, аудит конкретних компонентів інформаційної (автоматизованої) системи; генерує аудиторські записи для подій. Організація розробляє стратегію постійного моніторингу та реалізує програму безперервного моніторингу стану безпеки. Організація: визначає типи змін в інформаційній системі, які керуються конфігурацією; переглядає запропоновані зміни інформаційної (автоматизованої) системи, керовані конфігурацією, і схвалює або відхиляє

1	2
	такі зміни з явним урахуванням для аналізу впливу на безпеку; переглядає документи рішення щодо зміни конфігурації, пов'язані з інформаційною системою; упроваджує затверджені конфігураційні зміни до інформаційної (автоматизованої) системи; зберігає записи конфігураційних змін інформаційної (автоматизованої) системи. Організація: проводить аудит і перевірку діяльності, пов’язаної зі змінами інформаційної (автоматизованої) системи, що керуються конфігурацією; координує та забезпечує нагляд за діяльністю контролю змін конфігурації; розробляє та документує інвентаризацію компонентів інформаційної (автоматизованої) системи; переглядає та оновлює інвентаризацію компонентів інформаційної (автоматизованої) системи; забезпечує доступ виключно після авторизації; веде журнали перевірки фізичного доступу; забезпечує контроль доступу до територій всередині об’єкта, офіційно визначених як загальнодоступні; супроводжує відвідувачів та контролює активність відвідувачів; захищає ключі, комбінації та інші пристрої фізичного доступу; змінює комбінації та ключі та/або коли ключі втрачені, комбінації скомпрометовані; проводить моніторинг фізичного доступу до об’єкта, де знаходиться інформаційна (автоматизована) система, для виявлення інцидентів фізичної безпеки та реагування на них, переглядає журнали фізичного доступу після виникнення інциденту; переглядає журнали фізичного

1	2
	доступу після виникнення інциденту; узгоджує результати оглядів та розслідувань із можливостями реагування на інциденти організації. Організація: здійснює відстеження та моніторинг розташування та переміщення всередині; забезпечує використання технологій розташування активів відповідно до вимог чинного законодавства, розпоряджень, директив, правил, політик, стандартів і вказівок; проводить моніторинг інформаційної (автоматизованої) системи; визначає несанкціоноване використання інформаційної (автоматизованої) системи; розгортає пристрої моніторингу; захищає інформацію, отриману за допомогою засобів моніторингу вторгнень, від несанкціонованого доступу, зміни та видалення; підвищує рівень активності моніторингу інформаційної (автоматизованої) системи кожного разу, коли є ознаки підвищеного ризику для організаційних операцій та активів, окремих осіб, інших організацій чи країни на основі інформації правоохоронних органів, розвідувальної інформації чи інших надійних джерел інформації; одержує експертний висновок щодо діяльності з моніторингу інформаційної (автоматизованої) системи відповідно до вимог чинного законодавства, директив, політик або нормативних актів.
DE.CM-8. Сканування вразливостей виконується.	Організації рекомендовано визначити підходи та методи аналізування ризиків, які визначають та розставляють у порядку пріоритету ризики, пов'язані із загрозами безпеці, вразливостями та наслідками для

1	2
	матеріальних об'єктів ОТ/АСУ ТП. Організації рекомендовано виконати детальний аналіз вразливостей своїх окремих логічних ОТ/АСУ ТП, сфера охоплення якого залежить від результатів розширеного аналізу ризиків та пріоритету предмета ОТ/АСУ ТП відносно таких ризиків.

Таблиця 15 – Заходи кіберзахисту категорії DE.DP

Захід кіберзахисту	Опис
1	2
DE.DP-1. Обов'язки щодо виявлення кіберінцидентів чітко визначено задля забезпечення звітності.	Рекомендовано призначити організацію для управління і координації вдосконаленнями та внесення змін до CSMS, використання встановленого методу внесення та реалізації змін.
DE.DP-2. Заходи виявлення кіберінцидентів відповідають всім застосованим вимогам.	Керуючій організації рекомендовано періодично оцінювати всю систему CSMS для забезпечення досягнення цілей безпеки.
DE.DP-3. Процеси виявлення кіберінцидентів протестовані.	Керуючій організації рекомендовано періодично оцінювати всю систему CSMS для забезпечення досягнення цілей безпеки.
DE.DP-4. Інформацію про виявлені кіберінциденти повідомлено партнерів організації.	Зафіксована інформація про інцидент має бути своєчасно передана всім відповідним організаціям (тобто керівництву, підрозділам, що займаються інформаційними технологіями, безпекою технологічного процесу, автоматизацією, безпекою автоматичного управління та виробництвом).
DE.DP-5. Процеси виявлення кіберінцидентів постійно вдосконалюються.	Організації рекомендовано визначити та проводити відповідні коригувальні та превентивні заходи, щоб модифікувати CSMS для виконання цілей безпеки.

1.5. Клас заходів «Реагування на кіберінциденти» (RS)

Таблиця 16 – Підкатегорія заходів кіберзахисту категорії RS.RP

Захід кіберзахисту	Опис
RS.RP-1. План реагування виконується під час або після події.	Організації рекомендовано реалізувати план реагування на інциденти, в якому зазначити відповідальний персонал та заходи, які проводиться призначеними особами.

Таблиця 17 – Заходи кіберзахисту категорії RS.CO

Захід кіберзахисту	Опис
1	2
RS.CO-1. Персонал знає свої обов'язки та порядок дій у ситуаціях, коли необхідне реагування на кіберінциденти.	План реагування на інциденти має передаватися всім відповідним організаціям. Організації рекомендовано створити процедуру сповіщення про незвичайні дії чи події, які фактично можуть бути інцидентами у системі інформаційної безпеки. Персоналу повинні бути роз'яснені його обов'язки щодо повідомлення про інциденти в системі інформаційної безпеки та методи сповіщення про ці інциденти.
RS.CO-2. Факти про кіберінциденти задокументовано та повідомляються відповідно до встановлених критерій.	Організація має своєчасно повідомляти про інциденти у системі інформаційної безпеки.
RS.CO-3. Здійснюється обмін інформацією про кіберінциденти відповідно до планів реагування.	План реагування на інциденти має передаватися всім відповідним організаціям.
RS.CO-4. Координація з партнерами організації проводиться відповідно до планів реагування.	Організація має своєчасно повідомляти про інциденти у системі інформаційної безпеки.

1	2
RS.CO-5. З метою досягнення ширшої ситуативної обізнаності щодо стану кібербезпеки здійснюється обмін інформацією з основними суб'єктами національної системи кібербезпеки та зовнішніми партнерами організації.	Організація має встановлювати та інституціалізувати контакти з окремими групами та асоціаціями з рамках спільноти безпеки, зокрема сприяти безперервному навчанню організаційного персоналу з питань безпеки, підтримувати актуальність за допомогою рекомендованих методів, засобів і технологій безпеки для обміну поточною інформацією, пов'язаною з безпекою, включаючи загрози, вразливості та інциденти. Організація має постійно отримувати сповіщення про безпеку інформаційної (автоматизованої) системи, рекомендації та директиви, генерувати сповіщення внутрішньої безпеки, рекомендації та директиви, якщо вважає за необхідне, розповсюджувати сповіщення безпеки, рекомендації та директиви. Організація виконує директиви безпеки відповідно до встановлених термінів або повідомляє організацію, яка повідомляє, про ступінь невідповідності.

Таблиця 18 – Заходи кіберзахисту категорії RS.AN

Захід кіберзахисту	Опис
1	2
RS.AN-1. Повідомлення від систем виявлення кіберінцидентів досліджуються.	При виявленні інциденту організації рекомендовано негайно відреагувати на нього відповідно до затверджених процедур. В організації мають існувати процедури виявлення невдалих та вдалих спроб порушення інформаційної безпеки. Інформація про виявлений інцидент має бути зафіксована із зазначенням інциденту, процедури реагування, висновків та будь-яких дій, вжитих для зміни CSMS після інциденту.
RS.AN-2. Вплив кіберінциденту усвідомлено.	При виявленні інциденту організації рекомендовано негайно відреагувати на нього відповідно до затверджених процедур. В організації мають існувати процедури виявлення невдалих та вдалих спроб порушення інформаційної безпеки. Інформація про виявлений інцидент має бути зафіксована із зазначенням інциденту, процедури реагування, висновків та будь-яких дій, вжитих для зміни CSMS після інциденту.
RS.AN-4. Кіберінциденти класифіковано відповідно до планів реагування. Електронні докази збираються та фіксуються належним чином.	При виявленні інциденту організації рекомендовано негайно відреагувати на нього відповідно до затверджених процедур.
RS.AN-5. Створено процеси для отримання, аналізу та реагування на чинники вразливості, виявлені організацією з внутрішніх і зовнішніх джерел.	Конфліктуючі обов’язки та сфери відповідальності мають бути розподілені для зменшення можливостей неавторизованої чи ненавмисної модифікації або неправильного використання ресурсів систем захисту інформації організації.

Таблиця 19 – Заходи кіберзахисту категорії RS.MI

Захід кіберзахисту	Опис
1	2
RS.MI-1. Кіберінциденти стримано.	При виявленні інциденту організації рекомендовано негайно відреагувати на нього відповідно до затверджених процедур.
RS.MI-2. Наслідки кіберінцидентів мінімізовано.	При виявленні інциденту організації рекомендовано негайно відреагувати на нього відповідно до затверджених процедур. В організації має існувати методика вирішення виявлених проблем та забезпечення їх виправлення.
RS.MI-3. Вперше виявлені вразливості усунено або задокументовано як прийняті ризики.	Треба отримувати своєчасну інформацію щодо технічних вразливостей інформаційних (автоматизованих) систем, які використовуються, оцінювати підвладність організації таким вразливостям і вживати належних заходів, щоб урахувати пов’язаний з цим ризик.

Таблиця 20 – Заходи кіберзахисту категорії RS.IM

Захід кіберзахисту	Опис
1	2
RS.IM-1. У планах реагування враховано отриманий досвід.	В організації має існувати методика вирішення виявлених проблем та забезпечення їх виправлення. Організації рекомендовано визначити та проводити відповідні коригувальні та превентивні заходи, щоб модифікувати CSMS для виконання цілей безпеки.
RS.IM-2. Плани реагування оновлено.	Організація: розробляє план дій у надзвичайних ситуаціях для інформаційної (автоматизованої) системи; розповсюджує копії плану на

1	2
	випадок надзвичайних ситуацій; координує заходи з планування на випадок надзвичайних ситуацій з ліквідації інцидентів. Переглядає план дій у надзвичайних ситуаціях для інформаційної (автоматизованої) системи; оновлює план на випадок надзвичайних ситуацій, щоб внести зміни в організації, інформаційній системі або середовищі функціонування та розв'язати проблеми, що виникли під час впровадження, виконання або тестування плану на випадок непередбачених обставин; повідомляє про зміни плану на випадок надзвичайних ситуацій; захищає план дій у надзвичайних ситуаціях від несанкціонованого розкриття та модифікації. Організація реалізує можливість обробки інцидентів для інцидентів безпеки, що передбачає підготовку, виявлення та аналіз, стримування, ліквідацію та відновлення, координує заходи з ліквідації інцидентів з плануванням на випадок надзвичайних ситуацій і враховує досвід, отриманий з поточної діяльності з обробки інцидентів, при проведенні процедур реагування на інциденти, навчанні та тестуванні і впроваджує зміни, що виникли. Організація: розробляє план реагування на інциденти; розповсюджує копії плану реагування на інциденти; переглядає план реагування на інциденти. Оновлює план реагування на інциденти для вирішення

1	2
	системних/організаційних змін або проблем, які виникли під час впровадження, виконання або тестування плану; повідомляє про зміни плану реагування на інциденти та захищає план реагування на інциденти від несанкціонованого розкриття та модифікації.

1.6. Клас заходів «Відновлення стану кібербезпеки» (RC)

Таблиця 21 – Заходи кіберзахисту категорії RC.RP

Захід кіберзахисту	Опис
1	2
RC.RP-1. План відновлення виконується під час або після кіберінцидентів.	Реагування на інциденти інформаційної безпеки має здійснюватися відповідно до задокументованої процедури
RC.RP-2. Плани відновлення оновлено.	Організація: розробляє план дій у надзвичайних ситуаціях для інформаційної (автоматизованої) системи; розповсюджує копії плану на випадок надзвичайних ситуацій; координує заходи з планування на випадок надзвичайних ситуацій з ліквідації інцидентів. Переглядає план дій у надзвичайних ситуаціях для інформаційної (автоматизованої) системи; оновлює план на випадок надзвичайних ситуацій, щоб вирішити зміни в організації, інформаційній системі або середовищі функціонування та розв’язати проблеми, що виникли під час впровадження, виконання або тестування плану, на випадок непередбачених обставин; повідомляє про зміни плану на випадок надзвичайних ситуацій;

1	2
	захищає план дій у надзвичайних ситуаціях від несанкціонованого розкриття та модифікації; реалізує можливість обробки інцидентів безпеки, що передбачає підготовку, виявлення та аналіз, стримування, ліквідацію та відновлення; координує заходи з ліквідації інцидентів з плануванням на випадок надзвичайних ситуацій і включає навички, отримані з поточної діяльності з обробки інцидентів, у процедури реагування на інциденти, навчання та тестування і впроваджує зміни, що виникли; розробляє план реагування на інциденти, розповсюджує копії плану реагування на інциденти та переглядає план реагування на інциденти, оновлює план реагування на інциденти для вирішення системних/організаційних змін або проблем, які виникли під час впровадження, виконання або тестування плану; повідомляє про зміни плану реагування на інциденти; захищає план реагування на інциденти від несанкціонованого розкриття та модифікації.

Таблиця 22 – Заходи кіберзахисту категорії RC.IM

Захід кіберзахисту	Опис
RC.IM-1. Плани відновлення враховують отриманий досвід.	Організації рекомендовано визначити та проводити відповідні коригувальні та превентивні заходи, щоб модифікувати CSMS для виконання цілей безпеки.

Таблиця 23 – Підкатегорії заходів кіберзахисту категорії RC.CO

Захід кіберзахисту	Опис
1	2
RC.CO-1. Процес зв'язків з громадськістю організований та керований.	Організація спрямовує інтеграцію стратегії та операцій щодо ризику ІТ із стратегічними рішеннями та операціями щодо ризику організації.
RC.CO-2. Репутація після кіберінцидентів відновлюється.	Організація спрямовує інтеграцію стратегії та операцій щодо ризику ІТ із стратегічними рішеннями та операціями щодо ризику організації.
RC.CO-3. Заходи з відновлення повідомлено внутрішнім та зовнішнім партнерам організації, а також керівництву.	Розробляє план дій у надзвичайних ситуаціях для інформаційної (автоматизованої) системи; розповсюджує копії плану на випадок надзвичайних ситуацій; координує заходи з планування на випадок надзвичайних ситуацій з ліквідації інцидентів; переглядає план дій у надзвичайних ситуаціях для інформаційної (автоматизованої) системи, оновлює план на випадок надзвичайних ситуацій, щоб вирішити зміни в організації, інформаційній системі або середовищі функціонування та розв’язати проблеми, що виникли під час впровадження, виконання або тестування плану на випадок непередбачених обставин; повідомляє про зміни плану на випадок надзвичайних ситуацій; захищає план дій у надзвичайних ситуаціях від несанкціонованого розкриття та модифікації. Організація реалізує можливість обробки інцидентів для інцидентів безпеки, що передбачає

1	2
	підготовку, виявлення та аналіз, стримування, ліквідацію та відновлення, координує заходи з ліквідації інцидентів з плануванням на випадок надзвичайних ситуацій і враховує досвід, отриманий з поточної діяльності з обробки інцидентів, при проведенні процедур реагування на інциденти, навчання та тестування, і впроваджує зміни, що виникли.

2. Виконання завдань циклу управління кібербезпекою для ОТ/АСУ ТП

Діяльність із забезпечення кібербезпеки спрямована на зниження ризиків кібербезпеки, носить безперервний циклічний характер та формує цикл управління кібербезпекою, який складається з п’яти функцій кібербезпеки (рис.):

ідентифікація ризиків;

кіберзахист;

виявлення кіберінцидентів;

реагування;

відновлення поточного стану кібербезпеки.

Рисунок – Цикл управління кібербезпекою

Захист ОТ/АСУ ТП базується на поєднанні ефективних політик безпеки та належним чином налаштованого набору засобів захисту. У процесі вибору і впровадження засобів захисту для застосування до ОТ/АСУ ТП необхідно враховувати:

які засоби захисту необхідні для адекватного зниження ризику до прийнятного рівня, що підтримує належний рівень функціонування організації та її бізнес-функції;

чи впроваджено обрані засоби захисту або чи існує реалістичний план впровадження;

який необхідний рівень гарантії того, що вибрані засоби захисту впроваджуються правильно, працюють за призначенням і дають бажаний результат.

На зазначені запитання слід відповідати в контексті ефективного процесу управління ризиками в масштабі всієї організації та стратегії кібербезпеки, яка визначає, пом'якшує (у разі потреби) і постійно контролює ризики для її ОТ/АСУ ТП. Ефективна стратегія кібербезпеки для ОТ/АСУ ТП має застосовувати поглиблений захист — техніку пошарових механізмів безпеки, щоб звести до мінімуму вплив збою в будь-якому механізмі. Використання саме такої стратегії в керуванні безпекою ОТ/АСУ ТП описано в розділі 3. У ньому описується процес застосування циклу управління кібербезпекою до ОТ/АСУ ТП, який містить короткий опис діяльності з реалізації кожної з п'яти функцій кібербезпеки, вказує відповідні заходи захисту та містить інформаційні посилання на інші документи.

3. Порядок впровадження профілів захищеності ОТ/АСУ ТП та підтвердження їх виконання

3.1. Ідентифікація (ID)

Функція ідентифікації забезпечує основні дії для ефективного використання заходів з кібербезпеки. Результатом функції ідентифікації є розвиток організаційного управління ризиками кібербезпеки для систем, людей, активів, даних і можливостей.

3.1.1. Управління активами (ID.AM)

Здатність організацій належним чином і послідовно визначати та послідовно керувати даними, персоналом, пристроями, системами та засобами на основі їх відносної важливості забезпечує базову здатність підтримувати організаційну програму кібербезпеки. Крім того, оновлення інформації про інвентаризацію, коли компоненти додаються, видаляються або змінюються (наприклад, виправлення, встановлення нового мікропрограмного забезпечення, заміна компонентів під час обслуговування), допомагає організаціям точно керувати загальними ризиками середовища. Організаціям рекомендовано розглянути можливість внесення таких заходів для підтримки

своїх можливостей управління активами:

унікальні ідентифікатори для диференціації та відстеження активів;

керування інвентаризацією обладнання для відстеження обчислювальних і мережевих пристроїв у середовищі, включаючи деталі пристроїв і місцезнаходження. Деталі пристрою можуть містити інформацію про постачальника, модель, серійний номер, інформацію про придбання та інформацію про виробництво/збірку (наприклад, інформацію про походження);

управління інвентаризацією програмного та мікропрограмного забезпечення для відстеження програмного та мікропрограмного забезпечення, встановленого з компонентами операційних технологій, включаючи номери версій та інформацію про місцезнаходження, опис матеріалів програмного забезпечення тощо;

інформація про постачальника для створення сховища інформації про постачальника, контактних осіб, інформації про гарантії, місць відкликання та оновлення інформації тощо;

задокументовані ролі та обов'язки для визначення конкретних осіб, команд або організаційних груп, які представляють власника активів, а також тих, хто відповідає за експлуатацію, технічне обслуговування і кібербезпеку.

Додаткові вказівки щодо ID.AM викладені в НД ТЗІ 3.6-006-21 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних (автоматизованих) систем». Заходи захисту:

«IA-3 Ідентифікація та автентифікація пристроїв»;

«IA-4 Управління ідентифікацією»;

«PM-3 Ресурси забезпечення інформаційної безпеки та приватності»;

«PM-5 Інвентаризація системи».

