Платформа для підвищення кібербезпеки критично важливих інфраструктур

Версія 1.1

Національний інститут стандартів та технологій

16 квітня 2018 р.

https://doi.org/10.6028/NIST.CSWP.04162018uk

Translated by Andrii Paziuk (Ukrainian Academy of Cybersecurity, uacs.kiev.ua) with the support of the U.S. Embassy in Ukraine. Reviewed by Oleksandr Bolshov and Diplomatic Language Services. Official U.S. Government translation.

The official English language version of this publication is available free of charge from the National Institute of Standards and Technology (NIST): https://doi.org/10.6028/NIST.CSWP.04162018.

Примітка для читачів щодо оновлення

Версія 1.1 цієї Платформи кібербезпеки уточнює, роз'яснює і покращує Версію 1.0, яка була випущена в лютому 2014 року. Вона включає коментарі, отримані щодо двох проектів Версії 1.1.

Версія 1.1 призначена для реалізації початковими і поточними користувачами Платформи. Поточні користувачі повинні мати можливість впроваджувати Версію 1.1 з мінімальними порушеннями чи взагалі без них; явною метою була сумісність з Версією 1.0.

Нижченаведена таблиця підсумовує зміни між Версією 1.0 та Версією 1.1. Платформи

Таблиця NTR-1 - Резюме змін між Версією 1.0 та Версією 1.1. Платформи

Оновлення	Опис оновлення
Пояснюється, що терміни, такі як "відповідність", можуть бути заплутаними та означати щось різне для різних зацікавлених сторін Платформи	Додана чіткість в тому, що Платформа має корисність як структура та мова для організації і вираження відповідності власним вимогам організації з кібербезпеки. Проте різноманітність способів, якими організація може використовувати Платформу, означає, що фрази, такі як "дотримання Платформи", можуть бути заплутаними.
Новий розділ про самооцінку	Додано Розділ 4.0 *Самооцінка ризику для кібербезпеки за допомогою Платформи* для пояснення того, як організації можуть використовувати Платформу для розуміння та оцінки їхнього ризику для кібербезпеки, включаючи використання вимірювань.
Значно розширене пояснення використання Платформи для цілей Управління ризиком для кібербезпеки ланцюжків поставок	Розширений Розділ 3.3 *Повідомлення вимог щодо кібербезпеки зацікавленим сторонам* допомагає користувачам краще зрозуміти Управління ризиком ланцюжків поставок (SCRM), тоді як новий Розділ 3.4 *Рішення щодо покупки* висвітлює використання Платформи для розуміння ризику, пов'язаного з готовими комерційними продуктами та послугами. Додаткові критерії кібер-SCRM були додані до Рівнів впровадження. Нарешті, в Основу платформи було додано Категорію управління ризиком ланцюжків поставок для кібербезпеки, включаючи кілька Підкатегорій.

Вдосконалення для кращого обліку аутентифікації, авторизації та перевірки персональних даних	Мова Категорії контролю доступу була вдосконалена для кращого обліку аутентифікації, авторизації та перевірки персональних даних. Це включало додання одної Підкатегорії для аутентифікації, авторизації та перевірки персональних даних. Також Категорія була перейменована в Управління ідентифікацією та контроль доступу (PR.AC), щоб краще представляти сферу застосування Категорії та відповідних Підкатегорій.
Краще пояснення взаємозв'язку між Рівнями впровадження та Профілями	Додано текст до Розділу 3.2. *Встановлення або вдосконалення програми кібербезпеки* щодо використання Рівнів платформи в реалізації Платформи. Додано текст до Рівнів платформи, щоб відобразити інтеграцію основних міркувань Платформи в рамках організаційних програм управління ризиками. Концепції Рівнів платформи також були вдосконалені. Оновлено Рисунок 2.0 для включення дій з Рівнів платформи.
Розгляд координованого розкриття інформації про вразливість	Була додана Підкатегорія, яка стосується життєвого циклу розкриття інформації про вразливість.

Як і у Версії 1.0, користувачам Версії 1.1 пропонується адаптувати Платформу для максимізації індивідуальної організаційної цінності.

Подяка

Ця публікація є результатом постійних спільних зусиль із залученням промисловості, наукових кіл та уряду. Національний інститут стандартів і технологій (NIST) запустив проект шляхом скликання приватних і громадських організацій та приватних осіб у 2013 році. Ця *Платформа для підвищення для кібербезпеки критично важливих інфраструктур*, опублікована в 2014 році та переглянута протягом 2017 та 2018 років, опиралася на вісім громадських семінарів, кілька Запитів про коментар чи інформацію та тисячі прямих взаємодій із зацікавленими сторонами з усіх секторів у Сполучених Штатах разом із багатьма секторами з усього світу.

Поштовхом для зміни Версії 1.0 та змін, які з'являються у цій Версії 1.1, були:

- Зворотній зв'язок та поширені запитання до NIST після випуску Версії 1.0;
- 105 відповідей на запит про надання інформації (RFI) в грудні 2015 р. *Погляди на Платформу для підвищення кібербезпеки критично важливих інфраструктур*;
- Понад 85 коментарів 5 грудня 2017 року запропонували другий проект Версії 1.1;
- Понад 120 коментарів 10 січня 2017 року запропонували перший проект Версії 1.1; і
- Вхідні дані від більш ніж 1200 учасників семінарів щодо Платформи в 2016 та 2017 роках.

Крім того, NIST попередньо випустив Версію 1.0 Платформи кібербезпеки із супровідним документом *Дорожня карта NIST для підвищення кібербезпеки критично важливих інфраструктур*. Ця Дорожня карта висвітлила ключові "сфери підвищення" для подальшого розвитку, приведення у відповідність та співпраці. Завдяки зусиллям приватного та державного секторів деякі області підвищення досягли достатнього прогресу для включення до цієї Версії 1.1.

NIST висловлює вдячність тим, хто зробив свій внесок в цю Платформу.

Резюме

США залежать від надійного функціонування критично важливих інфраструктур. Загрози для кібербезпеки використовують підвищену складність і зв'язність систем критично важливих інфраструктур, ставлячи під загрозу національну безпеку, економіку та безпеку та здоров'я населення. Ризик для кібербезпеки, подібно до фінансових та репутаційних ризиків, впливає на чистий дохід компанії. Він може збільшити витрати та впливати на доходи. Він може спричинити шкоду здатності організації впроваджувати інновації, а також отримувати та тримати клієнтів. Кібербезпека може бути важливою та посилюючою складовою загального управління ризиками організації.

Щоб краще справлятися з цими ризиками, у Законі про вдосконалення кібербезпеки від 2014 року[1] (CEA) було оновлено роль Національного інституту стандартів та технологій (NIST): включено визначення та розвиток платформ ризику для кібербезпеки для добровільного використання власниками та операторами критично важливих інфраструктур. За допомогою CEA Національний інститут стандартів та технологій повинен визначити "пріоритетний, гнучкий, повторюваний, дієвий та економічно ефективний підхід, включаючи заходи та засоби захисту інформації, які можуть бути добровільно прийняті власниками та операторами критично важливої інфраструктури, щоб допомогти їм визначити, оцінити та управляти кібер-ризиками". Це формалізувало попередню роботу NIST по розробленню Версії 1.0 Платформи відповідно до Указу 13636 "Підвищення для кібербезпеки критично важливих інфраструктур" (лютий 2013 р.) та надало керівництво для подальшої еволюції Платформи. Платформа, що була розроблена згідно з Указом 13636 і продовжує розроблятися відповідно до CEA, використовує загальну мову для того, щоб справлятися з та управляти ризиками для кібербезпеки економічно ефективним методом, спираючись на ділові та організаційні потреби, не ставлячи додаткові регуляторні вимоги до бізнесу.

Платформа зосереджена на використанні рушійних сил бізнесу для управління діяльністю з кібербезпеки та розгляду ризиків для кібербезпеки як складової організації процесів управління ризиками. Платформа складається з трьох частин: Основа платформи, Рівні впровадження і Профілі платформи. Основа платформи - це набір заходів, результатів та інформаційних посилань, які є спільними для різних секторів та критичних інфраструктур. Елементи Основи дають детальні вказівки для розробки окремих організаційних Профілів. Завдяки використанню Профілів Платформа допоможе організації вирівняти та визначати пріоритети своєї діяльності з кібербезпеки, використовуючи вимоги бізнесу/місії, стійкість до ризику та ресурси. Рівні забезпечують механізм, який дозволяє організаціям переглядати та розуміти характеристики свого підходу до управління ризиком для кібербезпеки, що допоможе визначити пріоритети та досягти цілей для кібербезпеки.

Хоча цей документ був розроблений з метою поліпшення управління ризиками для кібербезпеки в галузі критично важливих інфраструктур, Платформа може використовуватися організаціями будь-якого сектора чи спільноти. Структура дає організаціям, незалежно від розміру, ступеня ризику для кібербезпеки або складності для кібербезпеки, застосовувати принципи та найкращі практики управління ризиками для підвищення безпеки та стійкості.

Платформа надає загальну організаційну структуру для багатьох підходів до кібербезпеки

[1] *Див.* 15 U.S.C. § 272(e)(1)(A)(i). Закон про підвищення ефективності кібербезпеки від 2014 року (S.1353) станом на 18 грудня 2014 року став публічним законом 113-274 і доступний за адресою: https://www.congress.gov/bill/113th-congress/senate- bill/1353/text.