Рекомендації з підтвердження виконання заходів для ОТ/АСУ ТП

В організації забезпечено повноту та точність інвентаризації активів для управління ризиками в середовищі ОТ. Точна інвентаризаційна інформація підтримує численні цілі управління ризиками, включаючи оцінку ризиків, управління вразливістю та відстеження старіння.

Хоча автоматизовані інструменти для підтримки управління активами, як правило, кращі, організаціям слід розглянути, як інструмент збирає інформацію та чи може метод збору (наприклад, активне сканування) мати негативний вплив на їхні системи ОТ. Перед розгортанням у виробничому середовищі ОТ рекомендується виконати тестування за допомогою автоматизованих інструментів керування активами в автономних системах або компонентах. Якщо автоматизовані інструменти неможливі через архітектуру мережі або інші проблеми середовища ОТ, організації слід розглянути ручні процеси для підтримки поточної інвентаризації.

3.1.1.1. Відображення потоків даних (ID.AM-3)

Діаграми потоку даних дозволяють виробнику зрозуміти потік даних між мережевими компонентами. Документування потоків даних дозволяє організаціям зрозуміти очікувану поведінку своїх мереж. Це розуміння того, як пристрої спілкуються, допомагає у розв'язанні проблем, а також у реагуванні та відновленні. Ця інформація може бути використана під час судово-медичної діяльності або для аналізу з метою виявлення аномалій.

Рекомендації з упровадження та підтвердження виконання заходів для ОТ/АСУ ТП

Організаціям слід враховувати вплив на системи ОТ від використання автоматизованих інструментів відображення потоку даних, які використовують активне сканування або вимагають інструменти моніторингу мережі (наприклад, вбудовані мережеві зонди). Вплив може бути спричинений характером інформації, обсягом мережевого трафіка або миттєвим відключенням компонентів виробничої системи від мережі. Розгляньте можливість використання інструментів відображення потоку даних, які використовують ці методи під час запланованого простою.

3.1.1.2. Документація щодо архітектури мережі (підтримує результат ID.AM)

Інструменти документування мережевої архітектури дозволяють виробнику ідентифікувати, документувати та складати схеми взаємозв'язків між мережевими пристроями, корпоративними мережами та іншими зовнішніми з'єднаннями. Повне розуміння взаємозв'язків у середовищі має вирішальне значення для успішного розгортання засобів кіберзахисту кібербезпеки. Ця інформація також важлива для ефективного моніторингу мережі.

Рекомендації з упровадження та підтвердження виконання заходів для ОТ/АСУ ТП

Інструменти документації мережевої архітектури, які використовують технології автоматизованого виявлення топології, здатні отримувати деталі лише з мережевих пристроїв на базі IP. Багато середовищ ОТ містять ізольовані системи, компоненти або системи, підключені до мереж, що побудовані не на стеку протоколів TCP/IP. Середовище ОТ може бути технічно нездатним використовувати автоматизовані засоби документування архітектури мережі. Для документування цих компонентів можуть знадобитися ручні процеси.

Власники активів можуть також розглянути, як автоматизоване сканування може потенційно вплинути на систему ОТ, тестуючи інструменти автоматизації в невиробничому середовищі. На основі результатів тестування власники активів повинні розглянути можливість використання автоматизованих інструментів документування архітектури мережі ОТ під час запланованого простою.

Організації також можуть розглянути можливість використання фізичних перевірок мережевих з'єднань ОТ або аналізу мережевих журналів для документування архітектури мережі ОТ, особливо якщо мережа невелика чи складна. Проведення моніторингу мережевої активності ОТ може допомогти організаціям визначити додавання або видалення пристроїв у середовищі між запланованими діями сканування.

3.1.2. Управління (ID.GV)

Ефективне управління передбачає долучення керівництвом організації цілей управління ризиками разом із цілями стійкості, конфіденційності та кібербезпеки до процесу стратегічного планування та надання необхідних ресурсів для ефективного впровадження та підтримки програми кібербезпеки. На основі цього процесу керівництво організації розробляє та поширює політику, що встановлює вимоги безпеки для свого середовища. Ці політики передбачають, наприклад, визначення та розподіл ролей, обов'язків, зобов'язань керівництва та дотримання вимог. Політики також можуть відображати координацію між організаційними підрозділами, відповідальними за різні аспекти безпеки (тобто технічні, фізичні, кадрові, кіберфізичні, контроль доступу, захист медіа, управління вразливістю, обслуговування, моніторинг).

Додаткові вказівки для ID.GV викладені в НД ТЗІ 3.6-006-21 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних (автоматизованих) систем».

Заходи захисту:

«PM-1 програма (концепція) інформаційної безпеки»;

«PM-2 Ролі програми інформаційної безпеки»;

«PM-3 Ресурси забезпечення інформаційної безпеки та приватності»;

«PM-4 План дій та етапи»;

«PM-9 Стратегія управління ризиками»;

«PM-10 Процес акредитації»;

«PM-11 Визначення Завдань і процесів»;

«PM-12 Програма інсайдерської загрози»;

«PM-13 Безпека та приватність працівників»;

«PM-16 Програма інформування про загрози»;

«PM-18 Програма (концепція) забезпечення приватності».

Рекомендації з упровадження та підтвердження виконання заходів для ОТ/АСУ ТП

Організаціям рекомендовано:

переконатися, що програма кібербезпеки забезпечена достатніми ресурсами для підтримки стратегії управління ризиками ІТ та ОТ організації;

переконатися, що політики враховують повний життєвий цикл систем ОТ;

переконатися, що законодавчі та нормативні вимоги кібербезпеки, що впливають на операції ОТ, розуміються та керуються ними.

переконатися, що встановлено одну чи кілька посад із відповідальністю за управління організацією та управління ризиками для програм кібербезпеки ІТ та ОТ;

переконатися, що налагоджено комунікації та координації між ІТ та ОТ організаціями;

здійснювати перехресне навчання персоналу ІТ та ОТ для підтримки програми кібербезпеки.

3.1.3. Оцінка ризику (ID.RA)

Оцінка ризиків кібербезпеки виконується для виявлення ризиків і оцінки масштабу шкоди для операцій, активів або осіб у результаті кіберінцидентів, таких як несанкціонований доступ, використання, розголошення, збій, модифікація або знищення інформаційної (автоматизованої) системи чи даних. Організаціям слід враховувати частоту оновлення оцінок ризиків і тестування засобів кіберзахисту кібербезпеки системи.

Додаткові вказівки щодо ID.RA наведені в НД ТЗІ 3.6-006-21 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних (автоматизованих) систем».

Заходи захисту:

«RA-1 Політика та процедури оцінювання ризику»;

«RA-2 Категоріювання безпеки»;

«RA-3 Оцінювання ризику»;

«RA-5 Сканування вразливостей»;

«RA-6 Заходи протидії технічній розвідці»;

«RA-7 Реагування на ризик»;

«RA-8 Оцінювання впливу на приватність»;

«RA-9 Аналіз критичності».

Рекомендації з упровадження та підтвердження виконання заходів для ОТ/АСУ ТП

У середовищі ОТ ризики та наслідки можуть бути пов’язані з безпекою, здоров’ям та навколишнім середовищем додатково до бізнес/фінансових наслідків. У результаті організації можуть виявити, що визначити аналіз витрат і вигод для деяких типів ризиків неможливо. У таких випадках організаціям слід розглянути можливість перегляду минулих кібер- і некібер-інцидентів, які спричинили втрату живлення, втрату контролю, втрату вихідної подачі, втрату вихідної потужності та основні збоїв обладнання. PHA, FMEA або аналіз минулих подій можна використовувати, щоб зрозуміти потенційний вплив кіберінциденту. ISA 62443-3-2 містить вказівки щодо того, як оцінити кіберризик у середовищі з такими потенційними наслідками.

Оцінки ризиків також вимагають виявлення як вразливостей, так і загроз для середовища ОТ. Ведення точної інвентаризації активів ІТ та ОТ у робочому середовищі, включаючи постачальника продукту, номери моделей, мікропрограми, ОС і версії програмного забезпечення, встановлені на активах, полегшує ідентифікацію, відстеження та усунення вразливостей. Інформація про вразливості ОТ доступна різними методами, зокрема:

моніторинг груп безпеки, асоціацій і постачальників для сповіщень безпеки та порад;

NVD для отримання детальної інформації про відомі вразливості в апаратних і програмних активах;

інформацію про загрози, що стосуються навколишнього середовища, можна отримати як із внутрішніх ресурсів, так і на зовнішніх форумах для обміну інформацією про загрози. Організаціям слід розглянути можливість участі в обміні інформацією про кіберзагрози.

3.1.4. Стратегія управління ризиками (ID.RM)

Стратегія управління ризиками вказує на те, як ризик формується, оцінюється, реагує на нього та контролюється, а також забезпечує послідовний підхід до прийняття рішень на основі оцінки ризику в усій організації. Толерантність до ризику, припущення, обмеження, пріоритети та компроміси визначаються для прийняття інвестиційних та операційних рішень. Крім того, стратегія управління ризиками визначає прийнятні методології оцінки ризиків, потенційні реакції на ризики та процес постійного моніторингу стану безпеки (або впровадження контрзаходів/результатів безпеки) організації.

Додаткові вказівки щодо ID.RM наведені в НД ТЗІ 3.6-006-21 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних (автоматизованих) систем».

Заходи захисту:

«PM-9 Стратегія управління ризиками»;

«PM-32 визначення ризиків».

Рекомендації з упровадження та підтвердження виконання заходів для ОТ/АСУ ТП

Розробляючи стратегію управління ризиками ОТ, організаціям рекомендовано враховувати:

забезпечення того, що стійкість до ризику середовища ОТ визначається роллю організації в критичній інфраструктурі та аналізі ризиків у певному секторі;

документування сценаріїв збоїв із залученням ІТ-компонентів у середовищі ОТ та їхнього впливу на роботу та безпеку;

встановлення процесів для періодичного оновлення інформації для визначення поточного стану ризику для навколишнього середовища та

координації необхідних коригувань управління ризиками та управлінських засобів контролю.

Загальний ризик також можна зменшити, розглянувши ймовірність і наслідки. Для систем ОТ стратегія управління ризиками повинна враховувати засоби контролю, не пов’язані з безпекою та захистом (наприклад, клапани скидання тиску, ручні клапани), які також можуть допомогти зменшити наслідки відмови.

3.1.5. Управління ризиками ланцюга поставок (ID.SC)

Ланцюжки поставок є багатогранними та побудовані на різноманітних ділових, економічних і технологічних факторах. Організації обирають своїх постачальників, а споживачі обирають свої джерела на основі низки факторів, які варіюються від корпоративних уподобань і існуючих/поточних ділових відносин до більш дискретних міркувань, таких як наявність обмежених джерел постачання або інших унікальних характеристик.

Підкатегорії (результати), які належать до категорії CSF Supply Chain Risk Management, забезпечують основу для розробки процесів і процедур з метою управління ризиками ланцюга поставок. Ці ризики передбачають введення підробок, несанкціоноване виробництво, зловмисних інсайдерів, втручання, крадіжку та вставлення зловмисного програмного та апаратного забезпечення, а також неналежну практику виробництва та розробки в ланцюжку кіберпостачання. Ці ризики необхідно ідентифікувати, оцінити та керувати ними. Категорія CSF також стосується контрактів із постачальниками та сторонніми партнерами, оцінок, а також планування реагування та відновлення.

Крім того, організаціям рекомендовано досліджувати технології SBOM і розподіленої книги (наприклад, блокчейн) для підтримки управління ризиками в ланцюзі поставок. Наприклад, інформація SBOM може ідентифікувати компоненти програмного забезпечення та зв’язки чи залежності від інших компонентів. Наявність цієї інформації може допомогти організації визначити, чи вражений пристрій повідомленими вразливими місцями програмного забезпечення.

Додаткові вказівки щодо ID.SC наведені в НД ТЗІ 3.6-006-21 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних (автоматизованих) систем».

Захід захисту:

«PM-31 План управління ризиком ланцюга постачання».

Рекомендації з упровадження та підтвердження виконання заходів для ОТ/АСУ ТП

Організаціям слід розглянути питання про документування та відстеження серійних номерів, контрольних сум, цифрових

сертифікатів/підписів або інших ідентифікаційних функцій, які можуть дозволити визначити автентичність апаратного, програмного та мікропрограмного забезпечення, наданого постачальником. Організаціям також слід враховувати, чи придбано ОТ безпосередньо у виробника оригінального обладнання або в уповноваженого стороннього дистриб'ютора чи торгового посередника. Постачальники повинні бути оцінені або перевірені, щоб переконатися, що вони продовжують дотримуватись найкращих практик.

Багато компонентів і пристроїв ОТ використовують бібліотеки з відкритим кодом для підтримки своїх функціональних можливостей. Організаціям рекомендовано визначити залежності від відкритого коду для своїх компонентів ОТ і встановити моніторинг інформації з відкритим кодом, такої як вебсайти постачальників або джерела кіберновин, щоб переконатися, що не було розкрито жодних відомих вразливостей або підробок. Крім того, організації можуть розглянути можливість використання визнаного галуззю процесу сертифікації продуктів ОТ для підтримки управління ризиками в ланцюзі поставок.

3.2. Захист (PR)

3.2.1. Керування ідентифікацією та контроль доступу (PR.AC)

Управління ідентифікацією та контроль доступу (PR.AC) визначає результати щодо встановлення та керування механізмами ідентифікації та обліковими даними для користувачів, пристроїв і послуг. Управління ідентифікацією підтримує принцип кібербезпеки, щоб ідентифікувати та авторизувати особу, процес або пристрій перед наданням фізичного або логічного доступу до ресурсів, таких як система, інформація чи місцезнаходження, які однозначно захищаються. Контроль доступу представляє політики, процеси та технології для використання системних ресурсів лише авторизованими користувачами, програмами, процесами чи іншими системами. Контроль PR.AC дозволяє організаціям керувати логічним і фізичним доступом до вимог системи управління ризиками підтримки.

Додаткові вказівки щодо PR.AC наведені в НД ТЗІ 3.6-006-21 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних (автоматизованих) систем».

Заходи захисту:

«AC-1 Політика та процедури управління доступом»;

«AC-2 Управління обліковими записами»;

«AC-3 Забезпечення доступу»;

«AC-5 Розмежування обов'язків»;

«AC-6 Мінімізація повноважень»;

«AC-7 Невдалі спроби входу в систему»;

«AC-8 Попередження про використання системи»;

«AC-9 Сповіщення про попередній вхід (доступ)»;
«AC-10 Управління паралельною сесією»;
«AC-11 Блокування пристрою»;
«AC-12 Припинення сеансу»;
«AC-13 Нагляд та огляд — управління доступом»;
«AC-14 Дозволені дії без ідентифікації або автентифікації»;
«AC-16 Атрибути безпеки та приватності»;
«AC-17 Віддалений доступ»;
«AC-18 Безпроводовий доступ»;
«AC-19 Контроль доступу для мобільних пристроїв»;
«AC-20 Використання зовнішніх систем»;
«AC-21 Розповсюдження інформації»;
«AC-22 Публічно доступний контент»;
«AC-23 Захист від несанкціонованого інтелектуального аналізу даних»;
«AC-24 Рішення щодо управління доступом»;
«AC-25 Диспетчер доступу»;
«IA-1 Політика та процедури ідентифікації та автентифікації»;
«IA-2 Ідентифікація та автентифікація (користувачів організації)»;
«IA-3 Ідентифікація та автентифікація пристроїв»;
«IA-4 Управління ідентифікацією»;
«IA-5 Управління автентифікатором»;
«IA-6 Зворотний зв’язок автентифікатора»;
«IA-7 Автентифікація криптографічного модуля»;
«IA-8 Ідентифікація та автентифікація (неорганізаційні користувачі)»;
«IA-9 Послуги ідентифікації та автентифікації»;
«IA-10 Адаптивна автентифікація»;
«IA-11 Повторна автентифікація»;
«IA-12 Перевірка справжності (ідентичності)».

Рекомендації з упровадження та підтвердження виконання заходів для ОТ/АСУ ТП

Організаціям слід враховувати життєвий цикл для керування обліковими даними ОТ, включаючи видачу, відкликання та оновлення в середовищі ОТ.

Організаціям слід розглянути можливість централізації ідентифікації та автентифікації для користувачів, пристроїв і процесів у середовищах ОТ, щоб покращити/зменшити навантаження на керування обліковими записами та розширити можливості моніторингу. Загальні мережеві технології, такі як Active Directory і протокол LDAP (Lightweight Directory Access Protocol) або подібні технології, можна використовувати для підтримки централізації керування ідентифікацією в різних середовищах. Якщо автентифіковані облікові записи з ІТ-середовища мають доступ у середовищі ОТ, організації повинні зважити підвищений ризик від дозволу та переваги використання централізованих облікових записів.

У ситуаціях, коли ОТ не може підтримувати автентифікацію, або

організація вирішує, що це недоцільно через несприятливий вплив на продуктивність, безпеку чи надійність, організації слід вибрати компенсаційний контрзахід, такий як використання фізичної безпеки (наприклад, доступ до центру керування ключ-картою для авторизованих користувачів), щоб забезпечити еквівалентну можливість безпеки або рівень захисту для ОТ. Ця рекомендація також стосується використання блокування сеансу та завершення сеансу в ОТ.

Унікальним викликом ОТ є необхідність негайного доступу до HMI в екстрених ситуаціях. Час, потрібний для введення облікових даних користувача, може перешкодити відповіді або втручанню оператора, що призведе до негативних наслідків для безпеки, здоров'я чи навколишнього середовища.

3.2.1.1. Логічний контроль доступу (PR.AC-1)

Логічний контроль доступу обмежує логічний доступ до систем, даних і мереж організації. Список управління доступом (Access Control List (ACL)) іноді використовується для підтримки логічного контролю доступу. ACL — одне або більше правил для визначення того, чи має бути наданий або відхилений запит на доступ. Правила використовуються для підтримки принципу найменшої функціональності та контролю доступу до зон обмеженого доступу. Вони зазвичай використовуються з технологіями ізоляції, такими як брандмауери, де ACL може вказувати джерело, призначення та протокол, дозволений через ізолювальний пристрій до або із захищеного сегмента мережі. ACL також може використовуватися для фізичного або логічного доступу до областей або інформації, такої як спільні файли в мережі, бази даних або інші сховища даних і програми.

Інша технологія для підтримки логічного контролю доступу називається керування доступом на основі ролей (Role Based Access Control, RBAC). RBAC — технологія, яка має потенціал для зменшення складності та вартості адміністрування безпеки в мережах із великою кількістю інтелектуальних пристроїв. RBAC побудована на принципі, що працівники змінюють ролі та обов'язки частіше ніж обов'язки в межах ролей та обов'язків. У RBAC адміністрування безпеки спрощено за допомогою ролей, ієрархій і обмежень для організації рівнів доступу користувачів.

Крім того, керування доступом на основі атрибутів (Attribute-Based Access Control, ABAC) — підхід до керування доступом, у якому доступ визначається на основі атрибутів, пов'язаних із суб'єктами (запитувачами) та об'єктами, до яких здійснюється доступ. Кожен об'єкт і суб'єкт мають набір пов'язаних атрибутів, таких як розташування, час створення, права доступу тощо. Доступ до об'єкта авторизується або забороняється залежно від того, чи можна встановити необхідну (наприклад, визначену політикою) кореляцію між атрибути цього об'єкта та суб'єкта запиту.

Персоналу організації може знадобитися підтвердження особи (Personal Identity Verification, PIV), що використовується відповідно до FIPS 201, для

досягнення контролю доступу. Організації можуть також розглянути один або кілька з цих методів, визначаючи, як підтримувати локальні засоби контролю доступу у своєму середовищі.

Додаткові вказівки щодо PR.AC-1 наведені в НД ТЗІ 3.6-006-21 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних (автоматизованих) систем».

Заходи захисту:

«AC-1 Політика та процедури управління доступом»;

«AC-2 Управління обліковими записами»;

«AC-3 Забезпечення доступу»;

«AC-7 Невдалі спроби входу в систему»;

«AC-16 Атрибути безпеки та приватності»;

«AC-17 Віддалений доступ»;

«AC-18 Безпроводовий доступ»;

«AC-19 Контроль доступу для мобільних пристроїв»;

«AC-20 Використання зовнішніх систем»;

«IA-1 Політика та процедури ідентифікації та автентифікації»;

«IA-2 Ідентифікація та автентифікація (користувачів організації)»;

«IA-3 Ідентифікація та автентифікація пристроїв»;

«IA-4 Управління ідентифікацією»;

«IA-8 Ідентифікація та автентифікація (неорганізаційні користувачі)»;

«IA-9 Послуги ідентифікації та автентифікації»;

«IA-10 Адаптивна автентифікація»;

«IA-11 Повторна автентифікація»;

«IA-12 Перевірка справжності (ідентичності)».

Рекомендації з упровадження та підтвердження виконання заходів для ОТ/АСУ ТП

Організаціям рекомендовано враховувати таке:

деякі засоби логічного контролю доступу, такі як RBAC, підтримують принцип найменших привілеїв і розподілу обов’язків, забезпечуючи уніфіковані засоби керування доступом до пристроїв ОТ, одночасно знижуючи витрати на підтримку рівнів доступу до окремих пристроїв і мінімізуючи помилки. Ці логічні елементи керування доступом також можуть обмежувати привілеї користувача ОТ лише тими, які необхідні для виконання роботи кожної особи (тобто налаштування кожної ролі на основі принципу найменших привілеїв). Рівень доступу може мати кілька форм, включаючи перегляд, використання та зміну певних даних ОТ або функцій пристрою;

упровадити рішення, які забезпечують керування обліковими даними, автентифікацію та авторизацію, а також технічні можливості моніторингу використання системи. Ці технології можуть допомогти в управлінні ризиками, пов’язаними з пристроями та протоколами ОТ, надаючи безпечну платформу, яка дозволяє авторизованому персоналу отримати доступ до пристроїв ОТ;

системи контролю доступу, які перевіряють особу, процес або пристрій перед наданням доступу, повинні бути розроблені таким чином, щоб мінімізувати затримки або затримки в обробці доступу до системи ОТ або команд;

упровадження високонадійних систем, які не заважають виконувати звичайні чи надзвичайні обов'язки персоналу ОТ. Рішення мають бути розроблені таким чином, щоб зменшити вплив визначення особи та авторизації на операції та безпеку ОТ.

Для підтримки контролю доступу організація не обмежується одним підходом до контролю доступу. У деяких випадках застосування різних методів контролю доступу до різних зон на основі критичності, безпеки та експлуатаційних вимог є ефективнішим. Наприклад, ACL на брандмауерах мережевої зони в поєднанні з RBAC на інженерних робочих станціях і серверах, а також ABAC, інтегрований у фізичну безпеку чутливих зон можуть досягти вимог щодо контролю доступу на основі ризиків для організації.

3.2.1.2. Контроль фізичного доступу (PR.AC-2)

Контроль фізичної безпеки – будь-які фізичні заходи, які обмежують фізичний доступ до активів. Ці заходи застосовуються для запобігання багатьом типам небажаних ефектів, включаючи несанкціонований фізичний доступ до конфіденційних місць; несанкціоноване впровадження нових систем, інфраструктури, комунікаційних інтерфейсів або змінних носіїв; несанкціоноване порушення фізичного процесу. Контроль фізичного доступу містить засоби керування фізичним доступом і моніторингу, ведення журналів і обробки відвідувачів.

Розгортання засобів контролю фізичної безпеки часто залежить від вимог щодо навколишнього середовища, безпеки, регулятивних, правових та інших вимог, які мають бути визначені та розглянуті в конкретному середовищі. Контроль фізичної безпеки може бути широко застосованим або може бути специфічним для певних активів.

Початкові рівні контролю фізичного доступу часто визначаються на основі ризику доступу до загального об'єкта, а не лише до компонентів ОТ.

Додаткові вказівки щодо PR.AC-2 наведені в НД ТЗІ 3.6-006-21 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних (автоматизованих) систем».

Заходи захисту:

«PE-1 Політика та процедури фізичного захисту та захисту робочого середовища»;

«PE-2 Авторизація фізичного доступу»;

«PE-3 Керування фізичним доступом»;

«PE-4 Контроль доступу до джерел і ліній електроживлення»;

«PE-5 Контроль доступу до пристроїв виведення інформації»;

«PE-6 Моніторинг фізичного доступу»;

«PE-7 Контроль відвідувачів»;
«PE-8 реєстр доступу відвідувачів»;
«PE-9 Енергетичне обладнання та кабелі»;
«PE-10 Аварійне відключення»;
«PE-11 Аварійне енергозабезпечення»;
«PE-12 Аварійне освітлення»;
«PE-13 Протипожежний захист»;
«PE-14 Контроль температури та вологості»;
«PE-15 Захист від пошкодження водою»;
«PE-16 Доставка та видалення»;
«PE-17 Альтернативне робоче місце»;
«PE-18 Розташування компонентів системи»;
«PE-19 Витік інформації»;
«PE-20 Моніторинг та відстеження активів»;
«PE-21 Захист від електромагнітного імпульсу»;
«PE-22 Маркування компонентів».

Рекомендації з упровадження та підтвердження виконання заходів для ОТ/АСУ ТП

Фізичний захист кіберкомпонентів і даних, пов'язаних з ОТ, має розглядатися як частина загальної безпеки середовищ ОТ. Безпека на багатьох об'єктах ОТ тісно пов'язана з експлуатаційною безпекою. Основна мета полягає в тому, щоб уберегти персонал від небезпечних ситуацій, не заважаючи йому виконувати свою роботу або виконувати процедури в надзвичайних ситуаціях.

Контроль фізичного доступу часто застосовується до середовища ОТ як компенсаційний контроль, коли застарілі системи не підтримують сучасні ІТ-логічні засоби контролю доступу (наприклад, актив може бути заблокований у шафі, коли порт USB або кнопку живлення неможливо логічно вимкнути). Впроваджуючи ці засоби пом'якшення, організації повинні враховувати, чи може захищений компонент ОТ бути скомпрометований за допомогою безпроводового або мережевого з'єднання, яке може обійти засоби контролю фізичної безпеки.

Рішення з глибоким захистом для фізичної безпеки має враховувати такі атрибути:

захист фізичних місць розташування. Класичні аспекти фізичної безпеки зазвичай включають архітектуру багаторівневих заходів безпеки, що створюють декілька фізичних бар'єрів навколо будівель, об'єктів, приміщень, обладнання чи інших інформаційних активів. Контроль фізичної безпеки повинен бути реалізований для захисту фізичних місць і може включати огорожі, протитранспортні канави, земляні насипи, стіни, посилені барикади, ворота, замки дверей і шаф, охорону або інші заходи;

контроль фізичного доступу. Шафи з обладнанням слід закривати на замок, якщо вони не потрібні для роботи чи безпеки, а електропроводка має бути акуратною та всередині шаф або під підлогою. Крім того, слід подумати

про те, щоб все обчислювальне та мережеве обладнання залишалося в безпечних місцях. Ключі активів ОТ, як-от ПЛК і системи безпеки, повинні постійно перебувати в положенні «Виконати», якщо вони не активно програмуються;

системи моніторингу доступу. Системи моніторингу доступу передбачають електронні можливості спостереження, такі як фото- та відеокамери, датчики та системи ідентифікації (наприклад, зчитувачі бейджів, біометричні сканери, електронні клавіатури). Такі пристрої зазвичай не перешкоджають доступу до певного місця, а зберігають і записують або фізичну присутність, або відсутність фізичної присутності осіб, транспортних засобів, тварин чи інших фізичних осіб. Необхідно забезпечити належне освітлення залежно від типу розгорнутого пристрою контролю доступу. Ці системи також іноді можуть попереджати або ініціювати дії при виявленні несанкціонованого доступу;

відстеження людей і активів. Розташування людей і транспортних засобів на об’єкті може бути важливим з міркувань безпеки, і це стає все більш важливим з міркувань безпеки. Технології локації активів можна використовувати для відстеження переміщень людей і транспортних засобів, щоб переконатися, що вони залишаються в дозволених зонах, ідентифікувати персонал, який потребує допомоги, і підтримувати реагування на надзвичайні ситуації.

Нижче наведено додаткові аспекти фізичної безпеки:

портативні пристрої. Організації повинні застосовувати процес перевірки, який передбачає сканування пристроїв (наприклад, ноутбуків, USB-накопичувачів тощо) на наявність шкідливого коду, перш ніж дозволити підключення пристрою до пристроїв ОТ або мереж;

прокладання кабелів. Неекранована кручена пара зв’язкового кабелю, хоча і прийнятна для офісного середовища, може не підходити для деяких ОТ через його чутливість до перешкод від магнітних полів, радіохвиль, екстремальних температур, вологи, пилу та вібрації. Організаціям слід розглянути можливість використання альтернативних кабелів або екранування, які забезпечують відповідний захист від загроз навколишнього середовища. Крім того, організації повинні розглянути кольорове кодування кабелів, з’єднувачів і каналів додатково до маркування, щоб чітко розмежувати сегменти мережі ОТ та ІТ і зменшити ризик потенційного перехресного з’єднання;

центри управління/пункти управління. Рекомендується забезпечити фізичну безпеку для центрів управління/диспетчерських, щоб зменшити потенціал багатьох загроз, у тому числі несанкціонований доступ. Доступ до цих зон повинен бути обмежений уповноваженим персоналом через підвищену ймовірність виявлення чутливих серверів, мережевих компонентів, систем керування та консолей для підтримки постійного моніторингу та швидкого реагування. Отримання фізичного доступу до диспетчерської або компонентів системи ОТ часто передбачає отримання логічного доступу до системи або компонентів системи. У надзвичайних

випадках організаціям може знадобитися розробка вибухозахищених центрів управління/пунктів управління або забезпечення диспетчерського центру/пункту управління за межами організації, щоб можна було підтримувати контроль, якщо основний центр управління/пункт управління стане непридатним для проживання**.**

3.2.1.3. Сегментація та ізоляція мережі (PR.AC-5)

Загальна архітектура для підтримки підходу до кібербезпеки поглибленого захисту передбачає використання сегментації мережі або зонування для організації пристроїв за розташуванням або функціями. Сегментація мережі зазвичай реалізується фізично за допомогою різних мережевих комутаторів або логічно за допомогою конфігурацій віртуальної локальної мережі (Virtual Local Area Network, VLAN). При належному налаштуванні сегментація мережі підтримує застосування політик безпеки та сегментованого трафіка на рівні Ethernet і полегшує ізоляцію мережі.

Для ізоляції мережі організації зазвичай використовують свої відображені потоки даних для ідентифікації необхідних комунікацій між сегментами. Пристрої ізоляції мережі, такі як шлюзи (включно з односпрямованими шлюзами або діодами даних) і брандмауери, потім налаштовуються для забезпечення цих обмежень зв’язку, відстежуючи весь трафік передачі даних та дозволяючи лише зв’язок між сегментами, які були явно авторизовані.

Додаткові вказівки щодо PR.AC-5 наведені в НД ТЗІ 3.6-006-21 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних (автоматизованих) систем».

Заходи захисту:

«AC-1 Політика та процедури управління доступом»;

«AC-2 Управління обліковими записами»;

«AC-3 Забезпечення доступу»;

«AC-17 Віддалений доступ»;

«AC-18 Безпроводовий доступ»;

«AC-19 Контроль доступу для мобільних пристроїв»;

«IA-4 Управління ідентифікацією»;

«IA-9 Послуги ідентифікації та автентифікації»;

«IA-10 Адаптивна автентифікація».

Рекомендації з упровадження та підтвердження виконання заходів для ОТ/АСУ ТП

Використання сегментації та ізоляції мережі має підтримувати глибоку архітектуру захисту кібербезпеки ОТ організації.

Хоча VLAN можуть бути економічно ефективним рішенням для сегментації мережі ОТ, організаціям слід розглянути можливість використання фізично окремих комутаторів для сегментації пристроїв високої

критичності, таких як підтримка систем безпеки.

Під час налаштування пристроїв ізоляції мережі організаціям може бути важко визначити, який мережевий трафік необхідний для належної роботи ОТ. У таких ситуаціях організації можуть тимчасово дозволити та записувати весь зв'язок між сегментами мережі. Це може надати доступні для перегляду журнали для ідентифікації та документування авторизованого зв'язку для впровадження правил ізоляції мережі. Крім того, ця діяльність також може виявити раніше невідому або незадокументовану комунікацію, яку організація має перевірити.

Організаціям також слід розглянути, чи нормативні вимоги передбачають тип пристроїв ізоляції мережі, необхідних для середовищ ОТ або окремих сегментів мережі. Якщо організації вирішують використовувати брандмауери для підтримки ізоляції мережі, слід розглянути сучасні брандмауери, такі як пристрої перевірки стану та глибокої перевірки пакетів, а також пристрої, спеціально розроблені для підтримки середовищ ОТ. Організаціям слід за можливості застосовувати політику заборони всім (дозвіл за винятком), а також переглядати розгортання брандмауера Центру захисту національної інфраструктури (CPNI) для SCADA та мереж керування процесами (Посібник із належної практики), щоб допомогти в упровадженні брандмауера.

Організаціям слід пам'ятати, що пристрої ізоляції мережі можуть не захистити від усіх мережевих ризиків. Наприклад, ізоляція мережі не зменшує ризики, пов'язані з боковим переміщенням у сегменті мережі, наприклад, розповсюдження «хробака» чи іншого шкідливого коду. Крім того, деякі IT-протоколи та багато промислових комунікаційних протоколів мають відомі вразливості безпеки, які можна використати через пристрої ізоляції мережі. Організаціям слід розглянути питання про обмеження потоку незахищених протоколів, обмеження потоку інформації, щоб він був односпрямованим, і використання безпечних і автентифікованих протоколів для підтримки обміну інформацією між середовищем ОТ та іншими сегментами мережі.

3.2.1.4. Автентифікація користувача, пристрою та активів (PR.AC-7)

Автентифікація за допомогою фізичного токена. Основною вразливістю, яку усуває автентифікація фізичного токена, є легке дублювання секретного коду або передача його іншим. Це усуває надто поширений сценарій, коли пароль до «захищеної» системи знаходиться на стіні поруч із ПК або станцією оператора організації. Токен безпеки не можна скопіювати без спеціального доступу до обладнання та витратних матеріалів.

Друга перевага полягає в тому, що секрет у фізичному токені може бути дуже великим, фізично безпечним і генеруватися випадковим чином. Оскільки він вбудований у метал або кремній, він не має таких ризиків, як паролі, введені вручну. Якщо токен безпеки втрачено або вкрадено, власник токена знає про відсутність токена та може повідомити персонал служби безпеки, щоб вимкнути доступ. Традиційні паролі можуть бути втрачені або викрадені без

попередження, що робить облікові дані більш вразливими для використання.

Поширені форми фізичної/жетонної автентифікації включають:

традиційний фізичний замок і ключі;

картки безпеки (наприклад, магнітні, смарт-чіп, оптичне кодування);

радіочастотні пристрої у формі карток або міток;

ключі з безпечними ключами шифрування, які підключаються до USB, послідовних або паралельних портів комп'ютерів;

генератори одноразових кодів автентифікації.

Для однофакторної автентифікації за допомогою фізичного токена найбільшою слабкістю є те, що фізичне утримання токена означає надання доступу (наприклад, кожен, хто знайшов набір втрачених ключів, тепер має доступ до всього, що він відкрив). Автентифікація за допомогою фізичного маркера є більш безпечною в поєднанні з другою формою автентифікації, такою як PIN-код, який використовується разом із маркером.

Якщо контроль доступу на основі токенів використовує криптографічну перевірку, в ОТ/АСУТП на об'єктах, віднесених згідно із законодавством до критичної інфраструктури, криптографічні засоби захисту мають впроваджуватися з урахуванням вимог Технічного регламенту засобів криптографічного захисту інформації, затвердженого постановою Кабінету Міністрів України від 21 жовтня 2020 року № 991.

Біометрична автентифікація покращує лише програмні рішення, такі як автентифікація за паролем, пропонуючи додатковий фактор автентифікації та позбавляючи людей необхідності запам'ятовувати складні секрети. Крім того, оскільки біометричні характеристики є унікальними для конкретної особи, біометрична автентифікація вирішує проблеми втрачених або вкрадених фізичних жетонів і смарт-карт. Біометричні пристрої роблять корисну вторинну перевірку порівняно з іншими формами автентифікації, які можна втратити або позичити. Використання біометричної автентифікації в поєднанні з контролем доступу на основі токенів або хронометражами співробітників, що працюють за бейджами, підвищує рівень безпеки.

Помічені проблеми з біометричною автентифікацією такі:

як відрізнити справжній предмет від підробки (наприклад, як відрізнити справжній людський палець від силіконово-гумового зліпка або справжній людський голос від записаного);

генерування помилок типу I та типу II (імовірність відхилення дійсного біометричного зображення та ймовірність прийняття недійсного біометричного зображення відповідно). Пристрої біометричної автентифікації мають бути налаштовані на найнижчий перехід між цими двома ймовірностями, відомий як частота помилок перетину;

робота з такими факторами навколишнього середовища, як температура та вологість, до яких чутливі деякі біометричні пристрої;

розгляд промислових застосувань, де працівники можуть носити захисні окуляри та/або рукавички; промислові хімікати, можуть вплинути на біометричні сканери;

перенавчання біометричних сканерів, які час від часу «дрейфують».

Біометричні характеристики людини також можуть змінюватися з часом, що вимагає періодичного перенавчання сканера;

вимагання особистої технічної підтримки та перевірки для навчання пристрою, на відміну від пароля, який можна надати по телефону, або картки доступу, яку може роздати адміністратор;

відмова в необхідному доступі до системи ОТ через тимчасову нездатність сенсорного пристрою розпізнати законного користувача;

соціальна прийнятність. Користувачі вважають деякі пристрої біометричної автентифікації більш прийнятними, ніж інші. Наприклад, сканування сітківки ока можна вважати дуже низьким за шкалою прийнятності, тоді як сканери відбитків пальців можна вважати високим за шкалою прийнятності. Користувачі пристроїв біометричної автентифікації повинні враховувати соціальну прийнятність для цільової групи, вибираючи серед технологій біометричної автентифікації.

Рекомендації з упровадження та підтвердження виконання заходів для ОТ/АСУ ТП

Хоча біометрія може надати цінний механізм автентифікації, організаціям може знадобитися ретельна оцінка цієї технології для використання в промислових програмах. Фізичні та екологічні проблеми в середовищах ОТ можуть знизити надійність авторизованої біометричної автентифікації. Організаціям може знадобитися координація дій з постачальниками чи виробниками систем щодо їхніх конкретних фізичних властивостей і властивостей навколишнього середовища та вимог до біометричної автентифікації.

Автентифікація через смарт-картку**.** Смарт-карти бувають різних форм-факторів, від USB-пристроїв до вбудованих чіпів на картках розміром приблизно з кредитні картки, які можна друкувати та тиснути. Смарт-картки можна налаштувати, індивідуалізувати та видавати власними силами або передати постачальникам послуг, які можуть випускати сотні тисяч карток на день. Смарт-карти покращують лише програмні рішення, такі як автентифікація за паролем, пропонуючи додатковий фактор автентифікації та усуваючи людський фактор при запам’ятовуванні складних секретів завдяки:

ізоляції важливих для безпеки обчислень, пов’язаних із автентифікацією, цифровими підписами та обміном ключами, від інших частин системи, яким не потрібно знати;

забезпеченню перенесення облікових даних та іншої приватної інформації між комп’ютерними системами;

наданню захищеного від злому сховища для захисту особистих ключів та інших форм особистої інформації.