шляхом збирання стандартів, керівних принципів та практик, які сьогодні ефективно працюють. Більше того, оскільки вона посилається на загальноприйняті світові стандарти для кібербезпеки, Платформа може слугувати моделлю міжнародної співпраці з метою посилення для кібербезпеки в критично важливих інфраструктурах та інших секторах і спільнотах.

Платформа пропонує гнучкий спосіб вирішення проблем для кібербезпеки, включаючи впливу кібербезпеки на фізичні, кібернетичні та людські аспекти. Це застосовується до організацій, що спираються на технології, незалежно від того, чи їх кібербезпека зосереджена на інформаційних технологіях (IT), промислових системах управління (ICS), кібер-фізичних системах (CPS) або підключених пристроях загалом, включаючи Інтернет речей (IoT) Платформа може допомогти організаціям у вирішенні питань кібербезпеки, оскільки це впливає на конфіденційність клієнтів, працівників та інших сторін. Крім того, результати Платформи слугують цільовими напрямками для розвитку робочої сили та еволюційної діяльності.
Платформа не є єдиним для всіх підходом до управління ризиком для кібербезпеки для критично важливих інфраструктур. Організації й надалі матимуть унікальні ризики - різні загрози, різні вразливості, різні допуски ризику. Вони також будуть різними в тому, як вони налаштують практики, описані в Платформі. Організації можуть визначати діяльність, важливу для надання критично важливих послуг, і можуть визначати пріоритетність інвестицій, щоб максимізувати вплив кожного витраченого долара. Врешті-решт, Платформа спрямована на зменшення та краще управління ризиками для кібербезпеки.

Щоб врахувати унікальні потреби організацій в кібербезпеці, існує безліч способів використання Платформи. Рішення про те, як її застосувати, залишається за організацією, що її впроваджує. Наприклад, одна організація може обрати для використання Рівні впровадження Платформи, щоб сформулювати передбачені практики управління ризиками. Інша організація може використовувати п'ять Функцій платформи, щоб аналізувати весь портфель управління ризиками; цей аналіз може покладатися або не покладатися на більш детальні супровідні вказівки, такі як каталоги контролю. Іноді є дискусія про "відповідність" до Платформи, і Платформа має корисність як структура та мова для організації та вираження відповідності власним вимогам організації щодо для кібербезпеки. Незважаючи на це, різноманітність способів, якими організація може використовувати Платформу, означає, що такі фрази, як " відповідність до Платформи", можуть бути заплутаними та означати щось різне для різних зацікавлених сторін.

Платформа є живим документом, і вона буде продовжувати оновлюватися та вдосконалюватися, коли індустрія провадить зворотний зв’язок щодо її впровадження. NIST буде продовжувати координувати роботу з приватним сектором та державними установами на всіх рівнях. Разом з тим, як Платформа буде все більше застосовуватися на практиці, в майбутні версії буде інтегровано додатковий досвід. Це забезпечить відповідність Платформи потребам власників та операторів критично важливих інфраструктур в динамічному та складному середовищі нових загроз, ризиків та рішень.

Розширене та більш ефективне використання та обмін найкращими практиками цієї добровільної Платформи - це наступні кроки щодо покращення для кібербезпеки критично важливих інфраструктур нашої країни: надання еволюційних рекомендацій окремим організаціям, з одночасним посиленням позиції для кібербезпеки критично важливих інфраструктур країни, економіки та суспільства.

Зміст

Перелік рисунків

Перелік таблиць

1.0 Введення Платформи

США залежать від надійного функціонування їхньої критично важливої інфраструктури. Ризики для кібербезпеки використовують підвищену складність і зв'язність систем критично важливих інфраструктур, ставлячи під загрозу національну безпеку, економіку та безпеку і здоров'я населення. Ризик для кібербезпеки, подібно до фінансових та репутаційних ризиків, впливає на чистий дохід компанії. Він може збільшити витрати та впливати на доходи. Він може спричинити шкоду здатності організації впроваджувати інновації, а також отримувати та підтримувати клієнтів. Кібербезпека може стати важливою та посилюючою складовою загального управління ризиками організації.

Для зміцнення стійкості цієї інфраструктури у Законі про вдосконалення для кібербезпеки від 2014 року [2] (CEA) було оновлено роль Національного інституту стандартів та технологій (NIST) для "сприяння і підтримки розвитку" платформ для усунення ризиків для кібербезпеки. За допомогою CEA NIST повинен визначити "пріоритетний, гнучкий, повторюваний, дієвий та економічно ефективний підхід, включаючи заходи та засоби захисту інформації, які можуть бути добровільно прийняті власниками та операторами критично важливих інфраструктур, щоб допомогти їм визначити, оцінити та управляти кібер-ризиками". Це формалізувало попередню роботу NIST по розробленню Версії 1.0 Платформи відповідно до Указу 13636 "Підвищення для кібербезпеки критично важливих інфраструктур" (лютий 2013 р.) [3] та провадило керівництво для подальшої еволюції Платформи.

Критична інфраструктура[4] визначена в Законі США 2001 року про боротьбу з тероризмом[5] як "фізичні або віртуальні системи та активи, що є настільки важливими для Сполучених Штатів, що недієздатність або знищення таких систем та активів матиме виснажливий вплив на безпеку, національну економічну безпеку, національну охорону здоров'я або безпеку, чи на будь-яке поєднання цих питань". Через посилення тиску зовнішніх та внутрішніх загроз, організації, відповідальні за критично важливу інфраструктуру, повинні мати послідовний та ітераційний підхід до визначення, оцінки та управління ризиком для кібербезпеки. Цей підхід повинен бути незалежний від розміру організації, впливу загроз або складності для кібербезпеки сьогодні.

Спільнота критичної інфраструктури включає державних та приватних власників та операторів, а також інші організації, які мають певну роль у забезпеченні інфраструктури країни. Члени кожного сектору критично важливої інфраструктури виконують функції, які підтримуються широкою категорією технологій, включаючи інформаційні технології (IT), промислові системи управління (ICS), кібер-фізичні системи (CPS) та загальнодоступні пристрої, включаючи Інтернет речей (IoT). Така залежність від технології, зв'язку та взаємозв'язків змінилася і розширила потенційні вразливі місця та збільшила потенційний

---

[2] *Див.* 15 U.S.C. § 272(e)(1)(A)(i). Закон про підвищення ефективності кібербезпеки від 2014 року (S.1353) станом на 18 грудня 2014 року став публічним законом 113-274 і доступний за [2] [2]*Див.* 15 U.S.C. § 272(e)(1)(A)(i). The Cybersecurity Enhancement Act of 2014 (S.1353) став публічним законом 113-274 18 грудня 2014 р. І доступний за адресою: https://www.congress.gov/bill/113th-congress/senate-bill/1353/text.

[3] Програма критичної інфраструктури Міністерства національної безпеки (DHS) надає перелік секторів та пов'язаних з ними критичних функцій та ланцюжків вартості. http ://www.dhs. gov/critical-infrastructure-sectors

[4] Указ № 13636, Підвищення кібербезпеки критичної інфраструктури, DCPD-201300091, 12 лютого 2013 р. https://www.gpo.gov/fdsys/pkg/CFR-2014-title3-vol1/pdf/CFR-2014-title3-vol1-co13636.pdf.

[5] Див. 42 U.S.C. § 5195c (e)). Закон про боротьбу з тероризмом в США 2001 р. (H.R.3162) став публічним законом 107-56 26 жовтня 2001 р., і доступний і за адресою: https://www.congress.gov/bill/107th-congress/house-bill/3162

ризик для операцій. Наприклад, оскільки технологія та дані, які вона створює та обробляє, все частіше використовуються для надання важливих послуг та підтримки бізнес-рішень/місії, слід розглянути потенційні наслідки, пов'язані з інформаційною безпекою для організації, здоров'я та безпеки людей, навколишнього середовища, громад, економіки та суспільства.

Щоб керувати ризиками для кібербезпеки, потрібно чітке уявлення про рушійні сили бізнесу та міркування безпеки організації, характерні для використання ним технології. Оскільки ризики, пріоритети та системи кожної організації є унікальними, інструменти та методи, які використовуються для досягнення результатів, описаних в Платформі, будуть різними.

Визнаючи роль, яку відіграє захист конфіденційності та громадянських свобод у створенні більшої довіри громадськості, Платформа включає методологію захисту персональної конфіденційності та громадянських свобод, коли організації з критично важливою інфраструктурою проводять діяльність з кібербезпеки. Багато організацій вже мають процеси для вирішення питань конфіденційності та громадянських свобод. Методологія розроблена таким чином, щоб доповнювати такі процеси та надати керівництво для полегшення управління ризиками до конфіденційності відповідно до підходу організації до управління ризиком для кібербезпеки. Інтеграція конфіденційності та кібербезпеки може принести користь організаціям завдяки підвищенню довіри споживачів, більш стандартизованому обміну інформацією та спрощенню операцій по всіх правових режимах.

Платформа залишається ефективною та підтримує технічні інновації, оскільки вона є нейтральною технологією, а також посилається на низку існуючих стандартів, керівних принципів та практик, які розвиваються разом з технологіями. Базуючись на тих глобальних стандартах, керівних принципах та практиках, які розробляються, управляються та оновлюються в галузях промисловості, інструменти та методи, доступні для досягнення основних результатів, будуть перетинати кордони, враховувати глобальний характер ризиків для кібербезпеки та розвиватися разом з технологічними досягненнями та бізнес-вимогами Використання існуючих та нових стандартів дозволить забезпечити економію масштабу та стимулюватиме розвиток ефективних продуктів, послуг та практик, які відповідають визначеним ринковим потребам. Ринкова конкуренція також сприяє швидшому розповсюдженню цих технологій та практики і реалізації багатьох переваг для зацікавлених сторін у цих секторах.