Більшість проблем, пов’язаних із використанням смарт-карт, пов’язані з матеріально-технічним забезпеченням і зосереджені на випуску карток, зокрема для заміни втрачених або вкрадених карток.

Рекомендації з упровадження та підтвердження виконання заходів для ОТ/АСУ ТП

Хоча смарт-карти пропонують корисну функціональність, у контексті ОТ їх реалізація повинна враховувати загальний контекст безпеки середовища ОТ. Необхідна ідентифікація осіб, видача карток, відкликання у разі підозри на компрометацію та призначення авторизацій автентифікованим особам, що є серйозною початковою та постійною проблемою. У деяких випадках корпоративні ІТ-ресурси або інші ресурси можуть бути доступні для допомоги в розгортанні смарт-карт і необхідної інфраструктури відкритих ключів. Організаціям також слід враховувати вплив на операційні можливості ОТ, якщо для підтримки технології смарт-карт потрібна залежність від ІТ-систем і служб.

Крім того, якщо смарт-картки впроваджуються в налаштуваннях ОТ, організації повинні розглянути положення щодо управління втраченими або пошкодженими картками, витрати на включення та підтримку відповідної системи контролю доступу, а також процес керування розповсюдженням і пошуком карток. Ці процедури повинні брати до уваги можливість надання тимчасового доступу персоналу ОТ, щоб запобігти порушенням роботи або безпеки.

Загальний підхід має базуватися на стандартизації смарт-карток PIV, що дозволяє організаціям використовувати той самий механізм облікових даних у кількох програмах з одним-трьома факторами автентифікації (лише картка, картка+PIN, картка+PIN+біометричний), залежно від рівня ризику ресурсу, що захищається.

Багатофакторна автентифікація**.** Організаціям слід враховувати, що існує кілька можливих факторів для визначення автентичності особи, пристрою або системи. Коли використовуються два або більше факторів, процес відомий як багатофакторна автентифікація (MFA). Загалом чим більше факторів використовується в процесі автентифікації, тим надійнішим є процес. Наприклад, автентифікація може ґрунтуватися на чомусь відомому (наприклад, PIN-коді або паролі), на чомусь наявному (наприклад, ключі, ключі, смарт-карті) або на вашій біологічній характеристиці (наприклад, відбиток пальця, підпис на сітківці ока).

Рекомендації з упровадження та підтвердження виконання заходів для ОТ/АСУ ТП

Організаціям рекомендовано розглянути, чи потрібна MFA для захисту середовищ ОТ повністю чи частково. MFA є прийнятою найкращою практикою для віддаленого доступу до програм ОТ. Визначаючи розміщення та використання MFA в середовищі ОТ, організаціям може знадобитися розгляд різних сценаріїв автентифікації, оскільки деякі компоненти ОТ підтримують лише один фактор або не підтримують автентифікацію. Організації можуть розглянути можливість коригування вимог до облікових даних на основі типу доступу або інших факторів, що пом’якшують середовище. Наприклад, для віддаленого доступу до середовища ОТ може знадобитися MFA, у той час як для локального доступу можуть знадобитися

лише ідентифікатор користувача та пароль через інші пом’якшуючі фактори, такі як контроль фізичного доступу перед отриманням фізичного доступу до області, де можуть використовуватися ідентифікатор користувача та пароль.

Парольна автентифікація. Хоча схеми автентифікації за паролем є найпоширенішою та найпростішою формою автентифікації, численні вразливості пов’язані з використанням і довірою до автентифікації лише за паролем. Наприклад, системи часто постачаються з паролями за замовчуванням, які можна легко вгадати, виявити або дослідити. Ще одна слабка сторона — легкість стороннього підслуховування. Паролі, введені з клавіатури, можуть візуально спостерігатися іншими або записуватися за допомогою реєстраторів натискань клавіш.

Деякі мережеві служби та протоколи передають паролі як відкритий текст (незашифрований), що дозволяє будь-якому інструменту захоплення мережі розкривати паролі. Крім того, паролі можуть бути загальними та нечасто змінюватися. Використання спільних облікових даних, у тому числі спільних паролів, обмежує можливість точно ідентифікувати окрему особу, процес або пристрій, які отримали доступ до захищеного ресурсу. Поглиблений захист часто використовується, щоб запобігти тому, щоб автентифікація пароля була єдиним контролем для запобігання неавторизованій зміні.

Рекомендації з упровадження та підтвердження виконання заходів для ОТ/АСУ ТП

Багато систем ОТ не пропонують механізмів відновлення пароля, тому безпечна та надійна обробка паролів має вирішальне значення для підтримки безперервної роботи.

Організаціям рекомендується змінити пароль за замовчуванням на обладнанні ОТ, щоб зловмисникам було важче вгадати пароль. Після зміни пароль потрібно зробити доступним для тих, хто повинен його знати. Організації можуть розглянути можливість використання інструменту керування паролями, який є безпечним і доступним для тих, хто повинен його знати.

Деякі ОС ускладнюють встановлення безпечних паролів, оскільки розмір пароля менший за поточні стандарти паролів, а система дозволяє лише групові паролі на кожному рівні доступу, а не окремі паролі. Деякі промислові та Інтернет-протоколи передають паролі у вигляді відкритого тексту, що робить їх чутливими до перехоплення. Коли цієї практики неможливо уникнути, важливо, щоб користувачі мали різні (і непов’язані) паролі для використання із зашифрованими та незашифрованими протоколами.

Крім того, можуть знадобитися особливі підходи під час застосування політик на основі автентифікації пароля для входу в середовищі ОТ. Без списку виключень на основі ідентифікації машини (ID) вхід без оператора організації може призвести до скасування таких політик, як тайм-аут автоматичного виходу із системи та заміна пароля адміністратора, що може завдати шкоди роботі системи ОТ.

Загальні рекомендації та зауваження щодо використання паролів:

змінити всі паролі за замовчуванням у компонентах ОТ;

паролі повинні мати належну довжину, надійність і складність, збалансовану між безпекою та простотою доступу в межах можливостей програмного забезпечення та основної ОС;

паролі не можна знайти в словнику або містити передбачувані послідовності цифр або літер;

слід обережно використовувати паролі на спеціалізованих пристроях ОТ, таких як консолі керування критичними процесами. Використання паролів на цих консолях може спричинити потенційні проблеми з безпекою, якщо оператори заблоковано або затримано доступ під час критичних подій;

слід розглянути фізичну або мережеву ізоляцію для пристроїв, де захист паролем не рекомендується;

копії спільних або головних паролів повинні зберігатися в безпечному місці з обмеженим доступом, до якого також можна отримати доступ у надзвичайних ситуаціях. Організаціям також може знадобитися розглянути процедури періодичної зміни паролів, якщо пароль зламано або особа з доступом залишає організацію;

паролі привілейованих (адміністративних) облікових записів вимагають додаткового захисту, наприклад, посилених вимог до пароля, більш частої зміни та додаткових фізичних засобів захисту;

паролі не слід надсилати через будь-яку мережу, якщо вони не захищені певною формою шифрування, схваленою FIPS, або спеціальним криптографічним хешем, розробленим для запобігання повторним атакам.

3.2.2. Обізнаність і навчання (PR.AT)

Категорія «Обізнаність і навчання» містить політику та процедури для забезпечення того, щоб усі користувачі отримали базову обізнаність із кібербезпеки та навчання.

Додаткові вказівки щодо PR.AT наведені в НД ТЗІ 3.6-006-21 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних (автоматизованих) систем».

Заходи захисту:

«АТ-1 Політика та процедури підвищення обізнаності та навчання»;

«АТ-2 Навчання з підвищення обізнаності»;

«АТ-3 Рольове навчання»;

«АТ-4 Навчальні записи».

Рекомендації з упровадження та підтвердження виконання заходів для ОТ/АСУ ТП

Персонал організації має пройти спеціальну обізнаність щодо безпеки ОТ та навчання для середовища та конкретних застосувань. Крім того, організації ідентифікують, документують і навчають весь персонал, який

виконує важливі функції та обов'язки ОТ. Обізнаність і навчання повинні охоплювати фізичний процес, що контролюється, а також систему ОТ.

Поінформованість про безпеку є важливою частиною запобігання інцидентам ОТ, особливо коли йдеться про загрози соціальної інженерії. Соціальна інженерія – техніка, яка використовується для маніпулювання людьми, щоб вони надали особисту інформацію, наприклад, паролі. Потім ця інформація може бути використана для компрометації безпечних систем.

Програми підвищення обізнаності та навчання щодо безпеки ОТ можуть містити: базове розуміння методів соціальної інженерії та виявлення аномальної поведінки в середовищі ОТ, інструкції щодо того, коли та як підключати та від'єднувати середовище ОТ від зовнішніх доменів безпеки, складність паролів та вимоги до керування та практики звітності. Увесь персонал, відповідальний за ОТ, має пройти навчання, але навчання може бути адаптоване відповідно до ролей і обов'язків. Ролі, які слід розглянути в програмі навчання, можуть містить ролі керівників вищої ланки, користувачів привілейованих облікових записів, сторонніх постачальників, персоналу фізичної безпеки, інженерів з контролю, операторів і супроводжувачів.

3.2.3. Безпека даних (PR.DS)

Забезпечення безпеки даних передбачає захист конфіденційності, цілісності та доступності даних під час зберігання та передачі, захист активів після видалення та запобігання витоку даних.

Використання криптографії може підтримувати вимоги безпеки даних. Шифрування, цифрові підписи, хешування та інші криптографічні функції доступні для запобігання несанкціонованому доступу або модифікації даних у стані споживання та передачі. При виборі криптографії організаціям слід використовувати сертифіковану криптографічну систему. Крім того, криптографічне обладнання має бути захищене від фізичного втручання та неконтрольованих електронних з'єднань.

В ОТ/АСУТП на об'єктах, віднесених згідно із законодавством до критичної інфраструктури, криптографічні засоби захисту мають впроваджуватися з урахуванням вимог Технічного регламенту засобів криптографічного захисту інформації, затвердженого постановою Кабінету Міністрів України від 21 жовтня 2020 року № 991.

Додаткові вказівки щодо PR.DS наведені в НД ТЗІ 3.6-006-21 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних (автоматизованих) систем».

Заходи захисту:

«SC-8 Конфіденційність та цілісність передачі»;

«SC-11 Довірений канал зв'язку»;

«SC-12 Встановлення та управління криптографічними ключами»;

«SC-13 Криптографічний захист»;

«SC-16 Передача атрибутів безпеки та приватності»;

«SC-17 Сертифікати інфраструктури відкритих ключів»;
«SC-28 Захист інформації в стані спокою».

Рекомендації з упровадження та підтвердження виконання заходів для ОТ/АСУ ТП

Слід визначити критичні типи файлів і дані, які потрібно захистити (як фізичні, так і електронні) у стані спокою. Це може містити особисту інформацію та конфіденційну, конфіденційну інформацію або інформацію, що є комерційною таємницею (наприклад, програмний код ПЛК, програми роботів, файли автоматизованого креслення/автоматизованого виробництва, посібники з експлуатації та документація, електричні схеми, схеми мереж, історичні дані виробництва). Організаціям слід розглянути можливість централізації критичних даних у безпечних місцях зберігання.

Коли дані ОТ зберігаються в хмарі або на серверах постачальників, організаціям слід розглянути можливість проведення аналізу ризиків, щоб визначити, як дані захищені постачальником послуг і чи потрібно вживати додаткових контрзаходів для управління ризиками до прийнятного рівня.

Інформація надходить із домену безпеки ОТ в інші домени безпеки, а з'єднання між доменами безпеки відстежуються. Для обмеження потоку інформації можна використовувати такі технології, як діоди даних, брандмауери та ACL. Приклади критичних інтерфейсів і взаємозв'язків можуть включати інтерфейси між ІТ і ОТ, ОТ і зовнішніми галузевими партнерами або ОТ і сторонніми постачальниками підтримки.

Щоб захистити дані на компонентах системи після завершення терміну служби, слід запровадити програму утилізації активів, включаючи можливість видалення, дезінфекції або іншого знищення критичних даних і носіїв перед утилізацією. Програма утилізації активів має містити будь-які знімні носії та мобільні пристрої, а також традиційне апаратне забезпечення ОТ.

Запровадження криптографічного захисту.

Критичні дані ОТ повинні бути захищені під час передачі, особливо через сторонні сегменти мережі та інші ненадійні або вразливі мережеві шляхи (наприклад, мобільний зв'язок, безпроводовий зв'язок, мережа Інтернет тощо). Спочатку слід визначити, які дані є критичними, а потім запровадити криптографічні механізми (наприклад, шифрування), щоб запобігти несанкціонованому доступу або модифікації системних даних і записів аудиту. Шифрування забезпечує механізм для забезпечення конфіденційності та цілісності даних, що передаються.

Застосунки ОТ часто зосереджені на забезпеченні доступності даних. Перш ніж розгортати шифрування в ОТ, слід переконатися, що конфіденційність або цілісність є актуальними для конкретного виду інформаційного обміну. Використання шифрування в середовищі ОТ може викликати затримку зв'язку через додатковий час і обчислювальні ресурси, необхідні для шифрування, дешифрування та автентифікації кожного повідомлення. Слід враховувати погіршення продуктивності кінцевого (термінального) обладнання або системи, викликане шифруванням або будь-

яким іншим методом безпеки. Перед розгортанням шифрування в середовищі ОТ слід протестувати рішення, щоб визначити, чи прийнятна затримка для програми. Щоб зменшити затримку шифрування, можна застосувати шифрування на рівні 2 OSI, а не на рівні 3.

Крім того, хоча шифрування забезпечує конфіденційність між пристроями шифрування/дешифрування, інструменти виявлення аномалій, що підтримують середовища ОТ, можуть не мати змоги зчитувати зашифровані дані. Тому шифрування слід ретельно планувати та впроваджувати для управління операційними ризиками.

Організаціям також слід враховувати, що криптографія може викликати проблеми з керуванням ключами. Правильні політики безпеки вимагають ключових процесів управління, які можуть ускладнюватися зі збільшенням географічного розміру ОТ. Оскільки відвідування сайтів для зміни або керування ключами може бути дорогим і повільним, організаціям слід розглянути, чи може криптографічний захист із віддаленим керуванням ключами бути корисним, наприклад, коли захищені одиниці настільки численні або географічно розосереджені, що керування ключами є складним або дорогим.

Для ОТ шифрування може бути застосовано як частину комплексної політики безпеки. Криптографічний ключ має бути достатньо довгим, щоб його вгадування або визначення шляхом аналізу потребувало більше зусиль, часу та витрат ніж вартість захищеного активу.

3.2.4. Процеси та процедури захисту інформації (PR.IP)

Політики, процеси та процедури слід підтримувати та використовувати для керування захистом інформаційних (автоматизованих) систем та активів. Контрзаходи та результати мають бути на місці для керування змінами конфігурації протягом життєвого циклу компонента та системи. Слід підтримувати резервні копії, а плани реагування та відновлення мають бути підготовлені та перевірені. Необхідно розробити та впровадити план управління вразливістю протягом усього життєвого циклу компонентів.

3.2.4.1. Найменша функціональність (PR.IP-1)

Принцип найменшої функціональності передбачає конфігурацію систем для надання лише основних функцій і послуг. Деякі функції та послуги, які зазвичай надаються за замовчуванням, можуть бути непотрібними для підтримки основних місій, функцій або операцій організації. Ці функції включають мережеві порти та протоколи, програмне забезпечення та служби.

Додаткові вказівки щодо PR.IP-1 наведені в НД ТЗІ 3.6-006-21 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних (автоматизованих) систем».

Заходи захисту:

«СМ-1 Політика та процедури управління конфігурацією»;
«СМ-2 Базова конфігурація»;
«СМ-6 Налаштування конфігурації»;
«СМ-7 Мінімально необхідна функціональність»;
«СМ-9 План управління конфігурацією»;
«СМ-10 Обмеження використання програмного забезпечення».

Рекомендації з упровадження та підтвердження виконання заходів для ОТ/АСУ ТП

Системи та пристрої в середовищі ОТ містять багато функцій і служб, які можуть бути непотрібними для їх належної роботи, деякі з яких можуть бути ввімкнені за замовчуванням і без відома організації. Будь-які функції чи служби, не потрібні для належної роботи, слід вимкнути, щоб зменшити вплив.

Слід бути обережним, вимикаючи ці функції та служби, оскільки ненавмисні впливи можуть виникнути, якщо критично важливу функцію чи послугу несвідомо вимкнено (наприклад, вимкнення всіх зовнішніх зв'язків із ПЛК може також вимкнути можливість зв'язуватися з пов'язаними HMI). Пристрої повинні пройти ретельне тестування перед розгортанням в мережі ОТ.

3.2.4.2. Контроль змін конфігурації (Керування конфігурацією) (PR.IP-3)

Управління конфігурацією допомагає гарантувати, що системи розгортаються та підтримуються в безпечному та узгодженому стані, дозволяючи організаціям зменшити ризики від збоїв через проблеми конфігурації та порушення безпеки завдяки покращеній видимості та відстеженню змін у системі. Крім того, керування конфігураціями може виявити неправильні конфігурації до того, як вони негативно вплинуть на продуктивність, безпеку чи захист. Інструменти керування конфігурацією дозволяють власнику активів установлювати та підтримувати цілісність апаратних і програмних компонентів системи, контролюючи процеси ініціалізації, зміни, моніторингу та аудиту конфігурацій компонентів протягом усього життєвого циклу системи.

Додаткові вказівки щодо PR.IP-3 наведені в НД ТЗІ 3.6-006-21 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних (автоматизованих) систем».

Заходи захисту:
«СМ-1 Політика та процедури управління конфігурацією»;
«СМ-2 Базова конфігурація»;
«СМ-3 Управління змінами конфігурації»;
«СМ-6 Налаштування конфігурації»;
«СМ-9 План управління конфігурацією»;
«СМ-10 Обмеження використання програмного забезпечення».

Рекомендації з упровадження та підтвердження виконання заходів для ОТ/АСУ ТП

Організаціям рекомендовано задокументувати затверджену базову конфігурацію для своїх пристроїв ОТ. Крім того, організаціям рекомендовано повинні встановити підхід життєвого циклу розробки системи (SDLC) для документування, тестування та затвердження змін перед розгортанням у середовищі ОТ.

Деякі організації можуть вести журнали або інші подібні методи для документування змін компонентів ОТ. Організаціям слід розглянути можливість централізації відстеження та документування змін у середовищі ОТ, щоб покращити видимість і забезпечити належне тестування та схвалення системних змін. Такий процес може дозволити організаціям запобігти випадковій зміні конфігурації або виявити навмисну зміну конфігурації компонентів до несхвалених або неперевірених версій.

У деяких випадках може бути доречним використання автоматизованих інструментів керування конфігурацією. Необхідно запровадити процеси для перевірки конфігурацій перед розгортанням. Багато змін в ОТ можна вносити лише під час планових простоїв на технічне обслуговування, щоб мінімізувати вплив. Розглядаючи інструменти автоматизованого керування конфігурацією, організації повинні враховувати потенційний вплив на систему ОТ. У деяких випадках ці інструменти передають мережею виробничої системи через численні типи даних і потенційно великі обсяги даних. Крім того, деякі інструменти також можуть потенційно впливати на роботу системи ОТ, намагаючись змінити конфігурацію пристрою або маніпулюючи активними файлами.

3.2.4.3. Резервне копіювання (PR.IP-4)

Створення, підтримка та тестування резервних копій є критично важливим результатом для процесу відновлення, якщо трапляється кіберінцидент або інцидент з надійністю.

Додаткові вказівки щодо PR.IP-4 наведені в НД ТЗІ 3.6-006-21 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних (автоматизованих) систем».

Захід захисту: «CP-9 Резервне копіювання».

Рекомендації з упровадження та підтвердження виконання заходів для ОТ/АСУ ТП

Слід розробити список усіх збережених резервних копій, у тому числі інсталяційний носій, ліцензійні ключі та інформацію про конфігурацію. Необхідно вжити додаткових заходів, щоб забезпечити доступність резервних копій, а саме необхідно:

перевірити резервні копії на надійність і цілісність (якщо це технічно можливо);

створити резервне копіювання на місці, яке буде доступним для всього персоналу, якому може знадобитися доступ під час відновлення;

встановити альтернативне вторинне місце зберігання для додаткових копій резервних копій, щоб переконатися, що той самий інцидент, який порушує первинні дані, не зможе змінити або знищити резервну копію (наприклад, зберігати логіку ПЛК і конфігураційні файли в іншому, географічно різному місці, яке не може бути знищено (ураган, лісова пожежа, торнадо, які можуть знищити ПЛК);

включити тестування процесу відновлення з резервних копій даних як частину тестування плану дій у непередбачених ситуаціях.

переконатися, що процедури резервного копіювання включені в процеси керування конфігурацією або змінами;

виконати безпечне резервне копіювання відповідно до вимог контролю доступу;

слідкувати за умовами середовища, де зберігаються резервні носії.

3.2.4.4. Фізичне робоче середовище (PR.IP-5)

Управління фізичним робочим середовищем містить елементи керування захистом від надзвичайних ситуацій, такі як аварійне відключення системи, резервне живлення та освітлення, контроль температури та вологості, а також захист від пожежі та пошкодження водою. Організації повинні розробити політику та процедури, щоб забезпечити виконання екологічних вимог до активів.

Рекомендації з упровадження та підтвердження виконання заходів для ОТ/АСУ ТП

Під час визначення потенційних контрзаходів для захисту фізичного робочого середовища організаціям варто враховувати такі фактори:

фактори навколишнього середовища можуть бути важливими. Наприклад, якщо ділянка запилена, системи слід розмістити у фільтрованому середовищі. Це особливо важливо, якщо пил, імовірно, є електропровідним або магнітним, як у випадку з підприємствами, які обробляють вугілля або залізо. Якщо вібрація є ймовірною проблемою, системи слід монтувати на гумові втулки, щоб запобігти збоям диска та проблемам підключення проводів. Крім того, середовища, де містяться системи та носії (наприклад, резервні стрічки, дискети), повинні мати стабільну температуру та вологість. Тривога для системи ОТ повинна бути ввімкнена, коли перевищено технічні характеристики середовища, такі як температура або вологість;

системи контролю навколишнього середовища. Системи HVAC для диспетчерських повинні підтримувати персонал ОТ під час нормальної роботи та аварійних ситуацій, які можуть включати викид токсичних речовин. Оцінка ризику повинна враховувати ризик роботи системи HVAC (наприклад,

повітрозабірників) у зайнятому укритті під час викиду токсичних речовин, а також продовження роботи під час відключення електроенергії (наприклад, використання джерела безперебійного живлення в критичних середовищах);

протипожежні системи повинні бути ретельно спроектовані, щоб уникнути заподіяння більше шкоди ніж користі (наприклад, щоб уникнути змішування води з несумісними продуктами). Системи опалення, вентиляції, вентиляції та кондиціонування повітря та протипожежні системи відіграють суттєво збільшену роль у забезпеченні безпеки, що виникає внаслідок взаємозалежності контролю процесу та безпеки. Наприклад, протипожежні системи та системи опалення, вентиляції та кондиціонування, які підтримують комп'ютери промислового керування, потребують захисту від кіберінцидентів;

потужність. Надійне живлення для ОТ є важливим, тому для критично важливих систем слід передбачити ДБЖ. Якщо на місці є аварійний генератор, час роботи батареї ДБЖ може становити лише кілька секунд. Однак, якщо сайт покладається на зовнішнє джерело живлення, час автономної роботи ДБЖ може становити години. Його розмір повинен бути принаймні таким, щоб систему можна було безпечно вимкнути.

3.2.4.5. Плани реагування та відновлення (PR.IP-9) і тестування плану реагування та відновлення (PR.IP-10)

Організаціям рекомендовано розробляти та підтримувати плани реагування, у тому числі реагування на інциденти та забезпечення безперервності бізнесу. Плани реагування слід порівнювати з послугою, що надається, а не лише з системою, яка була скомпрометована. Організаціям слід розглянути систематичний підхід до планування реагування, як-от процес, описаний у посібниках реагування на інциденти кібербезпеки та вразливості CISA. Загальні етапи планування передбачають підготовку, виявлення та аналіз, стримування, відновлення, діяльність після інциденту, комунікацію та координацію. Організаціям також варто запровадити регулярний перегляд та оновлення своїх планів реагування.

Плани реагування мають бути задокументовані в паперовій формі або в офлайн-системі (тобто без розриву), яка не може бути скомпрометована під час кібератаки. Окремі особи повинні пройти навчання щодо того, де знайти план реагування, а також дій, яких необхідно вжити в рамках реагування на інцидент. Крім того, під час підготовки плану реагування на інцидент необхідно отримати інформацію від різних зацікавлених сторін, включаючи експлуатацію, техніку, IT, постачальників системної підтримки, керівництво, організовану працю, юристів і безпеки. Ці зацікавлені сторони також повинні переглянути та затвердити план.

Планування безперервності бізнесу вирішує загальне питання підтримки або відновлення виробництва у разі перерви. Збій може включати типові проміжки часу в дні, тижні або місяці для відновлення після стихійного лиха або хвилини чи години для відновлення після зараження зловмисним програмним забезпеченням або механічної чи електричної несправності.

План безперервності діяльності (Business Continuity Plan - BCP) для інцидентів кібербезпеки має широко охоплювати довгострокові збої, включаючи аварійне відновлення, і короткострокові збої, що вимагають оперативного відновлення. При цьому важливе поєднання заходів кіберзахисту із заходами фізичної безпеки, що передбачає ідентифікацію критично важливого обладнання та відповідні контрзаходи для запобігання інциденту.

Перш ніж створювати BCP для вирішення можливих збоїв, важливо визначити цілі відновлення для різних залучених систем і підсистем на основі типових потреб бізнесу. Існує два типи цілей: відновлення системи та відновлення даних. Відновлення системи передбачає відновлення каналів зв'язку та можливостей обробки, і це зазвичай визначається в терміні цільового часу відновлення (recovery time objective - RTO). Керівництво має визначити прийнятний RTO, а технічний персонал має працювати над досягненням цієї мети. Відновлення даних передбачає відновлення даних, що описують виробництво або умови продукту в минулому і зазвичай визначається в як цільова точка відновлення (recovery point objective - RPO). Це визначається як період часу між аварією та відновленням, протягом якого можна допускати відсутність даних. RTO та RPO можуть виправдати інвестиції в системи резервування, якщо цілі відновлення не можуть бути досягнуті іншими засобами.

Після визначення цілей відновлення слід створити список потенційних перерв, а також розробити й описати процедуру відновлення. Потім створюється план дій у непередбачених ситуаціях для різноманітних потенційних перебоїв. План дій у надзвичайних ситуаціях слід переглянути разом із керівниками, щоб переконатися, що вартість виконання плану дій у надзвичайних ситуаціях затверджена. Для багатьох невеликих перебоїв запас критичних запчастин виявиться достатнім для досягнення цілей відновлення. Для більш масштабного відновлення, ймовірно, будуть використані відносини з постачальниками. Для всіх типів відновлення резервне копіювання є критичним.

План аварійного відновлення (Disaster recovery plan - DRP) — задокументований процес або набір процедур, що містить вичерпний опис дій з відновлення, які необхідно виконати до, під час і після катастрофи. DRP зазвичай документується як в електронному, так і в паперовому вигляді, щоб гарантувати, що він буде легкодоступним під час будь-якого типу катастрофи. Катастрофа може бути природною, екологічною або спричиненою людьми, навмисно чи ненавмисно. Організації повинні розробляти, підтримувати та перевіряти плани аварійного відновлення для своїх середовищ, щоб мінімізувати вплив подій шляхом скорочення часу, необхідного для відновлення можливостей.

Організації можуть уже мати деякі плани реагування на надзвичайні ситуації, і їм слід розглянути можливість використання існуючих планів під час розробки плану реагування на події, пов'язані з кібербезпекою.

Додаткові вказівки щодо DRP наведені в НД ТЗІ 3.6-006-21 «Порядок

вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних (автоматизованих) систем».

Заходи захисту:

«CP-1 Політика та процедури планування безперервної роботи»;

«CP-2 План забезпечення безперервної роботи та відновлення функціонування»;

«CP-4 Тестування плану забезпечення безперервної роботи та відновлення функціонування»;

«CP-10 Відновлення та відтворення системи»;

«IR-1 Політика та процедури реагування на інциденти»;

«IR-2 Навчання реагування на інциденти»;

«IR-3 Перевірка реагувань на інциденти»;

«IR-4 Обробка інциденту»;

«IR-5 Моніторинг інциденту»;

«IR-6 Звітність про інциденти»;

«IR-7 Підтримка реагування на інциденти»;

«IR-8 План реагування на інциденти»;

«IR-9 Реагування на витік інформації»;

«IR-10 Інтегрована команда аналізу інформаційної безпеки».

Рекомендації з упровадження та підтвердження виконання заходів для ОТ/АСУ ТП

План реагування на інцидент може містити такі пункти:

ідентифікація та класифікація інцидентів. Слід ідентифікувати та класифікувати різні типи інцидентів ОТ на основі потенційного впливу, щоб можна було сформулювати правильну відповідь на кожен потенційний інцидент;

дії відповіді. У разі інциденту можна вжити кілька заходів. Вони варіюються від нічого не робити до повного завершення роботи системи, що може призвести до зупинки фізичного процесу. Реакція буде залежати від типу інциденту та його впливу на систему ОТ і фізичний процес, що контролюється. Необхідно підготувати письмовий план реагування на кожен тип інциденту. Це дозволить керуватися планом у моменти, коли може виникнути плутанина або стрес через інцидент. Цей план має передбачати покрокові дії, які мають виконуватися різними організаціями. Якщо існують вимоги до звітності, їх слід задокументувати разом із контактною інформацією та форматом звітності, щоб уникнути плутанини.

Дії реагування повинні передбачати кроки для виявлення та аналізу; стримування, ліквідації та відновлення, а також діяльність після інциденту. Деякі міркування щодо ОТ можуть передбачати:

визначення пріоритету: або якомога швидше повернутися до нормальної роботи, або провести розслідування та зберегти дані судової експертизи;

спілкування з групою реагування на інциденти;

відключення заражених систем від мережі;

фізичну ізоляцію операційно незалежних мереж (наприклад, організація від контролю або контролю від безпеки);

перехід на ручні операції;

ресурси для підтримки додаткових операцій для ручної перевірки даних;

повідомлення керівництва, зв'язків із громадськістю та/або зовнішніх компаній і агентств, якщо це необхідно.

У разі виявлення інциденту організаціям рекомендовано провести цілеспрямовану оцінку ризику в середовищі ОТ, щоб оцінити ефект атаки і варіантів реагування. Наприклад, одним із можливих варіантів відповіді є фізична ізоляція атакованої системи. Однак це може мати негативний вплив на ОТ і може бути неможливим без впливу на експлуатаційні характеристики або безпеку. Цілеспрямована оцінка ризику повинна використовуватися для визначення відповідних дій.

У плані також повинні бути вказані вимоги щодо своєчасної заміни компонентів у разі виникнення аварійної ситуації. Якщо можливо, запасні частини для критичних компонентів, які важко отримати, слід зберігати в інвентарі.

Організації рекомендовано мати засоби для визначення пріоритетності діяльності з відновлення. Це визначення пріоритетів може використовувати існуючу документацію, таку як оцінка ризиків або процедури запуску. Як приклад, у центрі уваги може бути відновлення систем, що підтримують критично важливі утиліти, до систем, що підтримують виробництво, на основі порядку запуску дій.

Тестування процедур плану відновлення для компонентів ОТ може бути складним через експлуатаційні вимоги та вимоги безпеки. Організаціям може знадобитися визначити, чи можливі «стендові випробування» або інші офлайн-тестування для підтвердження процедур відновлення компонентів ОТ. Організації повинні принаймні перевірити цілісність резервних копій, якщо неможливо виконати тест на повне відновлення.

3.2.5. Технічне обслуговування (PR.MA)

Результати, які підпадають під категорію технічного обслуговування CSF, дають підстави для надання вказівок щодо виконання планового та профілактичного технічного обслуговування компонентів інформаційної (автоматизованої) системи. Це передбачає в себе використання засобів обслуговування (як локальних, так і дистанційних) і управління персоналом з обслуговування.

Додаткові вказівки щодо PR.MA наведені в НД ТЗІ 3.6-006-21 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних (автоматизованих) систем».

Заходи захисту:

«МА-1 Політика та процедури технічного обслуговування»;

«МА-2 Контрольоване обслуговування»;

«МА-3 Інструменти для обслуговування»;
«МА-4 Віддалене обслуговування»;
«МА-5 Технічний персонал»;
«МА-6 Своєчасне обслуговування».

Рекомендації з упровадження та підтвердження виконання заходів для ОТ/АСУ ТП

Рішення для відстеження технічного обслуговування дозволяють організації планувати, відстежувати, авторизувати, контролювати та перевіряти заходи з технічного обслуговування та ремонту ОТ, забезпечуючи належне документування журналів технічного обслуговування або внесених змін. Документування цих подій забезпечує контрольний слід, який може допомогти при розв'язанні проблем, пов'язаних із кібербезпекою, реагуванні та відновленні.

Відстеження технічного обслуговування також може забезпечити видимість планового технічного обслуговування пристроїв ОТ і допомогти прийняти інформовані рішення щодо завершення терміну служби.

Програмне забезпечення, що використовується для технічного обслуговування ОТ, має бути схвалено та контрольовано організацією. Схвалене програмне забезпечення слід отримати безпосередньо від постачальників і перевірити його автентичність (наприклад, перевіркою сертифікатів або порівнянням хешів інсталяторів).

Будь-яке технічне обслуговування пристрою ОТ може ненавмисно змінити його конфігурацію, що призведе до збільшення поверхні атаки. Загартований стан пристрою ОТ слід підтримувати незалежно від проведеного технічного обслуговування. Конфігурацію пристрою слід перевірити після технічного обслуговування та виправлення програмного забезпечення, оскільки деякі функції могли бути випадково повторно ввімкнені або встановлені нові функції. Рекомендації та інші супровідні документи слід отримати від постачальника пристрою, щоб керувати та інформувати про заходи з обслуговування.

Обмеження використання певних пристроїв лише для технічного обслуговування може допомогти зменшити ймовірність зламу пристрою через вплив зовнішніх мереж, неавторизованих користувачів або крадіжки. Пристрої для обслуговування, які залишаються безпечними в середовищі ОТ, зменшують їх вплив. Слід обмежити або звести до мінімуму використання пристроїв обслуговування поза межами середовища ОТ або підключення пристроїв до мереж, що не належать до ОТ.

Будь-який пристрій, підключений до системи ОТ, слід від'єднати після завершення технічного обслуговування, а будь-які тимчасові з'єднання слід видалити.

Слід добре розуміти роботу, можливості та особливості пристроїв, що використовуються для технічного обслуговування. Пристрої можуть містити безпроводові радіостанції та інші комунікаційні пристрої, які можуть бути вразливими до атак із сторонніх каналів або можуть дозволяти одночасне

з’єднання між мережами (тобто дводомні). Щоб зрозуміти ці можливості, необхідно ретельно переглянути документацію постачальника.

3.2.6. Захисна технологія (PR.PT)

Технічні механізми допомагають організаціям захистити пристрої та інформацію в їхньому середовищі. Ці технології самі по собі можуть бути недостатніми для підтримання можливостей безпеки, оскільки загрози розвиваються та змінюються. Організації повинні керувати технічними рішеннями, що забезпечують захист організаційних активів, відповідно до політик, процедур і угод.

3.2.6.1. Ведення журналів реєстрації подій (PR.PT-1)

Ведення журналів дозволяє організації фіксувати події, що відбуваються в її системах і мережах. Події можуть генеруватися різними системами, включаючи ОС, робочі станції, сервери, мережеві пристрої, програмне забезпечення для кібербезпеки та програми.

Додаткові вказівки щодо PR.PT-1 наведені в НД ТЗІ 3.6-006-21 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних (автоматизованих) систем».

Заходи захисту:

«AU-1 Політика та процедури аудиту та підзвітності»;
«AU-2 Події аудиту»;
«AU-3 Зміст записів аудиту»;
«AU-4 Місткість сховища записів аудиту»;
«AU-5 Реагування на відмови обробки даних аудиту»;
«AU-6 Огляд, аналіз і звітність аудиту»;
«AU-7 Скорочення записів аудиту та формування звіту»;
«AU-8 Позначка часу»;
«AU-9 Захист інформації аудиту»;
«AU-10 Неспростовність»;
«AU-11 Збереження записів аудиту»;
«AU-12 Генерація даних аудиту»;
«AU-13 Моніторинг розкриття інформації»;
«AU-14 Аудит сесії»;
«AU-15 Альтернативна можливість аудиту»;
«AU-16 Міжорганізаційний аудит».

Рекомендації з упровадження та підтвердження виконання заходів для ОТ/АСУ ТП

Запис подій до журналу має вирішальне значення для підтримки обізнаності про ситуацію в системі ОТ. Типові типи подій включають функції обслуговування (наприклад, контроль доступу, зміни конфігурації, резервне

копіювання та відновлення), функції ОС і події програми (тобто процесу). Конкретні типи подій, доступних для реєстрації, відрізнятимуться між пристроями ОТ і їх слід вибирати на основі можливостей пристрою та бажаних подій, які потрібно зафіксувати.

Кожен запис журналу має містити ідентифікатор пристрою, який згенерував подію, мітку часу події та ідентифікацію облікового запису користувача або системи, який згенерував подію. Кожен запис у журналі має містити інформацію про те, де сталася подія, тип події, коли подія сталася, джерело події, ідентифікаційні дані будь-яких користувачів або системних облікових записів, пов'язаних із подією, і результат події.

Кореляція подій між кількома пристроями АСУ ТП може бути складною, якщо мітки часу подій, створені пристроями, не надсилалися спільним джерелом часу. Внутрішні годинники кожного пристрою мають бути синхронізовані з основними годинниками для підтримки кореляції подій між пристроями. Записи журналу також мають створювати узгоджений формат позначки часу (наприклад, формат часового поясу, формат рядка, літній час).

Функції збору та пересилання подій можуть впливати на продуктивність пристрою ОТ. Розмір журналу може швидко зростати залежно від частоти подій, що реєструються, що призводить до збільшення використання простору. Дисковий простір і пам'ять обмежені на більшості пристроїв ОТ, тому необхідно забезпечити достатнє сховище локально або віддалено, щоб зменшити ймовірність перевищення ємності пристрою, що в кінцевому підсумку може призвести до втрати можливості реєстрації. Слід розглянути можливість перенесення журналів із пристроїв ОТ до іншого сховища.

3.2.7. Захист медіа (PR.PT-2)

Змінний носій захищено, а використання обмежено відповідно до політики. Це передбачає маркування носіїв для розповсюдження та вимог до поводження, а також зберігання, транспортування, санітарну обробку, знищення та утилізацію носіїв.

Додаткові вказівки щодо PR.PT-2 наведені в НД ТЗІ 3.6-006-21 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних (автоматизованих) систем».

Заходи захисту:

«MP-1 Політика та процедури щодо захисту носіїв інформації»;

«MP-2 Доступ до носіїв інформації»;

«MP-3 Маркування носіїв інформації»;

«MP-4 Зберігання носіїв інформації»;

«MP-5 Транспортування носіїв інформації»;

«MP-6 Знищення інформації на носіях інформації»;

«MP-7 Використання носіїв інформації»;

«MP-8 Зниження категорії безпеки носіїв інформації».