Виходячи з цих стандартів, керівних принципів та практики, Платформа забезпечує загальну таксономію та механізм для організацій, щоб:

1. Охарактеризувати їх поточну позицію кібербезпеки;
2. Охарактеризувати цільовий стан кібербезпеки;
3. Ідентифікувати та визначити пріоритети можливостей для вдосконалення в контексті безперервного та повторюваного процесу;
4. Оцінити прогрес у досягненні цільового стану;
5. Спілкуватися між внутрішніми та зовнішніми зацікавленими сторонами щодо ризику для кібербезпеки.

Платформа не є єдиним підходом для управління ризиком для кібербезпеки для критично важливих інфраструктур. Організації й надалі матимуть унікальні ризики - різні загрози, різні вразливості, різні стійкості до ризику. Вони також будуть різними в тому, як вони налаштують практики, описані в Платформі. Організації можуть визначати діяльність, важливу для надання критично важливих послуг, і можуть визначати пріоритетність

інвестицій, щоб максимізувати вплив кожного витраченого долара. Врешті-решт, Платформа спрямована на зменшення та краще управління ризиками для кібербезпеки.

Щоб врахувати унікальні потреби організації в кібербезпеці, існує безліч способів використання Платформи. Рішення про те, як її застосувати, залишається за впроваджуючою організацією. Наприклад, одна організація може обрати для використання Рівні впровадження Платформи, щоб сформулювати передбачені практики управління ризиками. Інша організація може використовувати п'ять Функцій платформи, щоб аналізувати весь портфель управління ризиками; цей аналіз може покладатися або не покладатися на більш детальні супровідні вказівки, такі як каталоги контролю. Існує іноді дискусія про "відповідність" до Платформи, і Платформа має корисність як структура та мова для вираження відповідності власним вимогам організації щодо кібербезпеки. Незважаючи на це, різноманітність способів, якими організація може використовувати Платформу, означає, що такі фрази, як " відповідність до Платформи", можуть бути заплутаними та означати щось різне для різних зацікавлених сторін.

Платформа доповнює, а не замінює процес управління ризиками та програму кібербезпеки організації. Організація може використовувати свої поточні процеси та використовувати Платформу для визначення можливостей для посилення та комунікації свого управління ризиком для кібербезпеки, пристосовуючись до галузевої практики. Або організація без існуючої програми кібербезпеки може використовувати Платформу як посилання для створення такої програми.

Хоча Платформа була розроблена з метою поліпшення управління ризиками для кібербезпеки щодо критично важливої інфраструктури, вона може бути використана організаціями будь-якого сектору економіки або суспільства. Вона призначена для компаній, державних установ та некомерційних організацій незалежно від їх спрямованості та розміру. Спільна таксономія стандартів, керівних вказівок та практик, які вона надає, також не залежить від країни. Організації за межами Сполучених Штатів також можуть використовувати Платформу для зміцнення своїх власних зусиль у сфері кібербезпеки, і Платформа може сприяти розробці спільної мови для міжнародної співпраці у галузі кібербезпеки критично важливих інфраструктур.

1.1 Короткий огляд Платформи

Платформа являє собою підхід, що ґрунтується на оцінці ризику, для управління ризиком для кібербезпеки і складається з трьох частин: Основи платформи, Рівнів впровадження Платформи та Профілів платформи. Кожен компонент Платформи підсилює зв'язок між рушійними силами бізнесу/місії та заходами з кібербезпеки. Ці компоненти пояснюються нижче.

- *Основа платформи* - це набір заходів з кібербезпеки, бажаних результатів та відповідних посилань, що є загальними в секторах критично важливих інфраструктур. Основа представляє галузеві стандарти, керівні принципи та практику таким чином, що забезпечує комунікацію діяльності та результатів з кібербезпеки в масштабах організації - від виконавчого рівня до рівня впровадження/операцій. Основа платформи складається з п'яти одночасних і безперервних Функцій - Ідентифікація, Захист, Виявлення, Реагування, Відновлення. Коли вони розглядаються разом, ці Функції забезпечують високий рівень і стратегічне бачення життєвого циклу управління ризиками для кібербезпеки в організації. Основа платформи визначає основні ключові Категорії та Підкатегорії, які є дискретними підсумками, для кожної Функції, і підбирає відповідники для них, провадячи приклади Інформаційних посилань, таких як

існуючі стандарти, керівні принципи та практики для кожної Підкатегорії.

- *Рівні впровадження Платформи* ("Рівні") забезпечують контекст того, як організація розглядає ризик для кібербезпеки, та процеси, які використовуються для управління цим ризиком. Рівні описують ступінь, в якому практика організації управління ризиком для кібербезпеки виявляє характеристики, визначені в рамках Платформи (наприклад, знання ризику і загроз, повторюваність та адаптивність). Рівні характеризують практику організації в діапазоні від Часткового (Рівень 1) до Адаптивного (Рівень 4). Ці рівні відображають прогрес від неформальних, реактивних реакцій до підходів, які є гнучкими та ризик-інформованими. Під час процесу вибору Рівня організація повинна розглянути свою поточну практику управління ризиками, навколишнє середовище загроз, юридичні та нормативні вимоги, цілі бізнесу/місії та організаційні обмеження.
- *Профіль Платформи* ("Профіль") представляє результати, виходячи з потреб бізнесу, які організація обрала з Категорій та Підкатегорій платформи. Профіль може бути охарактеризований як приведення стандартів, керівних вказівок та практик у відповідність з Основою платформи у конкретному сценарії реалізації. Профілі можуть використовуватися для визначення можливостей для поліпшення концепції кібербезпеки шляхом порівняння «Поточного» Профілю (стан «Як є») з «Цільовим» Профілем (стан «як повинно бути»). Для розробки Профілю організація може переглянути всі Категорії та Підкатегорії, і, виходячи з рушійних сил бізнесу/місії та оцінки ризику, визначити, які з них найбільш важливі; вона може додати Категорії та Підкатегорії, якщо це необхідно. для усунення ризиків організації. Поточний профіль може використовуватися для підтримки пріоритетних завдань та вимірювання прогресу досягнення Цільового профілю, а також для факторингу інших бізнес-потреб, включаючи економічну ефективність та інновації. Профілі можуть використовуватися для проведення самооцінки та спілкування в рамках організації або між організаціями.

1.2 Управління ризиками та Платформа кібербезпеки

Управління ризиками - це постійний процес визначення, оцінки та реагування на ризик. Щоб керувати ризиками, організаціям слід розуміти ймовірність того, що подія відбудеться, і її потенційні наслідки. За допомогою цієї інформації організації можуть визначити прийнятний рівень ризику для досягнення своїх організаційних цілей і можуть виразити це як свою стійкість до ризику.

З розумінням стійкості до ризику організації можуть визначати пріоритетність діяльності в галузі кібербезпеки, що дозволяє організаціям приймати обґрунтовані рішення щодо витрат на кібербезпеку. Реалізація програм управління ризиками пропонує організаціям можливість кількісно оцінювати та вносити коригування до своїх програм кібербезпеки. Організації можуть приймати різні підходи до управління ризиком, включаючи пом'якшення ризику, передачу ризику, уникнення ризику або прийняття ризику, залежно від потенційного впливу на надання критичних послуг. Платформа використовує процеси управління ризиками, що дозволяє організаціям інформувати та визначати пріоритетні рішення щодо забезпечення кібербезпеки. Вона підтримує повторювані оцінки ризиків та перевірку рушійних сил бізнесу, щоб допомогти організаціям обирати цільові стани для діяльності з кібербезпеки, що відображає бажані результати. Таким чином, Платформа надає організаціям можливість динамічно обирати та направляти вдосконалення управління ризиками для кібербезпеки для

середовищ IT та ICS.

Платформа може адаптуватися для забезпечення гнучкої та ризик-орієнтованої реалізації, яка може використовуватися з широким спектром процесів управління ризиком для кібербезпеки. Приклади процесів управління ризиком для кібербезпеки включають стандарт Міжнародної організації стандартизації (ISO) 31000:2009[6], стандарт ISO/Міжнародної електротехнічної комісії (IEC) 27005:2011[7], Спеціальну публікацію (SP) NIST (SP) 800-39[8] та *Керівні принципи процесу управління ризиком для кібербезпеки в підсекторі електроенергії* (RMP)[9].

1.3 Короткий огляд документа

Решта цього документа містить наступні розділи та додатки:

- Розділ 2 описує компоненти Платформи: Основу, Рівні і Профілі платформи.
- У Розділі 3 наведено приклади використання Платформи.
- Розділ 4 описує, як використовувати Платформу для самооцінки та демонстрації кібербезпеки за допомогою вимірювань.
- Додаток A представляє Основу платформи в табличному форматі: Функції, Категорії, Підкатегорії та Інформаційні посилання.
- Додаток B містить Словник термінів вибраних термінів.
- Додаток C містить перелік скорочень, що використовуються в цьому документі.