Рекомендації з упровадження та підтвердження виконання заходів для ОТ/АСУ ТП

Варто розробити процеси та процедури поводження з медіаактивами та дотримуватися їх. Медіаактиви включають знімні носії та пристрої, такі як дискети, компакт-диски, DVD-диски, SD-карти та USB-накопичувачі, а також друковані звіти та документи. Контроль фізичної безпеки має відповідати конкретним вимогам щодо безпечного та надійного обслуговування цих активів і надавати конкретні вказівки щодо транспортування, обробки та видалення чи знищення цих активів. Вимоги безпеки можуть містити безпечне зберігання від втрати, пожежі, крадіжки, ненавмисного розповсюдження або пошкодження навколишнього середовища.

Пристрої ОТ слід захищати від неправомірного використання медіа. Використання будь-яких неавторизованих знімних носіїв або пристроїв на будь-якому вузлі, який є частиною ОТ або підключеним до нього, не має бути дозволено. Рішення можуть бути процедурними або технічними, щоб запобігти впровадженню зловмисного програмного забезпечення або випадковій втраті чи крадіжці даних.

Фізичний захист медіа або шифрування даних на носії має вирішальне значення для захисту середовища ОТ. Наприклад, якщо зловмисник отримує доступ до медіа, що містить дані ОТ, він може надати цінну інформацію для початку атаки.

3.2.8. Безпека персоналу

Кібербезпека повинна бути введена в практику роботи з персоналом організації, щоб зменшити ризик людської помилки, крадіжки, шахрайства або іншого навмисного чи ненавмисного зловживання інформаційними системами.

Додаткові вказівки щодо безпеки персоналу наведені в НД ТЗІ 3.6-006-21 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних (автоматизованих) систем».

Заходи захисту:

«PS-1 Політика та процедури кадрової безпеки»;

«PS-2 Визначення посадового ризику»;

«PS-3 Перевірка персоналу»;

«PS-4 Звільнення персоналу»;

«PS-5 Переведення персоналу»;

«PS-6 Угоди про доступ»;

«PS-7 Безпека зовнішнього персоналу»;

«PS-8 Кадрові санкції».

Рекомендації з упровадження та підтвердження виконання заходів для ОТ/АСУ ТП

Слід розробити загальну програму безпеки персоналу організації, яка міститиме політику, визначення ризиків посади, перевірку персоналу, звільнення та переміщення, угоди про доступ, а також ролі та відповідальність третіх сторін. Персонал ОТ повинен підтримувати зв’язок із відділом кадрів, ІТ та відділом фізичної безпеки, якщо це необхідно, щоб забезпечити виконання вимог щодо безпеки персоналу.

Організаціям рекомендовано розглянути можливість укладення угоди про доступ і форми запиту для керування доступом (фізичним і/або логічним) до обладнання ОТ. Організаціям також рекомендовано перевіряти персонал, призначений на критичні посади, що контролюють і обслуговують ОТ.

Крім того, слід розробити навчальні програми, щоб гарантувати, що кожен працівник отримав навчання, відповідне та необхідне для його функціональних обов’язків. Співробітники повинні продемонструвати компетентність при виконанні своїх робочих функцій, щоб зберегти фізичний і логічний доступ до ОТ.

Організаціям слід розглянути можливість прийняття структури, такої як Національна ініціатива з освіти з кібербезпеки (NICE), для навчання персоналу ОТ.

3.2.9. Безпроводовий зв'язок

Безпроводовий зв'язок використовує радіочастоту (РЧ) для підтримки передачі даних. Це може включати зв’язок через локальну мережу Wireless Fidelity (WiFi) на основі протоколів IEEE 802.11, а також може включати мобільний або інший радіозв’язок. Зв'язок на основі РЧ забезпечує підвищену гнучкість порівняно з традиційними можливостями фізичного (проводового) зв'язку. Однак радіозв’язок також більш сприйнятливий до перешкод і може дозволяти підслуховувати неавторизований персонал.

У разі використання у безпроводових мережах передачі даних засобів криптографічного захисту інформації в ОТ/АСУТП на об’єктах, віднесених згідно із законодавством до критичної інфраструктури, криптографічні засоби захисту мають впроваджуватися з урахуванням вимог Технічного регламенту засобів криптографічного захисту інформації, затвердженого постановою Кабінету Міністрів України від 21 жовтня 2020 року № 991.

Додаткові вказівки щодо безпроводового зв’язку наведені в НД ТЗІ 3.6-006-21 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних (автоматизованих) систем».

Заходи захисту:

«SC-40 Захист безпроводового з’єднання»;

«AC-18 Безпроводовий доступ»;

«AC-19 Контроль доступу для мобільних пристроїв».

Рекомендації з упровадження та підтвердження виконання заходів для ОТ/АСУ ТП

Використання тимчасового або постійного безпроводового зв’язку в ОТ є рішенням, що базується на оцінці ризику, яке приймається організацією. Як правило, пристрої, що використовують безпроводовий зв’язок, слід розміщувати в окремому сегменті мережі та розгортати лише там, де залишкові ризики для здоров’я, безпеки, навколишнього середовища та фінансових наслідків є низькими.

Перед встановленням слід провести обстеження безпроводової мережі, щоб визначити розташування антени та потужність сигналу, щоб забезпечити належне покриття та мінімізувати вплив факторів зовнішнього середовища та прослуховування на безпроводову мережу перешкод. Організаціям слід враховувати, що зловмисники зазвичай використовують спрямовані антени, щоб розширити ефективний діапазон безпроводової мережі за стандартний діапазон.

Організації можуть вибрати впровадження безпроводової mesh-мережі, щоб підвищити стійкість або усунути області зі слабким сигналом. Mesh-мережі можуть забезпечити відмовостійкість за допомогою вибору альтернативного маршруту та превентивного перемикання мережі. Організаціям також слід враховувати вплив на продуктивність і безпеку, пов’язаний із використанням сітчастих мереж. Наприклад, під час роумінгу між точками доступу пристрої можуть тимчасово втрачати зв’язок. Для роумінгу також можуть знадобитися інші засоби захисту, щоб скоротити час переходу. Організаціям потрібно буде знайти відповідний баланс між функціональними можливостями та кібербезпекою, щоб досягти стійкості до ризику.

Безпроводові локальні мережі:

зв’язок безпроводового пристрою має бути зашифрованим. Шифрування не повинно погіршувати продуктивність роботи кінцевого (термінального) обладнання. Слід розглянути шифрування на рівні 2 OSI, а не на рівні 3, щоб зменшити затримку шифрування. Слід також розглянути використання апаратних прискорювачів для виконання криптографічних функцій;

безпроводові точки доступу повинні створювати незалежні сегменти мережі (не розширювати існуючий сегмент) і використовуватися в поєднанні з пристроєм захисту кордонів для обмеження та контролю зв’язку;

точки безпроводового доступу мають бути налаштовані так, щоб вони мали унікальний ідентифікатор набору послуг (SSID) і принаймні вмикали фільтрацію адреси керування доступом до медіа (MAC);

для безпроводових пристроїв може знадобитися інший контроль безпеки, тому їх слід зонувати відповідно;

якщо пристрої будуть використовуватися для безпроводової мобільності, слід розглянути адаптивний протокол маршрутизації. Час конвергенції мережі має бути якомога швидшим, забезпечуючи швидке відновлення мережі у разі збою або втрати живлення.

Безпроводові польові мережі:

Під час впровадження безпроводової польової мережі слід враховувати такі функції безпеки:

вибір стандартного непатентованого протоколу (наприклад, IEEE 802.15.x);

забезпечення шифрування між польовими інструментами та безпроводовими точками доступу;

додавання пристроїв до білого списку в диспетчері безпроводових пристроїв, щоб несанкціоновані пристрої не могли підключитися;

реалізація відповідних складних паролів і ключів приєднання.

Більшість безпроводових польових мереж за своєю суттю менш надійні ніж проводові аналоги через їх сприйнятливість до перешкод сигналу, обмеження відстані та вимоги прямої видимості. Варто працювати з постачальником системи, щоб розробити безпроводову мережу, яка підходить для програми.

3.2.10. Віддалений доступ

Під час віддаленого доступу до систем або даних слід запровадити засоби безпеки, щоб запобігти несанкціонованому доступу до мереж, систем і даних організації. Віртуальна приватна мережа (VPN) — набір технологій і протоколів, призначених для підтримки безпечного віддаленого доступу до мережевих середовищ. VPN може забезпечити як надійну автентифікацію, так і шифрування для захисту даних зв’язку шляхом створення приватної мережі, яка працює як накладення на загальнодоступну інфраструктуру. Найпоширенішими типами технологій VPN, які реалізуються сьогодні, є:

захищений Інтернет-протокол (IPsec). IPsec підтримує два режими шифрування: транспортний і тунельний. Транспортний режим шифрує лише частину даних (корисне навантаження) кожного пакета, залишаючи заголовок пакета недоторканим. Більш безпечний режим тунелювання додає новий заголовок до кожного пакета та шифрує оригінальний заголовок і корисне навантаження. На стороні приймача IPsec 3008-сумісний пристрій розшифровує кожен пакет;

безпека транспортного рівня (TLS). Іноді його називають застарілою термінологією Secure Sockets Layer (SSL). TLS забезпечує безпечний канал між двома машинами, який шифрує вміст кожного пакета. TLS найчастіше розпізнається як захист HTTP-трафіка. Ця реалізація протоколу відома як HTTP Secure (HTTPS). Однак TLS не обмежується трафіком HTTP, його можна використовувати для захисту багатьох програм прикладного рівня;

безпечна оболонка (SSH). SSH — командний інтерфейс і протокол для безпечного отримання доступу до віддаленого комп’ютера. Він широко використовується мережевими адміністраторами для віддаленого керування серверами на базі Linux. SSH є безпечною альтернативою програмі Telnet. SSH включено в більшість дистрибутивів UNIX і зазвичай він додається до інших платформ через сторонній пакет.

В ОТ/АСУТП на об’єктах, віднесених згідно із законодавством до

критичної інфраструктури, криптографічні засоби захисту мають впроваджуватися з урахуванням вимог Технічного регламенту засобів криптографічного захисту інформації, затвердженого постановою Кабінету Міністрів України від 21 жовтня 2020 року № 991.

Додаткові вказівки щодо віддаленого доступу наведені в НД ТЗІ 3.6-006-21 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних (автоматизованих) систем».

Заходи захисту:

«AC-17 Віддалений доступ»;

«MA-4 Віддалене обслуговування».

Рекомендації з упровадження та підтвердження виконання заходів для ОТ/АСУ ТП

Багато архітектур безпеки ОТ розроблено з декількома рівнями, як, наприклад, архітектура Purdue. Це може значно обмежити доступ, що може звести до мінімуму випадкові або несанкціоновані збої в роботі. Необхідно розробити та повідомити організації процес запиту та включення віддаленого доступу. Віддалений доступ має надаватися лише за виправданих умов і обмежуватися лише тим, що необхідно для задоволення бізнес-потреб. Віддалений доступ не повинен обходити або скасовувати засоби захисту.

У критичних ситуаціях або коли потрібна підтримка постачальника може знадобитися тимчасовий віддалений доступ для виконання технічного обслуговування. У таких випадках все одно слід дотримуватися процедур, щоб забезпечити використання безпечних з’єднань.

Існує кілька різних методів реалізації тимчасового віддаленого доступу, зокрема такі:

користувачі/протоколи (наприклад, RDP, SSH), тимчасово дозволені через ОТ/корпоративний брандмауер;

технології спільного використання екрана;

модеми;

VPN.

Незалежно від технології, організації повинні враховувати таке:

упровадження унікальних імен користувачів і складних паролів;

видалення, вимкнення або зміна будь-яких облікових даних за замовчуванням;

оновлення будь-якого ПЗ/прошивки до останніх версій;

видалення доступу, коли він більше не потрібен. Слід розглянути можливість упровадження автоматичних таймерів для скасування доступу або керування процесами змін для підтвердження скасування доступу вручну;

моніторинг віддаленої діяльності;

оперативний персонал обізнаний про заплановану віддалену діяльність у середовищі ОТ;

ініціювання підключення із середовища ОТ;

маркування пристроїв віддаленого підключення, щоб операції могли

швидко від’єднатися у разі несанкціонованого використання.

Dial-Up-модеми

Якщо в середовищах ОТ використовуються модеми комутованого доступу, варто розглянути можливість використання систем зворотного виклику. Це гарантує, що номеронабирач є авторизованим користувачем, оскільки модем встановлює робоче з’єднання на основі інформації номеронабирача та номера зворотного виклику, що зберігається в затвердженому ОТ списку авторизованих користувачів.

Якщо це можливо, відключайте модеми, коли вони не використовуються, або подумайте про автоматизацію цього процесу відключення, дозволивши модемам відключатися після того, як вони були увімкнені протягом певного часу. Слід зазначити, що інколи підключення через модем є частиною угоди про надання послуг юридичної підтримки з постачальником (наприклад, цілодобова підтримка з часом відповіді 15 хвилин). Персонал повинен знати, що відключення/видалення модемів може вимагати перегляду контрактів.

VPN

Пристрої VPN, які використовуються для захисту систем ОТ, слід ретельно протестувати, щоб переконатися, що технологія VPN сумісна з додатком і що впровадження пристроїв VPN не впливає негативно на характеристики мережевого трафіка.

Технологію VPN також можна застосовувати між сегментами мережі. Наприклад, на віддаленому сайті може бути пристрій захисту кордонів, який використовує VPN для встановлення безпечного тунелю через ненадійну мережу (наприклад, Інтернет) до пристрою з підтримкою VPN у головному центрі керування в іншому місці.

3.2.11. Усунення недоліків і керування виправленнями

Систематичний підхід до керування та використання програмних виправлень може допомогти організаціям покращити загальну безпеку своїх систем економічно ефективним способом. Організації, які активно керують та використовують програмні виправлення, можуть зменшити ймовірність того, що вразливі місця в їхніх системах можуть бути використані; крім того, вони можуть заощадити час і гроші, які можуть бути витрачені на реагування на інциденти, пов’язані з вразливістю.

Додаткові вказівки щодо усунення недоліків та керування виправленнями наведені в НД ТЗІ 3.6-006-21 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних (автоматизованих) систем».

Заходи захисту:

«CA-5 План усунення недоліків та контрольні показники»;

«CA-7 Безперервний моніторинг»;

«SI-2 Виправлення дефектів».

Рекомендації з упровадження та підтвердження виконання заходів для ОТ/АСУ ТП

Застосовуючи патчі до компонентів ОС, слід бути дуже обережними. Патчі необхідно перевірити належним чином (наприклад, офлайн-тестування системи), щоб визначити прийнятність будь-яких впливів на продуктивність. Рекомендується регресійне тестування. Нерідко трапляються випадки, коли патчі негативно впливають на інше програмне забезпечення. Виправлення може усунути вразливість, але також може створити більший ризик з точки зору виробництва чи безпеки. Виправлення вразливості також може змінити спосіб роботи ОС або програми з керуючими програмами, внаслідок чого керуюча програма втрачає частину своєї функціональності. Багато систем ОТ використовують старіші версії ОС, які більше не підтримуються постачальником, а отже, патчі можуть бути недоступними.

Організації повинні впроваджувати систематичний, підзвітний і задокументований процес керування виправленнями ОТ для керування вразливістю. Процес керування виправленнями має містити вказівки щодо того, як відстежувати наявність виправлень, коли застосовувати виправлення, як тестувати виправлення (наприклад, у постачальників або в автономних системах) і як вибрати компенсаційні елементи керування для обмеження впливу вразливої системи під час встановлення виправлень.

Багато вразливостей ОТ публікуються в CISA як рекомендації; однак не всі постачальники повідомляють CISA про відомі вразливості. Організації часто можуть бути в курсі вразливостей, підписавшись на сповіщення від постачальників на додаток до сповіщень і порад CISA. Приватні компанії з кібербезпеки також пропонують послуги, щоб допомогти організаціям бути в курсі відомих вразливостей у їхньому середовищі ОТ. Організація несе відповідальність за те, щоб залишатися в курсі своїх вразливостей ОТ і визначати, коли слід застосовувати виправлення, як частину свого задокументованого процесу керування виправленнями.

Коли та як розгортати виправлення, повинен визначити досвідчений персонал ОТ. Слід розглянути можливість відокремлення автоматизованого процесу для керування виправленнями ОТ від автоматизованого процесу для додатків, які не належать до ОТ. Виправлення слід розгортати під час запланованих відключень ОТ.

Організації можуть дотримуватися галузевих інструкцій щодо керування виправленнями. В іншому випадку вони можуть розробити процедури керування виправленнями на основі існуючих стандартів, таких як NIST SP 800-40 Rev. 4; NERC CIP-007, Кібербезпека - Управління безпекою системи Управління безпекою системи; або ISA 62443-2-3, Керування виправленнями в середовищі IACS.

3.2.12. Синхронізація часу

Рішення для синхронізації часу дозволяють організації синхронізувати час на багатьох пристроях. Це важливо для багатьох функцій, включаючи

кореляцію подій і журналів, механізми автентифікації, контроль доступу та якість обслуговування.

Додаткові вказівки щодо позначки часу наведені в НД ТЗІ 3.6-006-21 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних (автоматизованих) систем».

Захід захисту: «AU-8 Позначка часу».

Рекомендації з упровадження та підтвердження виконання заходів для ОТ/АСУ ТП

Синхронізація внутрішнього годинника систем і пристроїв ОТ має вирішальне значення для кореляції кіберподій та інших функцій ОТ (наприклад, керування рухом).

Якщо пристрій або системний годинник неточні, мітки часу, згенеровані годинником для подій і записів журналу, також будуть неточними, як і будь-які інші функції, які використовують годинник.

На всіх пристроях ОТ слід використовувати спільний час. Використання кількох джерел часу може принести користь пристроям ОТ, зменшивши помилку годинника та забезпечивши резервні джерела часу, якщо основне джерело часу втрачено або якість часу основного джерела часу погіршилася.

Автентифікований протокол мережевого часу (NTP) і безпечний протокол точного часу (PTP) (тобто PTP із TLV автентифікації (тип, довжина, значення) можна використовувати, якщо існує ризик зловмисної зміни мережевого часу (наприклад, RF, глушіння, підробка пакетів, відмова в обслуговуванні). Неавтентифікований NTP чутливий до спуфінгу та має розташовуватися за брандмауером.

Джерела часу, розташовані в середовищі ОТ, повинні бути внесені в програми моніторингу системи та мережі. Якщо доступно, журнали з кожного джерела часу (наприклад, syslog) слід пересилати до системи збору журналів.

3.3. Виявлення (DE)

Функція Detect дозволяє своєчасно виявляти події кібербезпеки, забезпечуючи розроблення та впровадження відповідних заходів.

3.3.1. Аномалії та події (DE.AE)

Організації повинні розуміти різні події та аномалії та їхній потенційний вплив на системи, організацію та середовище, щоб створити ефективні можливості виявлення. У будь-якому середовищі майже безперервно відбуваються численні нешкідливі та потенційно шкідливі події та аномалії. Деякі приклади типових подій містять:

1) інформаційні події:

кілька невдалих спроб входу;

заблоковані облікові записи;

неавторизоване створення нових облікових записів;

неочікувані віддалені входи в систему (наприклад, вхід осіб, які перебувають у відпустці, віддалений вхід, коли особа, як очікується, буде локальною, віддалений вхід для підтримки технічного обслуговування, коли підтримка не запитувалася);

очищено журнали подій;

неочікувано повні журнали подій;

антивірусні або IDS сповіщення;

вимкнено антивірус або інші вимкнені засоби безпеки;

запити інформації про систему або архітектуру (соціальна інженерія або спроби фішингу);

2) операційні події:

несанкціоновані зміни конфігурації;

несанкціоноване патчування систем;

позапланові відключення;

3) події фізичного доступу:

фізичні вторгнення;

4) мережеві події:

неочікуваний зв'язок, у тому числі нові порти чи протоколи, що використовуються без належного керування змінами;

незвично інтенсивний мережевий трафік;

неавторизовані пристрої підключаються до мережі;

несанкціонований зв'язок із зовнішніми IP-адресами.