[6] Міжнародна організація стандартизації, управління ризиками - *Принципи та керівні принципи*, ISO 31000:2009, 2009. http://www.iso.org/iso/home/standards/iso31000.htm

[7] Міжнародна організація стандартизації / Міжнародна електротехнічна комісія, *Інформаційні технології - Технології безпеки - Управління ризиками інформаційної безпеки*, ISO/IEC 27005:2011, 2011. https://www.iso.org/standard/56742.html

[8] Спільна ініціатива з трансформації цільової групи, *Управління ризиком інформаційної безпеки: інформація про організацію, місію та інформаційну систему*, спеціальна публікація NIST 800-39, https://doi.org/10.6028/NIST.SP.800- 39

[9] Міністерство енергетики США, *Керівні принципи процесу управління ризиком кібербезпеки в підсекторі електроенергії*, DOE/OE-0003, травень 2012 р. https://energy.gov/sites/prod/files/Cybersecurity Risk Management Process Guideline - Final - May 2012.pdf

2.0 Загальна характеристика Платформи

Платформа забезпечує спільну мову для розуміння, управління та вираження ризику для кібербезпеки для внутрішніх та зовнішніх зацікавлених сторін. Вона може використовуватися для того, щоб допомогти визначати та встановлювати пріоритетні заходи щодо зниження ризику для кібербезпеки і є інструментом для узгодження політичних, ділових та технологічних підходів до управління цим ризиком. Вона може використовуватися для управління ризиком для кібербезпеки в усій організації або може зосереджуватися на наданні важливих послуг в рамках організації. Різні типи організацій, включаючи сектор, який координує структури, асоціації та організації, можуть використовувати Платформу для різних цілей, включаючи створення загальних Профілів.

2.1 Основа платформи

Основа платформи провадить комплекс заходів для досягнення конкретних *результатів* кібербезпеки та посилання на приклади керівних принципів для досягнення цих результатів. Основа не є контрольним списком для дій. Вона представляє основні результати в галузі кібербезпеки, визначені зацікавленими сторонами як корисні для управління ризиком для кібербезпеки. Основа містить чотири елементи: Функції, Категорії, Підкатегорії та Інформаційні посилання, наведені на **Рисунку 1**:

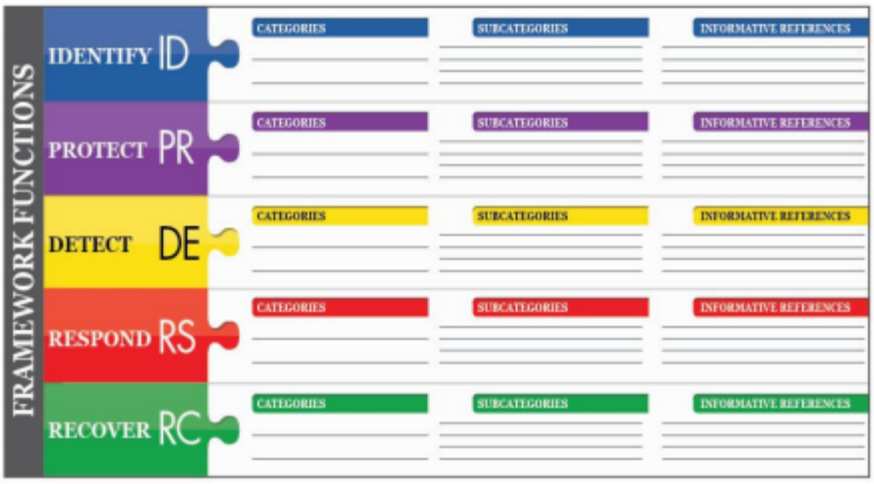

Рисунок 1. Структура Основи платформи

(* framework functions – функції Платформи; identify – визначення; protect – захист; detect - виявлення; respond - реагування; recover - відновлення; categories - Категорії; subcategories - Підкатегорії; informative references – інформаційні посилання).

Елементи Основи платформи працюють разом, як вказано нижче:

- **Функції** організують основну діяльність з кібербезпеки на найвищому рівні. Ці Функції - Ідентифікація, Захист, Виявлення, Реагування та Відновлення. Вони допомагають організації формулювати управління ризиком для кібербезпеки, організуючи інформацію,

робити можливими рішення управління ризиком, займатися загрозами та удосконалювати, засвоюючи уроки попередньої діяльності. Функції також узгоджуються з існуючими методологіями для управління інцидентами і допомагають демонструвати вплив інвестицій на кібербезпеку. Наприклад, інвестиції в планування та тренування підтримують дії своєчасного реагування і відновлення, знижуючи вплив на надання послуг.]

- **Категорії** поділяють Функцію на групи результатів кібербезпеки, які тісно пов'язані з програмними потребами та окремими видами діяльності. Приклади Категорій включають "Управління активами", "Управління ідентифікацією та контроль доступу" та "Процеси виявлення".
- **Підкатегорії** далі поділяють Категорію на конкретні результати технічної та/або управлінської діяльності. Вони забезпечують набір результатів, які, хоча і не є вичерпними, допомагають підтримувати досягнення результатів у кожній Категорії. Приклади Підкатегорій включають "Зовнішні інформаційні системи каталогізовано", "Дані, що зберігаються, захищено" та "Сповіщення від систем виявлення розслідуються".
- **Інформаційні посилання** - це конкретні розділи стандартів, керівних принципів та практик, що є загальними для секторів критично важливих інфраструктур, які ілюструють метод досягнення результатів, пов'язаних із кожною Підкатегорією. Інформаційні посилання, представлені в Основі платформи, є ілюстративними, а не вичерпними. Вони базуються на міжгалузевих керівних принципах, найчастіше згаданих під час процесу розробки Платформи.

Нижче наведено п'ять Функцій основи Платформи. Ці Функції не призначені для формування послідовного шляху або приведення до статичного бажаного кінцевого стану. Скоріше, Функції повинні виконуватися одночасно та безперервно для формування операційної культури, яка стосується динамічного ризику для кібербезпеки. Див. Додаток А для повного переліку Основи платформи.

- **Ідентифікація** - Розробити організаційне розуміння для управління ризиком для кібербезпеки для систем, людей, активів, даних та можливостей.

  Діяльність в рамках Функції ідентифікації є основою для ефективного використання Платформи. Розуміння бізнес-контексту, ресурсів, що підтримують критичні функції та пов'язані з ними ризики для кібербезпеки, дозволяють організації зосередити зусилля та визначати їх пріоритети відповідно до її стратегії управління ризиками та бізнес-потреб. Приклади Категорій результатів, отриманих в рамках цієї Функції, включають Управління активами, Бізнес-середовище, Врядування, Оцінку ризиків і Стратегію управління. ризиками.

- **Захист** - Розробити та запровадити відповідні гарантії для забезпечення надання критично важливих послуг.

  Функція Захист підтримує можливість обмежувати або стримувати вплив потенційної події кібербезпеки. Приклади Категорій результатів в рамках цієї Функції включають Управління ідентифікацією та контроль доступу, Усвідомлення та тренування, Безпеку даних, Процеси та процедури захисту інформації, Технічне обслуговування і Захисні технології.

- **Виявлення** - Розробити та здійснити відповідні заходи для ідентифікації події кібербезпеки.

Функція Виявлення дозволяє своєчасно виявляти події кібербезпеки. Приклади результатів Категорії в межах цієї функції включають Аномалії та події, Безперервний моніторинг безпеки і Процеси виявлення.

- **Реагування** - Розробити та впровадити відповідні види діяльності для вжиття заходів щодо виявленого інциденту кібербезпеки.

  Функція Реагування підтримує здатність стримувати вплив потенційного інциденту з кібербезпеки. Приклади Категорій результатів в рамках цієї Функції включають Планування реагування, Комунікації, Аналіз, Пом'якшення наслідків та Вдосконалення.

- **Відновлення** - Розробити та здійснити відповідні заходи для підтримки планів стійкості та відновлення будь-яких можливостей або послуг, які були порушені внаслідок інциденту з кібербезпеки.

  Функція Відновлення підтримує своєчасне відновлення нормальних операцій, щоб зменшити вплив інциденту кібербезпеки. Приклади Категорій результатів, отриманих в рамках цієї Функції, включають Планування відновлення, Вдосконалення і Комунікації.

2.2 Рівні впровадження Платформи

Рівні впровадження Платформи ("Рівні") забезпечують контекст того, як організація розглядає ризик для кібербезпеки та процеси, які використовуються для управління цим ризиком. Починаючи від Часткового (Рівень 1) до Адаптивного (Рівень 4), Рівні описують зростаючу ступінь суворості та складності в практиці управління ризиками для кібербезпеки. Вони допомагають з'ясувати, в якій мірі управління ризиками для кібербезпеки поінформоване про потреби бізнесу і інтегрується в загальну практику організації по управлінню ризиками. Міркування з управління ризиками включають багато аспектів кібербезпеки, включаючи ступінь інтеграції міркувань конфіденційності та громадянських свобод в управління організацією ризиками для кібербезпеки та можливих реагувань на ризики.

Процес вибору Рівня враховує поточну практику управління ризиками організації, навколишнє середовище загроз, юридичні та регуляторні вимоги, практику обміну інформацією, цілі бізнесу/місії, вимоги кібербезпеки ланцюжків поставок та організаційні обмеження. Організація повинна визначити бажаний Рівень, забезпечити, що обраний рівень відповідає організаційним цілям, може бути впроваджений та знижує ризик для кібербезпеки для критичних активів та ресурсів до рівнів, прийнятних для організації. Організаціям слід розглянути використання зовнішніх рекомендацій, отриманих від федеральних урядових департаментів та агентств, Центрів обміну та аналізу інформації (ISAC), Організацій з обміну та аналізу інформації (ISAO), існуючих моделей зрілості або інших джерел, які допоможуть визначити бажаний для них рівень.

Хоча організаціям, визначеним як Рівень 1 (Частковий), рекомендується розглянути питання про перехід до Рівня 2 або вище, Рівні не відображають рівнів зрілості. Рівні призначені для підтримки прийняття організаційних рішень про те, як керувати ризиком для кібербезпеки, а також про те, які аспекти організації мають вищий пріоритет і можуть отримати додаткові ресурси. Перехід до вищих Рівнів рекомендується, коли аналіз економічної ефективності свідчить про здійсненне та економічно ефективне зниження ризику для кібербезпеки.

Успішне впровадження Платформи базується на досягненні результатів, описаних у Цільовому(их) профілі(ях) організації, а не на визначенні Рівнів. Тим не менш, вибір і

призначення Рівня, природно, впливає на Профілі платформи. Рекомендації щодо Рівня від керівників Рівня бізнесу/процесу, затверджені Рівнем старшого керівництва, допоможуть встановити загальний тон того, як буде впроваджено управління ризиком для кібербезпеки в організації, а також повинні впливати на визначення пріоритетів у межах Цільового профілю та оцінку прогресу в усуненні прогалин.

Визначення Рівнів такі:

Рівень 1: Частковий

- *Процес управління ризиками* - Організаційна практика управління ризиками для кібербезпеки не формалізована; управління ризиками здійснюється ситуативним, а часом і реактивним способом. Інформація для визначення пріоритетів у діяльності з кібербезпеки може не буде доступна безпосередньо з організаційних цілей управління ризиками, середовища загрози або вимог бізнесу/місії.
- *Інтегрована програма управління ризиками* – Знання ризику для кібербезпеки на організаційному рівні обмежене. Організація впроваджує управління ризиками для кібербезпеки нерегулярно, залежно від конкретного випадку, через різноманітний досвід або інформацію, отриману зі сторонніх джерел. Організація може не мати процесів, які дозволяють спільно використовувати інформацію про кібербезпеку в організації.
- *Зовнішня участь* - Організація не розуміє своєї ролі в більшій екосистемі як щодо її залежних осіб, так і щодо залежних об’єктів. Організація не співпрацює з іншими організаціями (наприклад, покупцями, постачальниками, залежними особами, залежними об’єктами, ISAO, дослідниками, урядами), а також не отримує та не ділиться інформацією (наприклад, інформацією про загрозу, найкращі практики, технології). В цілому, організація не знає про кібер-ризики для ланцюжків поставок щодо продуктів та послуг, які вона надає і які вона використовує.

Рівень 2: Ризик-орієнтований

- *Процес управління ризиками* - Практика управління ризиками затверджена керівництвом, але може не встановлена як організаційна політика. Інформація для визначення пріоритетів діяльності з кібербезпеки та потреб захисту безпосередньо отримується з організаційних цілей управління ризиками, навколишнього середовища загрози або вимог бізнесу/місії.
- *Інтегрована програма управління ризиками* - Існує усвідомлення ризику для кібербезпеки на організаційному рівні, але загально-організаційний підхід до управління ризиком для кібербезпеки не встановлено. Інформація про кібербезпеку поширюється всередині організації на неформальній основі. Розгляд кібербезпеки в організаційних цілях та програмах може відбуватися на деяких, але не на всіх рівнях організації. Оцінка кібер-ризиків для організаційних та зовнішніх активів відбувається, але зазвичай не повторюється або не проводиться знову.
- *Зовнішня участь* - Взагалі, організація розуміє свою роль у більшій екосистемі як щодо власних залежностей, так і для залежних осіб, але не обох. Організація співпрацює з іншими організаціями та отримує певну інформацію від інших організацій, а також створює певну свою інформацію, але може ділитися інформацією з іншими. Крім того, організація усвідомлює кібер-ризики для ланцюжків поставок, пов'язані з продуктами та послугами, які вона надає та використовує, але не діє послідовно чи формально щодо цих ризиків.

Рівень 3: Повторюваний

- *Процес управління ризиками* - Практика управління ризиками організації офіційно схвалена та виражена як політика. Організаційна практика кібербезпеки регулярно оновлюється на основі застосування процесів управління ризиками до змін у вимогах бізнесу/місії та змінного ландшафту загроз і технології.
- *Інтегрована програма управління ризиками* - Існує загально-організаційний підхід до управління ризиками для кібербезпеки. Ризик-орієнтовані політика, процеси та процедури визначаються, виконуються як передбачено та переглядаються. Послідовно застосовуються методи ефективного реагування на зміни ризику. Персонал володіє знаннями та навичками для виконання своїх призначених ролей та обов'язків. Організація послідовно і точно контролює ризики для кібербезпеки для організаційних активів. Вище керівництво з питань кібербезпеки та керівництво, не пов’язане з питаннями кібербезпеки, регулярно обмінюються інформацією про проблеми, пов’язані з ризиком для кібербезпеки. Вищі керівники забезпечують врахування кібербезпеки у всіх напрямках діяльності в організації.
- *Зовнішня участь* - Організація розуміє свою роль, залежних осіб та залежних об’єктів у більшій екосистемі та може сприяти широкому розумінні ризиків громадою. Вона співпрацює та регулярно отримує інформацію від інших організацій, що доповнює внутрішньо сформовану інформацію, та ділиться інформацією з іншими суб'єктами. Організація усвідомлює кібер-ризики для ланцюжків поставок, пов'язані з продуктами та послугами, які вона надає і які вона використовує. Окрім того, вона зазвичай діє формально щодо цих ризиків, включаючи механізми, такі як письмові договори для передачі базових вимог, структури управління (наприклад, ради з питань управління ризиками) та впровадження політики та моніторингу.

Рівень 4: Адаптивний

- *Процес управління ризиками* - Організація адаптує свої технології кібербезпеки на основі попередньої та поточної діяльності з кібербезпеки, включаючи досвід та прогнозні показники. Завдяки процесу безперервного вдосконалення, що включає передові технології та практику кібербезпеки, організація активно адаптується до мінливого ландшафту загроз ї технології та своєчасно та ефективно реагує на виникаючі складні загрози.
- *Інтегрована програма управління ризиками* - Існує загально-організаційний підхід до управління ризиками для кібербезпеки, який використовує інформацію про ризики, процеси та процедури для подолання можливих подій, пов'язаних із кібербезпекою. Зв'язок між ризиком для кібербезпеки та організаційними цілями чітко розуміється та враховується при прийнятті рішень. Вище керівництво контролює ризики для кібербезпеки в тому ж контексті, що й фінансовий ризик та інші організаційні ризики. Бюджет організації базується на розумінні поточного та передбачуваного ризику та стійкості до ризику. Бізнес-підрозділи реалізують виконавче бачення та аналізують ризики системного рівня в контексті стійкості організації до ризиків. Управління ризиками для кібербезпеки є частиною організаційної культури та розвивається з усвідомлення попередньої діяльності та постійної обізнаності про діяльність у своїх системах та мережах. Організація може швидко та ефективно враховувати зміни в цілях бізнесу/місії щодо підходу до ризику і повідомлення про нього.
- *Зовнішня участь* - Організація розуміє свою роль, залежних осіб та залежних об’єктів у великій екосистемі та сприяє більш широкому розумінню ризиків громадою. Вона

отримує, генерує та переглядає пріоритетну інформацію, що забезпечує безперервний аналіз її ризиків при зміні ландшафтів загроз та технології. Організація ділиться цією інформацією всередині та зовні з іншими співробітниками. Організація використовує інформацію в режимі реального або майже реального часу, щоб розуміти і послідовно діяти при виникненні кібер-ризиків для ланцюжків поставок, пов'язаних з продуктами та послугами, які вона надає і які вона використовує. Окрім того, вона активно спілкується, використовуючи формальні (наприклад, угоди) та неформальні механізми для розвитку та підтримки надійних зв'язків ланцюжків поставок.

2.3 Профіль платформи

Профіль платформи ("Профіль") - це приведення функцій, Категорій та Підкатегорій у відповідність з бізнес-вимогами, стійкістю до ризику та ресурсами організації. Профіль дозволяє організаціям створювати дорожню карту для зниження ризику для кібербезпеки, яка добре узгоджується з організаційними та галузевими цілями, враховує юридичні/ регуляторні вимоги та найкращі практики в галузі та відображає пріоритети управління ризиками. Враховуючи складність багатьох організацій, вони можуть прийняти рішення мати кілька Профілів, узгоджених з окремими компонентами, враховуючи їхні індивідуальні потреби.

Профілі платформи можуть використовуватися для опису поточного стану або бажаного цільового стану конкретних заходів з кібербезпеки. Поточний профіль вказує результати кібербезпеки, які досягнуті на даний час. Цільовий профіль показує результати, необхідні для досягнення бажаних цілей управління ризиком для кібербезпеки. Профілі підтримують вимоги бізнесу/місії та допомагають у повідомленні про ризик всередині та між організаціями. Ця Платформа не встановлює шаблони Профілю, що забезпечує гнучкість у реалізації.