Організаціям рекомендовано враховувати, що не всі події та аномалії є зловмисними або потребують подальшого розслідування. Організаціям рекомендовано визначити порогові значення попередження про інциденти та вимоги до реагування на події та аномалії, що впливають на їхні системи та середовище, щоб створити ефективні можливості виявлення інцидентів.

Організаціям слід розглянути можливість збору та кореляції даних про події з багатьох джерел і датчиків, використовуючи автоматизовані механізми, де це можливо, щоб покращити можливості виявлення та сповіщення. Наприклад, централізована система виявлення вторгнень може приймати канали даних і журнали з кількох пристроїв і мережевих сегментів для ідентифікації та сповіщення про події, що стосуються організації чи середовища. Засоби виявлення також повинні бути інтегровані з інструментами управління активами. Ця інтеграція може надати додатковий контекст події (наприклад, де розташована система, яку версію мікропрограми вона використовує, яка критичність системи), щоб допомогти організації визначити вплив події.

Додаткові вказівки щодо DE.AE наведені в НД ТЗІ 3.6-006-21 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних (автоматизованих) систем».

Заходи захисту:

«AT-3 Рольове навчання»;

«SI-4 Моніторинг системи»;

«SI-6 Перевірка функцій безпеки та приватності»;

«SI-7 Цілісність програмного забезпечення, вбудованого програмного забезпечення та інформації»;

«SI-15 Фільтрація вихідних даних».

Рекомендації з упровадження та підтвердження виконання заходів для ОТ/АСУ ТП

Організаціям рекомендовано враховувати специфічні для ОТ події та аномалії для своїх процесів і середовищ. Крім того, організаціям рекомендовано враховувати, що деякі інструменти та сповіщення про поведінку чи події, які можуть вказувати на вторгнення, можуть бути нормальною поведінкою та подіями в середовищі ОТ. Щоб зменшити кількість хибних спрацьовувань і неприємних тривог, організації повинні встановити свої порогові значення оповіщення ОТ на основі базових показників нормального мережевого трафіка та потоків даних додатково до нормальної поведінки людини та процесу ОТ. Крім того, компоненти ОТ часто фізично віддалені та не мають постійного персоналу. Порогові значення сповіщень можуть також враховувати час відповіді, пов’язаний із сповіщенням. Наприклад, для виправлення ситуації з метою уникнення інциденту може знадобитися встановити порогове значення попередження про температуру, щоб попереджати раніше на основі очікуваного часу реакції.

Спільні облікові дані часто використовуються в системах ОТ. Аномальну поведінку спільних облікових записів може бути складніше визначити, тому організаціям слід розглянути, чи потрібні додаткові засоби контролю, наприклад, визначення використання спільних облікових даних за допомогою моніторингу фізичного доступу.

3.3.2. Безперервний моніторинг безпеки (DE.CM)

Організація рекомендовано впроваджувати постійний моніторинг як частину організаційної стратегії управління ризиками для моніторингу ефективності захисних заходів. Це передбачає встановлення частоти для оцінювання впровадження бажаних результатів.

Безперервний моніторинг може проводитися за допомогою внутрішніх або зовнішніх ресурсів для виявлення прогалин безпеки в середовищі. Настійно заохочуються експертні оцінки (тобто «холодні огляди») між сайтами однієї організації. Використовуючи сторонні служби для безперервного моніторингу безпеки, важливо розуміти й оцінювати, як дані постійного моніторингу організації захищаються третьою стороною. Третя сторона, яка збирає інформацію постійного моніторингу від кількох організацій, може бути бажаною мішенню для зловмисників.

Додаткові вказівки щодо DE.CM наведені в НД ТЗІ 3.6-006-21 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних (автоматизованих) систем».

Заходи захисту:

«CA-1 Політика і процедури оцінювання, акредитації та моніторингу»;

«CA-7 Безперервний моніторинг».

Рекомендації з упровадження та підтвердження виконання заходів для ОТ/АСУ ТП

Організації можуть виявити, що автоматизація в середовищах ОТ може бути неможливою через чутливість систем або ресурсів, необхідних для підтримки автоматизації. Наприклад, деякі автоматизовані системи можуть використовувати активне сканування для підтримки вразливостей або керування виправленнями або для перевірки конфігурацій пристрою. Рішення, які виконують активне сканування або використовують локальні ресурси для підтримки автоматизації, повинні тестуватися перед розгортанням у системі ОТ.

Безперервний моніторинг може бути досягнутий за допомогою автоматизованих інструментів шляхом пасивного сканування або ручного моніторингу, який виконується з частотою, яка відповідає ризику. Як приклад, оцінка ризику може визначити, що журнали ізольованих (тобто не мережевих) некритичних пристроїв повинні переглядатися щомісяця персоналом ОТ, щоб визначити, чи відбувається аномальна поведінка. Крім того, пасивний мережевий монітор може виявити вразливі мережеві служби без сканування пристроїв.

Коли організації впроваджують методологію вибірки, слід враховувати критичність компонентів. Наприклад, методологія вибірки не повинна випадково виключати пристрої з підвищеним ризиком, такі як брандмауери рівня 3/рівня 4.

Використовуючи треті сторони для постійного моніторингу засобів контролю безпеки, слід переконатися, що залучений персонал має відповідний набір навичок для аналізу середовища ОТ.

3.3.2.1. Моніторинг мережі (DE.CM-1)

Моніторинг мережі передбачає, що організації переглядають сповіщення та журнали та аналізують їх на ознаки можливих інцидентів кібербезпеки. Організаціям слід розглянути можливість автоматизації, включаючи власно розроблені, комерційно доступні рішення або певну комбінацію інструментів, щоб допомогти з моніторингом. Інструменти та можливості, що підтримують виявлення аномалій поведінки (BAD), інформацію про безпеку та керування подіями (SIEM) або системи виявлення/попередження вторгнень (IDS/IPS), можуть допомогти організаціям у моніторингу трафіка в мережі та створювати сигнали тривоги, коли вони виявляють аномальні або підозрілі трафіки. Деякі інші можливості для моніторингу мережі передбачають:

управління активами, включаючи виявлення та інвентаризацію пристроїв, підключених до мережі;

базування типового мережевого трафіка, потоків даних і зв’язку між

пристроями;

діагностику проблем продуктивності мережі;

виявлення неправильної конфігурації або несправності мережевих пристроїв.

Додаткові вказівки щодо DE.CM-1 наведені в НД ТЗІ 3.6-006-21 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних (автоматизованих) систем».

Заходи захисту:

«CA-1 Політика і процедури оцінювання, акредитації та моніторингу»;

«CA-7 Безперервний моніторинг»;

«IR-5 Моніторинг інциденту»;

«PM-14 Тестування, навчання та моніторинг».

Рекомендації з упровадження та підтвердження виконання заходів для ОТ/АСУ ТП

Моніторинг мережі може значно підвищити здатність виявляти атаки, що входять або виходять з мереж ОТ, тим самим покращуючи безпеку. Він також може покращити ефективність мережі, виявляючи несуттєвий трафік. Персонал відділу кібербезпеки ОТ має брати участь у діагностичному процесі інтерпретації сповіщень, які надають інструменти моніторингу мережі. Ретельний моніторинг і розуміння нормального стану мережі ОТ можуть допомогти відрізнити тимчасові умови від легітимних атак і надати розуміння подій, які виходять за межі нормального стану.

Отримання доступу до мережевого трафіка зазвичай здійснюється за допомогою портів комутованого аналізатора портів (SPAN) і мережевих відгалужень. Порти SPAN — функція мережевих пристроїв, яка може логічно дублювати та пересилати вибраний мережевий трафік до рішення для моніторингу мережі. Відводи — мережеві пристрої, які дублюють трафік з одного фізичного каналу. Для обох типів датчиків слід бути обережним, оскільки їх використання може вплинути на продуктивність системи ОТ.

Мережеві датчики слід розмістити для ефективного моніторингу мережі ОТ. Типові установки розташовують мережеві датчики між мережею керування та корпоративною мережею, але інші місця можуть містити периметри мережі, ключові сегменти мережі (наприклад, DMZ) і критичні пристрої ОТ.

Незалежно від типу мережевого датчика, усі датчики мають ретельно тестуватися та впроваджуватися в тестовому середовищі перед розгортанням у мережі ОТ. Налаштування датчика в режим тестування або навчання після його встановлення в мережі дає можливість налаштувати пристрій на реальний мережевий трафік ОТ. Налаштування може допомогти зменшити помилкові спрацьовування сповіщень, зменшити «шум» сповіщень від типового мережевого трафіка та допомогти виявити проблеми впровадження та конфігурації.

Необхідно розглянути режими відмови мережевих датчиків у разі збою

датчика (наприклад, чи є датчик безвідмовним або розмикається, якщо пристрій виходить з ладу).

3.3.2.2. Моніторинг використання системи (DE.CM-1 і DE-CM-3)

Рішення для моніторингу використання системи дозволяють організації відстежувати, зберігати та перевіряти системні події (наприклад, системні журнали, запущені процеси, доступ до файлів і модифікація, зміни конфігурації системи та програм), що відбуваються в системі. Відстеження користувачів і систем допомагає переконатися, що вони поводяться належним чином, і може допомогти у розв'язанні проблем у разі виникнення подій, надаючи інформацію про те, які користувачі працювали в системі під час події. Також можна виявити неправильну конфігурацію системи та пристрою.

Порівняно з моніторингом мережі рішення для моніторингу використання системи можуть аналізувати діяльність, яка не проходить через мережу. У хост-рішеннях цього можна досягти за допомогою моніторингу міжпроцесних зв'язків та інших внутрішніх даних ОС у режимі реального часу, тоді як рішення з активним скануванням збирають інформацію, надсилаючи запити ОС або інтерфейсам прикладного програмування (API).

Додаткові вказівки щодо DE.CM-1 і DE-CM-3 наведені в НД ТЗІ 3.6-006-21 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних (автоматизованих) систем».

Заходи захисту:

«CA-1 Політика і процедури оцінювання, акредитації та моніторингу»;

«CA-7 Безперервний моніторинг»;

«IR-5 Моніторинг інциденту»;

«PM-14 Тестування, навчання та моніторинг»;

«SI-4 Моніторинг системи».

Рекомендації з упровадження та підтвердження виконання заходів для ОТ/АСУ ТП

Ситуаційна обізнаність про систему ОТ є обов'язковою для розуміння поточного стану системи, перевірки того, що вона працює належним чином і що жодні порушення політики чи кіберінциденти не перешкоджали її роботі. Для збору, кореляції та аналізу інформації, пов'язаної з безпекою, необхідний потужний моніторинг, ведення журналів і аудит пристроїв, що призводить до дієвої передачі інформації про стан безпеки по всій системі ОТ. У разі інциденту кібербезпеки інформація, зібрана рішеннями моніторингу використання системи, може бути використана для проведення криміналістичного аналізу системи ОТ.

Системні рішення для моніторингу можуть генерувати значну кількість подій. Зазвичай пропонується використовувати ці рішення в поєднанні із системою керування журналом керування, такою як SIEM, щоб допомогти

відфільтрувати типи подій і зменшити втому від сповіщень. Рівень налаштування подій і сповіщень залежить від типу системи ОТ і кількості пристроїв у системі.

Рішення для моніторингу використання системи мають ретельно тестуватися та впроваджуватися в тестовому середовищі перед розгортанням на пристроях у системі ОТ. Проблеми передбачають вплив агентів на основі хоста на пристрої, вплив активного сканування на пристрої та пропускну здатність мережевої інфраструктури. Окремі пристрої можуть розвантажити обробку. Агенти на основі хоста можуть впливати на продуктивність пристрою ОТ через ресурси, які вони споживають з хоста.

3.3.2.3. Виявлення шкідливого коду (DE.CM-4)

Під час зберігання, обробки та передачі файли та потоки даних слід сканувати за допомогою спеціальних інструментів із поєднанням евристичних алгоритмів і відомих сигнатур зловмисного програмного забезпечення для виявлення та блокування потенційно шкідливого коду. Інструменти захисту від зловмисного коду функціонують ефективно лише тоді, коли вони встановлені, налаштовані, працюють постійно та належним чином підтримуються проти стану відомих методів атак і корисного навантаження.

Додаткові вказівки щодо DE.CM-4 наведені в НД ТЗІ 3.6-006-21 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних (автоматизованих) систем».

Заходи захисту:

«SC-26 Приманка для зловмисників (honeypots)»;

«SI-3 Захист від шкідливого коду»;

«SC-35 Розпізнавання приманок для зловмисників (honeyclient)».

Рекомендації з упровадження та підтвердження виконання заходів для ОТ/АСУ ТП

Незважаючи на те, що антивірусні засоби є загальноприйнятою практикою безпеки в комп’ютерних системах ІТ, використання антивірусу з ОТ може вимагати застосування спеціальних практик, включаючи перевірку сумісності, керування змінами та показники впливу на продуктивність. Ці методи слід використовувати для тестування нових сигнатур і нових версій антивірусного програмного забезпечення.

Деякі постачальники ОТ рекомендують і навіть підтримують використання спеціальних антивірусних інструментів. У деяких випадках постачальники систем ОТ могли провести регресійне тестування своєї лінійки продуктів для підтримуваних версій певного антивірусного засобу та надати відповідну документацію щодо встановлення та налаштування.

Загалом:

системи загального призначення Windows, Unix, Linux тощо, які використовуються як інженерні робочі станції, архіви даних, ноутбуки для обслуговування та сервери резервного копіювання, можуть бути захищені як

комерційне ІТ-обладнання: варто інсталювати антивірусне програмне забезпечення з автоматичним оновленням або з оновленнями, які розповсюджуються через антивірус сервер, розташований всередині мережі керування процесом; слід дотримуватися розроблених організацією процедур для передачі останніх оновлень із завідомо справних сайтів постачальників на антивірусні сервери ОТ на інші комп'ютери та сервери ОТ;

варто дотримуватися рекомендацій постачальника щодо всіх інших серверів і комп'ютерів (наприклад, DCS, PLC, приладів), які мають залежний від часу код, модифіковані чи розширені ОС або будь-які інші зміни, які відрізняють їх від стандартного ПК. Необхідно виконати тестування антивірусного програмного забезпечення та оновлень в автономній системі, якщо це можливо (наприклад, інсталюйте на резервний HMI та переконайтеся, що продуктивність не погіршилася перед застосуванням до основного HMI).

Відповідно до NIST SP 1058 антивірусне програмне забезпечення може негативно впливати на критичні за часом процеси керування ICS. SP також виявив значне використання ЦП під час сканування вручну та оновлення підписів, що може мати негативний вплив на комп'ютери та сервери ОТ. Як результат:

конфігурація антивірусного програмного забезпечення повинна бути перевірена в автономній системі, якщо це можливо;

ручне сканування та оновлення підписів слід виконувати, поки система не є критичною для операцій;

слід розглянути надлишковість для критично важливих систем, які вимагають постійних оновлень антивірусу, щоб оновлення сигнатур можна було виконувати без впливу на роботу (наприклад, консолі та HMI);

під час налаштування списків виключень файлів визначте, які файли контрольної програми не слід сканувати під час виробництва через можливу несправність системи ОТ або зниження продуктивності.

CISA надає рекомендації щодо оновлення антивірусної програми в середовищах ОТ.

3.3.2.4. Сканування вразливостей (DE.CM-8)

Вразливі місця можна виявити за допомогою поєднання автоматизованих і ручних методів. Ці сканування вразливостей слід виконувати на постійній основі, щоб виявити нові вразливості в міру їх виявлення.

Додаткові вказівки щодо DE.CM-8 наведені в НД ТЗІ 3.6-006-21 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних (автоматизованих) систем».

Захід захисту: «RA-5 Сканування вразливостей».

Рекомендації з упровадження та підтвердження виконання заходів для ОТ/АСУ ТП

Нижче наведено кілька поширених способів ідентифікації вразливостей у середовищі ОТ:

постійний моніторинг з використанням пасивних або активних можливостей сканування. Організаціям слід розглянути, як інструменти сканування вразливостей можуть вплинути на компоненти ОТ і комунікації шляхом тестування в автономному середовищі перед впровадженням у виробництво;

інструменти пасивного сканування зазвичай використовують аналізатори мережевого трафіка для виявлення активів і визначення можливих вразливостей, що впливають на активи;

інструменти активного сканування зазвичай використовують агента для підключення до мережевих активів і виконання детальних запитів і аналізу компонентів для визначення можливих вразливостей, що впливають на активи;

тестування продуктивності, тестування навантаження та тестування на проникнення, якщо тест не матиме негативного впливу на виробниче середовище;

регулярні аудити, оцінки та експертні перевірки для виявлення прогалин у безпеці.

3.3.3. Процес виявлення (DE.DP)

Процес виявлення передбачає підтримку та тестування процесів, процедур та інструментів для забезпечення швидкого виявлення аномальних подій і сповіщення відповідальних сторін (осіб), а також надання списків відповідальних за адекватне реагування. Щоб забезпечити постійну обізнаність про аномальні події, слід: визначити ролі та обов’язки для забезпечення відповідальності; періодично перевіряти відповідність діяльності з виявлення вимогам; регулярно перевіряти процеси виявлення; повідомляти про виявлені події відповідному персоналу для вжиття заходів; постійно покращувати можливості виявлення.

3.4. Реагування (RS)

Функція реагування підтримує можливість вжити відповідних заходів для стримування інциденту кібербезпеки, коли він виникає.

3.4.1. Планування реагування (RS.RP)

Реагуючи на події, організації повинні намагатися охопити деталі, пов’язані з виконанням задокументованих планів реагування. Це може допомогти організаціям під час процесу аналізу після інциденту виявити прогалини або потенційні можливості для вдосконалення плану реагування.

Через чутливість часу реагування, якщо фіксація деталей виконання впливає на безпеку або збільшує час для виконання плану реагування, організації можуть розглянути інші методи, такі як перегляд журналів, перегляд відеозаписів, знятих під час реагування, або опитування персоналу реагування.

3.4.2. Зворотні зв’язки (RS.CO)

Реагування на інцидент кібербезпеки передбачає координацію з внутрішніми та зовнішніми зацікавленими сторонами. Необхідно створити групу реагування на інциденти. Залежно від складності та впливу інциденту, група реагування на інцидент може складатися з одного або кількох осіб, які пройшли навчання щодо реагування на інциденти. Національну систему управління інцидентами FEMA (NIMS) можна використовувати для стандартизації загальної термінології та ролей для реагування на інциденти.

До інциденту організаціям рекомендовано розглядати, як спілкуватися з персоналом реагування та зовнішніми організаціями, зокрема:

розробка списку розсилки електронної пошти для реагування на інциденти;

використання системи екстреного сповіщення;

створення резервних планів зв’язку для радіо/телефону/електронної пошти, якщо основні інформаційно-комунікаційні системи вийдуть з ладу;

призначення прес-секретаря для зовнішніх комунікацій;

призначення секретаря для внутрішнього зв’язку з інцидентами.

Рекомендації з упровадження та підтвердження виконання заходів для ОТ/АСУ ТП

Персонал, відповідальний за реагування на інцидент, повинен бути проінформований і навчений щодо своїх обов'язків.

План реагування має містити детальний перелік організацій та персоналу, з якими слід зв’язатися для реагування на інцидент та звітування за різних обставин. Кожній особі слід призначити роль або ролі, необхідні для реагування на інциденти, які можуть включати ролі командира інциденту, керівника або члена відділу операцій, планування, логістики або фінансів/адміністрації; офіцера із громадської інформації, безпеки або зв'язку.

Організація інформує про кіберінцидент, що мав місце, державного координатора з питань кібербезпеки відповідно до чинного законодавства, а також галузевого координатора.