Порівняння Профілів (наприклад, Поточного профілю та Цільового профілю) може виявити прогалини, які необхідно усунути для досягнення цілей управління ризиком для кібербезпеки. План дій щодо усунення цих прогалин для виконання даної Категорії або Підкатегорії може сприяти дорожній карті, описаній вище. Визначення пріоритетів у зменшенні прогалин обумовлюється бізнес-потребами організації та процесами управління ризиками. Цей підхід, що ґрунтується на оцінці ризику, дає змогу організації оцінювати необхідні ресурси (наприклад, кадрове забезпечення, фінансування) для досягнення поставлених цілей з кібербезпеки економічним та пріоритетним чином. Крім того, Платформа є ризик-орієнтованим підходом, в якому застосовність і виконання даної Підкатегорії залежить від обсягу Профілю.

2.4 Координування впровадження Платформи

На **Рисунку 2** описано загальний потік інформації та рішень на наступних рівнях в межах організації:

- Вище керівництво
- Бізнес/процеси
- Впровадження/операції

Рівень вищого керівництва повідомляє про пріоритети місії, наявні ресурси та загальну стійкість до ризиків на рівні бізнесу/процесу. Рівень бізнесу/процесів використовує інформацію як вхідні дані в процесі управління ризиками, а потім співпрацює з рівнем

впровадження/операцій, щоб повідомити про потреби бізнесу та створити Профіль. Рівень впровадження/операцій повідомляє про прогрес впровадження Профілю рівню бізнесу/процесів. Рівень бізнесу/процесів використовує цю інформацію для проведення оцінки впливу. Рівень бізнесу/процесів звітує про результати цієї оцінки впливу рівню вищого керівництва, щоб інформувати про загальний процес організації управління ризиками та рівню впровадження/операцій для усвідомлення впливу на бізнес.

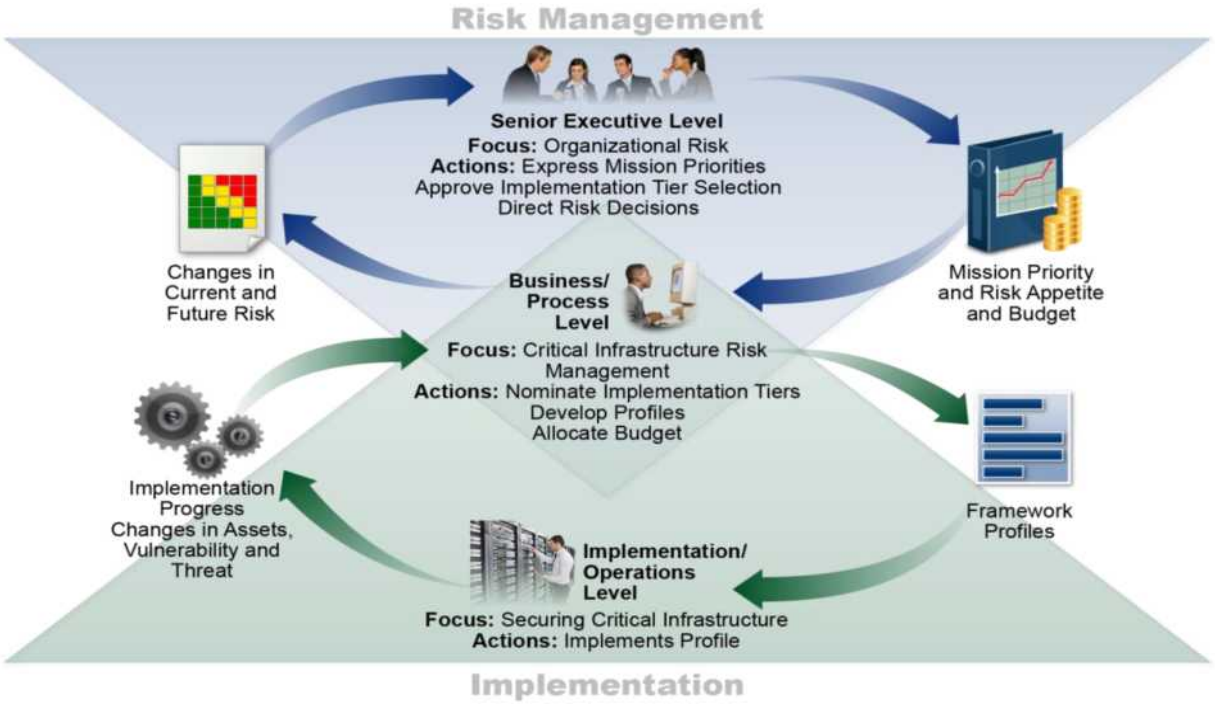

Рисунок 2: Умовні інформаційні потоки та потоки рішень в організації

(*Risk Management – управління ризиком. Implementation – впровадження.
*Senior Executive Level – рівень старшого керівництва; focus - акцент; organizational risk – організаційний ризик; actions - дії; express mission priorities –формулювання пріоритетів місії; approve implementation tier selection – затвердження вибору рівня впровадження; direct risk decision – визначення рішень щодо ризику.
*Changes in Current and Future Risk – зміни наявного та майбутнього ризику.
*Implementation progress – прогрес впровадження; Changes in Assets, Vulnerability and Threat – зміна активів, вразливих ланок та загроз.
*Business/process level – рівень бізнесу/процесів; Focus - акцент; Critical Infrastructure Risk Management – управління ризиками критично важливих інфраструктур; Actions - дії; Nominate Implementation Tiers – призначити рівні впровадження; Develop Profiles – розробити Профілі; Allocate Budget – розподілити бюджет.
* Implementation/Operations level - рівень впровадження/операцій; Focus - акцент; Securing Critical Infrastructure - захист об'єктів важливих інфраструктур; Actions - дії; Implements Profile – впроваджує Профіль.
*Mission Priority and Risk Appetite and Budget – пріоритет місії/стійкість до ризику та бюджет.
*Framework profiles – Профілі платформи).

3.0 Як користуватися Платформою

Організація може використовувати Платформу як ключову частину свого систематичного процесу для визначення, оцінки та управління ризиком для кібербезпеки. Платформа не призначена для заміни існуючих процесів; організація може використовувати свій поточний процес і накладати його на Платформу, щоб визначити прогалини у поточному підході до ризику для кібербезпеки та розробити дорожню карту для вдосконалення. Використовуючи

Платформу як інструмент управління ризиком для кібербезпеки, організація може визначати діяльність, яка є найважливішою для надання критично важливих послуг, і визначити пріоритетні видатки для максимізації впливу інвестицій.

Платформа покликана доповнювати існуючі бізнес-операції та операції кібербезпеки. Вона може слугувати основою для нової програми кібербезпеки або механізму вдосконалення існуючої програми. Платформа – це засіб вираження вимог кібербезпеки для ділових партнерів та клієнтів, і вона може допомогти виявити прогалини в практиці організації з кібербезпеки. Вона також містить загальний набір міркувань і процесів для розгляду питань конфіденційності та громадянських свобод у контексті програми для кібербезпеки.

Платформа може застосовуватися протягом етапів життєвого циклу плану, проектування, побудови/купівлі, розгортання, експлуатації та зняття з експлуатації. Фаза плану починає цикл будь-якої системи і закладає основу для всього наступного. Загальні міркування щодо для кібербезпеки повинні бути оголошені та описані якомога чіткіше. План повинен визнати, що ці міркування та вимоги, ймовірно, розвиватимуться протягом решти життєвого циклу. На етапі проектування слід враховувати вимоги до кібербезпеки, як частину більшого міждисциплінарного процесу проектування систем. [10] Ключовою віхою етапу проектування є підтвердження того, що специфікації кібербезпеки системи відповідають потребам та стійкості організації до ризику, як це було відображено у Профілі платформи. Бажані результати кібербезпеки, визначені як пріоритет у Цільовому профілі, повинні бути включені a) при розробці системи під час фази побудови; b) під час придбання або аутсорсингу системи на етапі покупки. Цей самий Цільовий профіль служить як перелік функцій системи кібербезпеки, які слід оцінювати під час розгортання системи для перевірки реалізації всіх функцій. Результати кібербезпеки, визначені за допомогою Платформи, повинні служити основою для постійної роботи системи. Це включає періодичну переоцінку, фіксацію результатів у Поточному профілі, щоб перевірити виконання вимог до кібербезпеки. Як правило, складна мережа залежностей (наприклад, компенсації та спільного контролю) між системами означає, що результати, задокументовані у Цільових профілях відповідних систем, необхідно ретельно розглянути при виведенні систем з експлуатації.

У наступних розділах представлені різні способи, в яких організації можуть користуватися Платформою.

3.1 Основний огляд практики кібербезпеки

Платформа може використовуватися для порівняння поточних заходів діяльності організації з кібербезпеки з тими, що викладені в Основі платформи. Завдяки створенню Поточного профілю організації можуть перевірити, в якій мірі вони досягають результатів, описаних у Категоріях та Підкатегоріях основи, відповідно до п'яти Функцій високого рівня: Ідентифікація, Захист, Виявлення, Реагування та Відновлення. Організація може виявити, що вона вже досягла бажаних результатів, тим самим керуючи кібербезпекою відповідно до відомих ризиків. Альтернативно, організація може визначити, що вона має можливості для (або потребує) вдосконалення. Організація може використовувати цю інформацію для розробки плану дій для посилення існуючої практики кібербезпеки та зменшення ризику для кібербезпеки. Організація також може виявити, що вона вкладає занадто багато для досягнення певних результатів. Організація може використовувати цю інформацію для

[10] Спеціальна публікація NIST 800-160, том 1, *Інжиніринг системи безпеки, міркування для багатоПрофільного підходу в розробці надійних безпечних систем*, Росс та інш., листопад 2016 р. (Оновлено 21 березня 2018 р.), https://doi.org/10.6028/NIST.SP.800-160v1

переорієнтації пріоритетності ресурсів.

Хоча вони не замінюють процес управління ризиками, ці п'ять Функцій високого рівня забезпечують короткий шлях для вищих керівників та інших осіб, щоб розібрати фундаментальні концепції ризику для кібербезпеки, щоб вони могли оцінити, яким чином здійснюється управління визначеними ризиками і як їхня організація порівнюється на високому рівні з існуючими стандартами, керівними принципами та практиками кібербезпеки. Платформа також може допомогти організації відповісти на основні питання, включаючи "Як у нас справи?". Тоді можна більш інформовано просувати свої практики кібербезпеки, де і коли організація вважатиме це необхідним.

3.2 Встановлення або вдосконалення програми кібербезпеки

Наступні кроки показують, як організація могла б використовувати Платформу для створення нової програми кібербезпеки або вдосконалення існуючої програми. Ці кроки слід повторювати, як необхідно, для постійного підвищення кібербезпеки.

Крок 1. Визначення пріоритетів та сфери застосування. Організація визначає свої цілі бізнесу/місії та організаційні пріоритети на високому рівні. За допомогою цієї інформації організація приймає стратегічні рішення щодо реалізації кібербезпеки та визначає обсяг систем та активів, які підтримують обраний напрям діяльності або процес. Платформа може бути адаптована для підтримки різних напрямів діяльності або процесів в рамках організації, яка може мати різні бізнес-потреби та пов'язані стійкості до ризику. Стійкості до ризику можуть відображатися у цільовому Рівні впровадження.

Крок 2. Орієнтування. Після визначення сфери застосування програми кібербезпеки для напряму діяльності або процесу, організація визначає відповідні системи та активи, нормативні вимоги та загальний підхід до ризику. Потім організація консультується з джерелами для визначення загроз та вразливостей, що застосовуються до цих систем та активів.

Крок 3. Створіть Поточний профіль. Організація розробляє Поточний профіль, вказуючи, яких результатів Категорій та Підкатегорій з Основи платформи досягнуто. Якщо результат частково досягнутий, зазначення цього факту допоможе підтримати наступні кроки шляхом надання базової інформації.

Крок 4: Проведення оцінки ризику. Ця оцінка може регулюватися загальним процесом управління ризиками організації або попередніми заходами з оцінки ризиків. Організація аналізує операційне середовище, щоб визначити вірогідність події, пов’язаної з кібербезпекою, та наслідки, які ця подія може мати для організації. Важливо, щоб організації визначали нові ризики та використовували інформацію про вірусні загрози від внутрішніх та зовнішніх джерел, щоб краще зрозуміти вірогідність та наслідки подій, пов'язаних із кібербезпекою.

Крок 5: Створення Цільового профілю. Організація створює Цільовий профіль, орієнтований на оцінку. Категорій та Підкатегорій Платформи, що описують бажані результати кібербезпеки організації. Організації також можуть розробити власні додаткові Категорії та Підкатегорії з урахуванням унікальних організаційних ризиків. При створенні Цільового профілю організація може також розглянути впливи та вимоги зовнішніх зацікавлених сторін, таких як суб'єкти господарювання в галузі, клієнти та ділові партнери. Цільовий профіль повинен належним чином відображати критерії в рамках цільового Рівня

впровадження.

Крок 6. Визначення, аналіз та пріоритизація прогалин. Організація порівнює поточний Профіль з Цільовим профілем для визначення прогалин. Далі, вона створює у Цільовому профілі пріоритетний план дій для усунення прогалин, що відображає рушійні сили місії, витрати та переваги, а також ризики, для досягнення результатів. Потім організація визначає ресурси, включаючи фінансування та робочу силу, необхідні для подолання прогалин. Використання Профілів таким способом спонукає організацію приймати обґрунтовані рішення щодо діяльності з кібербезпеки, підтримує управління ризиками та дає змогу організації здійснювати економічно ефективні цільові вдосконалення.

Крок 7. Реалізація плану дій. Організація визначає, які дії потрібно вжити для усунення прогалин, якщо такі є, визначені на попередньому кроці, а потім налаштовує поточну практику кібербезпеки для досягнення Цільового профілю. Для подальшого керівництва Платформа ідентифікує приклади Інформаційних посилань щодо Категорій та Підкатегорій, але організації повинні визначати, які стандарти, керівні принципи та практики, включаючи ті, що є конкретними для сектора, найкраще працюють на їхні потреби.

Організація повторює кроки, необхідні для постійної оцінки та вдосконалення своєї кібербезпеки. Наприклад, організації можуть виявити, що частіше повторення етапу орієнтації покращує якість оцінки ризиків. Крім того, організації можуть стежити за прогресом через ітеративні оновлення Поточного профілю, а потім порівнювати Поточний профіль з Цільовим профілем. Організації також можуть використовувати цей процес, щоб привести свою програму кібербезпеки у відповідність з бажаним Рівнем реалізації Платформи.

3.3 Повідомлення зацікавленим сторонам про вимоги щодо кібербезпеки

Платформа забезпечує загальну мову для обміну вимогами між взаємозалежними зацікавленими сторонами, відповідальними за доставку важливих продуктів та послуг критично важливих інфраструктур. Приклади включають:

- Організація може використовувати Цільовий профіль для вираження вимог щодо управління ризиком для кібербезпеки для зовнішнього постачальника послуг (наприклад, постачальника хмари, до якої він експортує дані).
- Організація може відобразити свій стан кібербезпеки через Поточний профіль, щоб повідомити про результати або порівняти з вимогами щодо придбання.
- Власник/оператор критичної інфраструктури, визначивши зовнішнього партнера, від котрого залежить ця інфраструктура, може використовувати Цільовий профіль, щоб передати необхідні Категорії та Підкатегорії.
- Сектор критично важливих інфраструктур може створити Цільовий профіль, який може бути використаний серед його складових як початковий Профіль базової лінії, щоб створити свої спеціальні Цільові профілі.
- Організація може краще керувати ризиками для кібербезпеки серед зацікавлених сторін, оцінюючи їхню позицію в критично важливій інфраструктурі та більш широку цифрову економіку, використовуючи Рівні впровадження.

Комунікація особливо важлива серед зацікавлених сторін впродовж усіх ланцюжків поставок. Ланцюжки поставок являють собою складні, глобально розподілені та взаємопов'язані набори ресурсів і процесів між різними рівнями організації. Ланцюжки поставок починаються з джерел постачання продуктів і послуг і включають розробку, виробництво, обробку, оперування та доставку продуктів і послуг кінцевому користувачеві. Враховуючи ці складні та взаємопов'язані відносини, управління ризиками ланцюжків поставок (SCRM) є критичною організаційною функцією. [11]

Кібер-SCRM - це набір заходів, необхідних для управління ризиком для кібербезпеки, пов'язаним із зовнішніми сторонами. Більш конкретно, кібер-SCRM розглядає як ефект для кібербезпеки, який має організація для зовнішніх учасників, так і ефект для кібербезпеки, який зовнішні сторони мають для організації.

Основна мета кібер-SCRM полягає у визначенні, оцінці та пом'якшенні "продуктів і послуг, які можуть містити потенційно шкідливу функціональність, які є підробленими або вразливими через неякісну практику виробництва та розробки в системі кібер-ланцюжків поставок[12]". Заходи кібер-SCRM можуть включати:

- Визначення вимог до кібербезпеки для постачальників,
- Застосування вимог до кібербезпеки за допомогою формальної угоди (напр., контрактів);
- Повідомлення постачальникам, яким чином будуть перевірені та підтверджені ці вимоги до кібербезпеки.
- Перевірку того, що вимоги до кібербезпеки виконуються за допомогою різних методологій оцінки, та
- Управління та керівництво зазначеними заходами.

Як показано на Рисунку 3, кібер-SCRM охоплює постачальників і покупців технологій, а також постачальників та покупців, не пов’язаних з технологіями, де технологія мінімально складається з інформаційних технологій (IT), промислових систем управління (ICS), кібер-фізичних систем (CPS), а також пов'язаних пристроїв в цілому, включаючи Інтернет речей (IoT). На рисунку 3 зображено організацію в один момент часу. Проте, через звичайний бізнес-процес більшість організацій будуть як постачальниками початкової продукції, так і покупцями переробленої продукції у відношенні до інших організацій або кінцевих користувачів.

[11] Повідомлення про вимоги до кібербезпеки (Розділ 3.3) та рішення щодо покупки (Розділ 3.4) стосуються лише двох способів використання Платформи для кібер-SCRM та не мають на меті повноцінно розглядати кібер-SCRM.