Для підтримки реагування в середовищі ОТ організація повинна розглянути можливість включення наступного персоналу до плану реагування:

1) внутрішні ресурси:
керівник з інцидентів;
операційне керівництво;
охоронний персонал;
черговий персонал систем ОТ;
ІТ-персонал за викликом;4
персонал фізичної охорони;
адміністративний персонал;
закупівлі;
2) зв'язки з громадськістю та юридичний персонал;

3) зовнішні галузеві партнери:

технічна підтримка ОТ (вендори, інтегратори);

операційний ланцюг постачання (наприклад, постачальники, клієнти, дистриб'ютори, ділові партнери);

група реагування на інциденти;

підтримка перенапруги;

постраждала громада (наприклад, сусіди організації).

Юридичні служби організації часто можуть допомогти в розробці угод про нерозголошення інформації або інших контрактів, якщо організація планує використовувати зовнішні ресурси для реагування на інциденти. Може бути корисно розробити ці контракти до того, як станеться інцидент, щоб реагувати на інцидент можна було негайно.

3.4.3. Аналіз повідомлень систем безпеки (RS.AN)

Аналіз інцидентів кібербезпеки проводиться для забезпечення ефективного реагування та заходів з відновлення відповідно до процесу виявлення та плану реагування. Аналіз передбачає перегляд повідомлень і визначення необхідності подальшого розслідування, розуміння потенційного впливу, проведення криміналістичних заходів, класифікацію інциденту відповідно до плану реагування та аналіз виявлених вразливостей.

Додаткові вказівки щодо RS.AM наведені в НД ТЗІ 3.6-006-21 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних (автоматизованих) систем». Захід захисту: «AU-6 Огляд, аналіз і звітність аудиту».

Рекомендації з упровадження та підтвердження виконання заходів для ОТ/АСУ ТП

Визначаючи загальний вплив інциденту кібербезпеки, слід враховувати залежності ОТ і його кінцевий вплив на операції. Наприклад, система ОТ може залежати від ІТ для бізнес-додатків, так що інцидент в ІТ-мережі призводить до відключення або завершення роботи ОТ.

Якщо організація не має достатніх ресурсів або можливостей для проведення криміналістичної експертизи ОТ, варто розглянути можливість залучення зовнішніх організацій для проведення криміналістичного аналізу.

Організаціям рекомендовано ідентифікувати та класифікувати кібер-і некібер-інциденти, що впливають на середовище ОТ, відповідно до плану реагування на інциденти. Під час розробки плану реагування на інциденти ОТ потенційні класи інцидентів можуть включати випадкові дії, вжиті уповноваженим персоналом, цілеспрямовані зловмисні атаки та нецільові зловмисні атаки.

3.4.4. Пом'якшення наслідків (RS.MI)

Виконуються заходи, щоб запобігти розширенню інциденту, пом'якшити його наслідки та вирішити інцидент. Діяльність зі зменшення

наслідків має узгоджуватися з планом реагування.

Рекомендації з упровадження та підтвердження виконання заходів для ОТ/АСУ ТП

Компоненти ОТ часто фізично віддалені та не мають постійного персоналу. Для цих випадків слід розглянути, як організація буде реагувати під час інциденту та додатковий час, необхідний для координації реагування. Може, необхідно розробити систему з можливістю мінімізації впливу, поки персонал не зможе прибути на місце (наприклад, дистанційне відключення або відключення).

Пом’якшення кіберінцидентів може передбачати зупинку процесів або відключення зв’язку, що впливає на роботу. Цей вплив слід розуміти та повідомляти про нього під час пом’якшення інциденту.

3.4.5. Покращення реагування (RS.IM)

Діяльність організаційного реагування покращується шляхом урахування досвіду, отриманого з поточних і попередніх заходів виявлення та реагування. Рекомендується призначити особу(-ів), відповідальну(их) за документування та передачу дій реагування групі реагування на інциденти, які пізніше можуть бути переглянуті на предмет отриманого досвіду.

3.5. Відновлення (RC)

Вчасне відновлення нормальної роботи після інциденту кібербезпеки має вирішальне значення. Функція відновлення спрямована на розробку та впровадження заходів для підтримки стійкості систем і забезпечення своєчасного відновлення можливостей і послуг, постраждалих від інциденту кібербезпеки.

3.5.1. Планування відновлення (RC.RP)

Під час відновлення після подій організаціям рекомендовано спробувати зафіксувати деталі, пов’язані з виконанням задокументованих планів відновлення. Обговорення деталей виконання може допомогти організаціям під час аналізу інциденту і визначити, чи слід враховувати будь-які прогалини або потенційні можливості для покращення плану відновлення. Через чутливість часу відновлення, якщо запис деталей виконання впливає на безпеку або збільшує час для завершення плану відновлення, організації можуть захотіти розглянути інші методи, такі як перегляд журналів, перегляд відеозаписів, знятих під час відновлення, або опитування персоналу відновлення.

Додаткові вказівки щодо RC.RP наведені в НД ТЗІ 3.6-006-21 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних (автоматизованих) систем».

Захід захисту: «CP-2 План забезпечення безперервної роботи та відновлення функціонування».

3.5.2. Покращення відновлення (RC.IM)

Оскільки зусилля з відновлення тривають, вжиті кроки відновлення повинні бути задокументовані, щоб розробити отримані навички, які можна використовувати для покращення планів і процесів відновлення.

Додаткові вказівки щодо RC.IM наведені в НД ТЗІ 3.6-006-21 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних (автоматизованих) систем».

Захід захисту: «CP-2 План забезпечення безперервної роботи та відновлення функціонування».

3.5.3. Комунікування під час відновлення (RC.CO)

Реставраційна діяльність узгоджується з внутрішніми та зовнішніми сторонами. Окрім оперативного відновлення, організації може знадобитися налагодження зв’язків з громадськістю та відновлення своєї репутації.

Додаткові вказівки щодо RC.CO наведені в НД ТЗІ 3.6-006-21 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних (автоматизованих) систем».

Захід захисту: «CP-2 План забезпечення безперервної роботи та відновлення функціонування».

Рекомендації з упровадження та підтвердження виконання заходів для ОТ/АСУ ТП

Перелік внутрішніх і зовнішніх ресурсів для діяльності з відновлення слід розробити як частину зусиль з планування відновлення. Під час події цей список слід використовувати, щоб залучити весь необхідний персонал, якщо потрібно, для відновлення в RTO та RPO.

1) внутрішні комунікації:

персонал ОТ;

ІТ-персонал;

закупівлі;

керівництво з відповідними повноваженнями затверджувати вартість відновлення;

складський персонал;

2) зовнішні комунікації:

постачальники ОТ;

охоронні компанії, які можуть бути затримані для реагування та відновлення;

складський персонал;

постачальники електронних комунікаційних послуг;

власники атакуючих систем і потенційні жертви.

V. Вимоги до цільових профілів кіберзахисту автоматизованих систем управління технологічними процесами

1. Класифікація автоматизованих систем управління технологічними процесами за рівнем негативного впливу

Рівні негативного впливу автоматизованих систем управління технологічними процесами відповідають рівням негативного впливу на надання основних послуг у разі знищення, пошкодження або порушення функціонування об’єкта критичної інфраструктури, що визначені у додатку 1 до Методики категоризації об’єктів критичної інфраструктури, затвердженої постановою Кабінету Міністрів України від 09 жовтня 2020 року № 1109.

2. Стандартні цільові профілі кіберзахисту об’єктів критичної інфраструктури

2.1. Стандартний цільовий профіль кіберзахисту визначає мінімальний необхідний рівень упровадження для кожної підкатегорії заходів кіберзахисту ОТ/АСУ ТП відповідно до рівня негативного впливу на надання основних послуг у разі знищення, пошкодження або порушення функціонування об’єкта критичної інфраструктури.

2.2. Досягнення рівня впровадження заходів кіберзахисту визначається за повнотою виконання цих заходів з урахуванням поточної практики щодо реалізації заходів кіберзахисту та управління ризиками кібербезпеки на ОКІ, характеристики загроз кібербезпеки, з урахуванням законодавчих та нормативних вимог, комерційних та стратегічних цілей ОКІ, вимог до кібербезпеки в ланцюзі поставок програмного/апаратного забезпечення, організаційних та інших обмежень. Додаткова інформація про визначення 1 - 4 рівнів впровадження заходів кіберзахисту наведена в розділі 3 частини V цих Рекомендацій.

2.3. Рівень впровадження підкатегорії заходів кіберзахисту визначається експертним шляхом відповідно до Рекомендацій.

2.4. Рівень впровадження заходів кіберзахисту стандартного цільового профілю для кожної категорії заходів кіберзахисту розраховується так:

$$СЦ_{кат} = \frac{\sum V_{підкат}}{N_{кат}},$$

де $СЦ_{кат}$ – мінімальний середній рівень впровадження заходів;

$V_{підкат}$ – рівень упровадження підкатегорії заходів, яка належить до категорії;

$N_{кат}$ – кількість підкатегорій заходів, що належить до категорії.

2.5. Стандартні цільові профілі кіберзахисту для ОТ/АСУ ТП I та II рівня негативного впливу наведено в табл. 24.

Таблиця 24 – Стандартний цільовий профіль кіберзахисту

Функція кібербезпеки	Категорія заходів кіберзахисту	Підкатегорія заходів кіберзахисту	Стандартний цільовий профіль кіберзахисту (мінімальний рівень упровадження)	
			для I рівня (катастрофічні наслідки)	для II рівня (критичні наслідки)
1	2	3	4	5
Ідентифікація ризиків кібербезпеки (ID)	ID.AM Управління активами	ID.AM-1 ID.AM-2 ID.AM-3 ID.AM-4 ID.AM-5 ID.AM-6	3	3
	ID.BE Середовище надання життєво важливих послуг та функцій	ID.BE-1 ID.BE-2 ID.BE-3 ID.BE-4 ID.BE-5	3	3
	ID.GV Управління безпекою	ID.GV-1 ID.GV-2 ID.GV-3 ID.GV-4	4	3
	ID.RA Оцінка ризиків	ID.RA-1 ID.RA-2 ID.RA-3 ID.RA-4 ID.RA-5 ID.RA-6	3	3
	ID.RM Стратегія управління ризиками організації	ID.RM-1 ID.RM-2 ID.RM-3	3	3
	ID.SC Управління ризиками системи постачання	ID.SC-1 ID.SC-2 ID.SC-3 ID.SC-4	4	3

1	2	3	4	5
Захист (PR)	PR.AC Управління ідентифікацією, автентифікацією та контроль доступу	PR.AC-1 PR.AC-2 PR.AC-3 PR.AC-4 PR.AC-5 PR.AC-6	4	3
	PR.AT Обізнаність та навчання	PR.AT-1 PR.AT-2 PR.AT-3 PR.AT-4 PR.AT-5	4	3
	PR.DS Безпека даних	PR.DS-1 PR.DS-2 PR.DS-3 PR.DS-4 PR.DS-5 PR.DS-6 PR.DS-7	4	3
	PR.IP Процеси та процедури кіберзахисту	PR.IP-1 PR.IP-2 PR.IP-3 PR.IP-4 PR.IP-5 PR.IP-6 PR.IP-7 PR.IP-8 PR.IP-9 PR.IP-10	4	3
	PR.MA Технічне обслуговування	PR.MA-1 PR.MA-2	4	3
	PR.PT Технології кіберзахисту	PR.PT-1 PR.PT-2 PR.PT-3 PR.PT-4 PR.PT-5	4	3
Виявлення кіберінцидентів (DE)	DE.AE Аномалії та кіберінциденти	DE.AE-1 DE.AE-2 DE.AE-3 DE.AE-4 DE.AE-5	4	3

1	2	3	4	5
	DE.CM Безперервний моніторинг кібербезпеки	DE.CM-1 DE.CM-2 DE.CM-3 DE.CM-4 DE.CM-5 DE.CM-6 DE.CM-7 DE.CM-8	4	3
	DE.DP Процеси виявлення кіберінцидентів	DE.DP-1 DE.DP-2 DE.DP-3 DE.DP-4 DE.DP-5	4	3
Реагування на кіберінциденти (RS)	RS.RP Планування реагування	RS.RP-1	4	3
	RS.CO Комунікації	RS.CO-1 RS.CO-2 RS.CO-3 RS.CO-4 RS.CO-5	4	3
	RS.AN Аналіз	RS.AN-1 RS.AN-2 RS.AN-3 RS.AN-4	3	3
	RS.MI Мінімізація наслідків	RS.MI-1 RS.MI-2 RS.MI-3	4	3
	RS.IM Удосконалення	RS.IM-1 RS.IM-2	3	3
Відновлення стану кібербезпеки (RC)	RC.RP Планування відновлення	RC.RP-1 RC.RP-2	3	3
	RC.IM Удосконалення	RC.IM-1	3	3
	RC.CO Комунікації	RC.CO-1 RC.CO-2 RC.CO-3	3	3

3. Методика оцінювання рівня впровадження заходів кіберзахисту

Відповідно до Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури, затверджених наказом

Адміністрації Держспецзв'язку від 06 жовтня 2021 року № 601, та NIST Framework for Improving Critical Infrastructure Cybersecurity (далі – NIST CSF) визначено чотири ієрархічних рівні впровадження заходів кіберзахисту:

частковий;
ризик-орієнтований;
повторюваний;
адаптивний.

3.1. Визначення рівня впровадження заходів кіберзахисту АСУ ТП

Заходи кіберзахисту АСУ ТП є невід'ємною частиною кіберзахисту об'єкта критичної інфраструктури (далі - ОКІ). Упровадження заходів кіберзахисту буде неефективним без врахування рівнів зрілості ІТ процесів ОКІ. Пропонується використання відповідності рівнів упровадження заходів кіберзахисту, визначених цими Рекомендаціями, а також NIST CSF, ISA 62443-1-1, рівням зрілості ІТ процесів, визначених Методологією COBIT 5, наведеної в табл. 25.

Таблиця 25 – Відповідність рівнів упровадження заходів кіберзахисту, рівнів захищеності інформації рівням зрілості ІТ процесів

Рекомендації/NIST CSF	**ISA 62443-1-1 (ISA 62443-3-3 Annex A)**	**COBIT 5**
1	2	3
1. Частковий	0. Не має засобів захисту 1. Захищений від випадкового/ненавмисного порушення безпеки	0. Incomplete process (Не існуючий) 1. Performed process (Початковий)
2. Ризик-орієнтований	2. Захищений від слабкого навмисного втручання (невеликі ресурси та знання, низька мотивація, прості засоби)	2. Managed process (повторюваний, але інтуїтивний)
3. Повторюваний	3. Захищений від наполегливого навмисного втручання (задіяно суттєві ресурси, підключено професіоналів і спеціалізовані засоби, але атакуюча сторона має обмеження в можливостях та/або ресурсах та/або часі)	3. Established process (визначений)

1	2	3
4. Адаптивний	4. Захищений від цілеспрямованої наполегливої атаки (коли атакуюча сторона має ресурси на регулярні ворожі дії, постійно вдосконалює механізми атаки, вичікує, шукає нові вразливості)	4. Predictable process (керований та вимірюваний) 5. Optimising process (оптимізований)

За результатами такого порівняння для АСУ ТП будуть застосовуватися такі рівні впровадження заходів кіберзахисту:

0 – підкатегорію заходів кіберзахисту не імплементовано;

1 – імплементовано частково, несистемно;

2 – вона переважно імплементовано, системи контролю дотримання немає чи вона недостатня;

3 – переважно імплементовано, контролюється дотримання на поточному рівні;

4 – імплементовано в необхідному обсязі і працюють процедури контролю та актуалізації вимог.

Основою для визначення рівнів впровадження згідно з цими Рекомендаціями є процеси управління ризиками. Необхідний рівень впровадження залежить від рівня ризику для держави, який визначається з урахуванням рівня негативного впливу на надання основних послуг у разі знищення, пошкодження або порушення функціонування об’єкта критичної інфраструктури відповідно до постанови Кабінету Міністрів України від 09 жовтня 2020 року № 1109 «Деякі питання об’єктів критичної інфраструктури».

Залежність необхідного рівня впровадження заходів кіберзахисту від наявного рівня ризику наведено в табл. 26.

Таблиця 26 - залежність необхідного рівня впровадження від наявного рівня ризику

Рекомендації/NIST CSF	**COBIT 5**	**Низький ризик**	**Середній ризик**	**Високий ризик**
1	2	3	4	5
1. Частковий	0. Incomplete process (не існуючий) 1. Performed process (початковий)			
2. Ризик-орієнтований	2. Established process (визначений)			

1	2	3	4	5
3. Повторюваний	3. Established process (налагоджені)			
4. Адаптивний	4. Predictable process (керований та вимірюваний) 5. Optimising process (оптимізований)			

Враховуючи визначення терміна «ризик» у ДСТУ ISO/IEC 27001 як вплив невизначеності на цілі, більший ризик матиме ОКІ з вищим рівнем можливого негативного впливу у разі порушення його функціонування.

Оцінювання рівня ризику для АСУ ТП ОКІ здійснюється за стандартом ДСТУ ISO/IEC 27005, що є методичною основою для оцінювання ризиків на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури відповідно пункту 4 додатку «Перелік базових вимог із забезпечення кіберзахисту об’єктів критичної інфраструктури» до Загальних вимог до кіберзахисту об'єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 року № 518.

3.2. Оцінювання рівня впровадження комплексу заходів кіберзахисту (цільового профілю)

Після визначення рівня ризику для ОКІ визначається рівень упровадження комплексу заходів кіберзахисту (цільового профілю).

Використовується шкала оцінювання відповідно до рекомендацій стандарту ДСТУ ISO/IEC 33004:2016 «Інформаційні технології. Оцінювання процесу. Вимоги до еталонної моделі процесу, моделі оцінювання процесу та моделі зрілості (ISO/IEC 33004:2015, IDT)»:

«повністю впроваджено»: рівень можливостей досягається понад 85 відсотків;

«переважно впроваджено»: рівень можливостей досягається між 50 і 85 відсотками;

«частково впроваджено»: рівень можливостей досягається між 15 і 50 відсотками;

«не впроваджено»: рівень можливостей досягнуто менше ніж на 15 відсотків.

Рівень впровадження визначається на основі повноти базових атрибутів процесів:

обізнаність і комунікація;

політики, плани і процедури;

інструменти та автоматизація;

навички і знання;

відповідальність і підзвітність;

постановка цілей і вимірювання ризику.

Базові атрибути повинні бути оцінені, враховуючи цілі організації та результати процесів.

Базові атрибути визначаються для кожного заходу кіберзахисту відповідно до вимог законодавства, стандартів безпеки та політик організації.

Для ОКІ використовується такий алгоритм дій для оцінювання рівня впровадження заходів з кіберзахисту АСУ ТП:

1) за наявною моделлю загроз визначити величину ризику відсутності кожного заходу кіберзахисту зі стандартного цільового профілю;

2) визначити власний поточний профіль як множину наявних заходів кіберзахисту на момент оцінювання ризиків;

3) визначити власний цільовий профіль як суму множин заходів кіберзахисту поточного профілю і множини необхідних заходів кіберзахисту за результатами попереднього аналізування ризиків;

4) визначити базові атрибути заходів кіберзахисту власного поточного профілю;

5) визначити базові атрибути заходів кіберзахисту власного цільового профілю;

6) на основі визначених НД ТЗІ середніх значень рівнів впровадження для підкатегорій заходів кіберзахисту визначити поточне значення рівня впровадження поточного профілю;

7) на основі визначених НД ТЗІ середніх значень рівнів впровадження для підкатегорій заходів кіберзахисту визначити цільове середнє значення рівня впровадження цільового профілю;

8) визначити пріоритети впровадження заходів кіберзахисту або їх поліпшення для досягнення рівня впровадження, який визначено в цільовому профілі.

Директор Департаменту кіберзахисту
Адміністрації Держспецзв’язку
полковник Данило МЯЛКОВСЬКИЙ