[12] Спеціальна публікація 800-161 *Практика управління ризиком ланцюжків поставок для Федерльних інформаційних систем та організацій*, Бойенс та інш., квітень 2015 р., https://doi.org/10.6028/NIST.SP.800-161

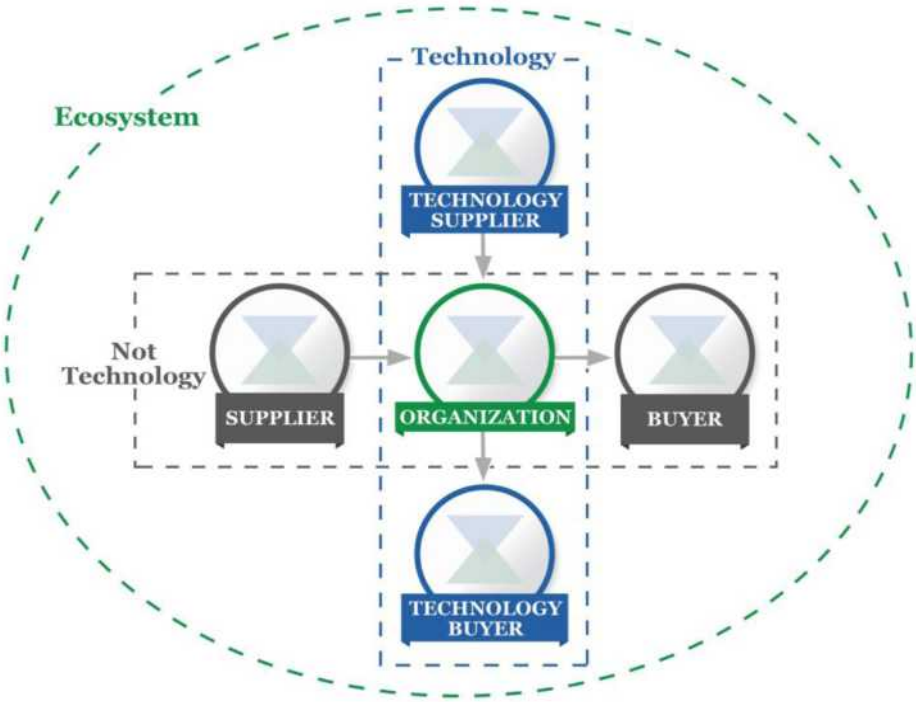

Рисунок 3: Зв'язки у кібер-ланцюжку поставок

(*Ecosystem - екосистема; technology -технологія; not technology – не технологія; technology supplier – постачальник технології; supplier - постачальник; organization -організація ; buyer - покупець; technology buyer – покупець технології)

Сторони, описані на Рисунку 3, складають екосистему кібербезпеки організації. Ці відносини підкреслюють вирішальну роль кібер-SCRM в усуненні ризику для кібербезпеки в критично важливій інфраструктурі та більш широкій цифровій економіці. Ці відносини, продукти та послуги, які вони надають, і ризики, які вони представляють, необхідно врахувати у можливостях організації щодо захисту та виявлення, а також в їхніх протоколах реагування та відновлення.

На Рисунку вище "Покупець" відноситься до людей або організацій, які споживають певний продукт або послугу від організації, включаючи як комерційні, так і некомерційні організації. "Постачальник" охоплює виробників і постачальників послуг, які використовуються для внутрішніх цілей організації (наприклад, IT-інфраструктури) або інтегровані в продукти або послуги, надані Покупцеві. Ці умови застосовні як до технологічних, так і до нетехнологічних продуктів і послуг.

Якщо розглядати окремі Підкатегорії Основи або всебічні міркування Профілю, Платформа пропонує організаціям та їх партнерам метод, який допоможе забезпечити, що новий продукт чи послуга відповідає критичним результатам в галузі безпеки. Спочатку обираючи результати, що мають відношення до контексту (наприклад, передача персональних ідентифікаційних даних (PII), надання критично важливої послуги, служба перевірки даних, цілісність продукту або послуги), організація може оцінити партнерів за цими критеріями. Наприклад, якщо купується система, яка буде відслідковувати операційну технологію (OT) для аномального мережевого зв'язку, доступність може бути особливо важливою метою кібербезпеки та повинна стимулювати оцінку постачальників технологій у застосовних Підкатегоріях (наприклад, ID.BE-4 , ID.SC-3, ID.SC-4, ID.SC-5, PR.DS-4, PR.DS-6, PR.DS-7, PR.DS-8, PR.IP-1, DE .AE-5).

3.4 Рішення про покупку

Оскільки Цільовий профіль Платформи є пріоритетним переліком організаційних вимог кібербезпеки, Цільові профілі можуть використовуватися для інформування про рішення щодо придбання продуктів та послуг. Ця операція відрізняється від повідомлення зацікавлених сторін щодо вимог кібербезпеки (розглянуто в Розділі 3.3), оскільки може не бути можливо встановити для постачальника цілий комплекс вимог кібербезпеки. Мета повинна полягати в тому, щоб прийняти найкраще рішення про покупку серед декількох постачальників з огляду на ретельно визначений перелік вимог кібербезпеки. Часто це означає певний ступінь компромісу, порівнюючи кілька продуктів або послуг з відомими прогалинами в Цільовому Профілі.

Після придбання продукту або послуги Профіль також може використовуватися для відстеження та вирішення залишкового ризику для кібербезпеки. Наприклад, якщо придбана послуга чи продукт не відповідає всім цілям, описаним у Цільовому профілі, організація може усунути залишковий ризик за допомогою інших заходів керівництва. Профіль також забезпечує організацію методом оцінки того, чи відповідає продукт результатам кібербезпеки, за допомогою механізмів періодичного аналізу та тестування.

3.5 Визначення можливостей для нових або переглянутих Інформаційних посилань

Платформа може використовуватися для визначення можливостей для нових або переглянутих стандартів, керівних принципів або практик, коли додаткові Інформаційні посилання допоможуть організаціям задовольняти нові потреби. Організація, яка впроваджує певну Підкатегорію або розробляє нову Підкатегорію, може виявити, що для відповідної діяльності є мало Інформаційних посилань (якщо такі є). Щоб задовольняти цю потребу, організація може співпрацювати з лідерами технологій та/або органами стандартизації для розробки, складання та узгодження стандартів, керівних принципів або практик.

3.6 Методологія захисту конфіденційності та громадянських свобод

В цьому розділі описується методологія, спрямована на подолання ускладнень щодо конфіденційності приватних осіб та громадянських свобод, які можуть бути результатом кібербезпеки. Ця методологія покликана бути загальним набором міркувань та процесів, оскільки ускладнення щодо конфіденційності та громадянських свобод можуть відрізнятися по секторах або в часі, і організації можуть розглядати ці міркування та процеси з низкою технічних впроваджень. Тим не менш, не всі заходи в програмі для кібербезпеки ставлять під загрозу міркування про конфіденційність та громадянські свободи. Можливо, потрібно буде розробити технічні стандарти конфіденційності, керівні принципи та додаткові найкращі практики для підтримки вдосконалених технічних впроваджень.

Між конфіденційністю та кібербезпекою існує тісний зв'язок. Діяльність організації з кібербезпеки також може створювати ризики для конфіденційності та громадянських свобод, коли персональна інформація використовується, збирається, обробляється, підтримується або розкривається. Деякі приклади включають діяльність з кібербезпеки, яка призводить до надмірного збирання або надмірного збереження персональної інформації, розкриття або використання персональної інформації, не пов'язаної з діяльністю з кібербезпеки, та заходи для пом'якшення наслідків кібербезпеки, які призводять до відмови у наданні послуг або інших подібних потенційно несприятливих наслідках, включаючи деякі види виявлення або моніторингу інцидентів, які можуть заважати свободі вираження поглядів або об'єднання.

Уряд та його агенти відповідають за захист громадянських свобод, що виникають у діяльності з кібербезпеки. Як згадано нижче в методології, уряд або його агенти, які володіють або забезпечують функціонування критично важливих інфраструктур, повинні мати процес, який би підтримував відповідність діяльності з кібербезпеки до діючих законів, норм та конституційних вимог.
Для усунення ускладнень щодо конфіденційності організації можуть враховувати, як їх програма кібербезпеки може включати принципи конфіденційності, такі як мінімізація даних при зборі, розкритті та збереженні матеріалу з персональною інформацією, пов'язаного з інцидентом кібербезпеки, використання обмеження поза діяльністю з кібербезпеки на будь-яку інформацію, спеціально зібрану для діяльності з кібербезпеки, прозорість для певної діяльності з кібербезпеки, індивідуальна згода та відшкодування за несприятливі наслідки, пов'язані з використанням персональної інформації в діяльності з кібербезпеки, якість даних, цілісність та безпека, і підзвітність та аудит.

Коли організації оцінюють Основу платформи в Додатку А, наступні процеси та дії можуть розглядатися як засіб для вирішення згаданих вище ускладнень щодо конфіденційності та громадянських свобод.

Управління ризиком для кібербезпеки

- Оцінка організацією ризику для кібербезпеки та можливих відповідей на ризик розглядає аспекти конфіденційності її програми кібербезпеки.
- Особи, відповідальні за конфіденційність, пов'язану з кібербезпекою, звітують перед відповідним керівництвом і отримують відповідну підготовку.
- Впроваджено процес підтримки відповідності діяльності з кібербезпеки відповідним законам, нормам і конституційним вимогам.
- Запроваджено процес для оцінки виконання вищезазначених організаційних заходів та контролю.

Підходи до ідентифікації, аутентифікації та авторизації осіб для доступу до організаційних активів та систем

- Вжито кроки, спрямовані на виявлення та вирішення ускладнень щодо конфіденційності заходів з управління ідентифікацією та контролю доступу в тій мірі, в якій вони передбачають збір, розкриття або використання персональної інформації.

Заходи з підвищення обізнаності та підготовки

- Інформація про політику конфіденційності, яка застосовується організацією, включена до заходів з підвищення обізнаності та підготовки працівників з кібербезпеки.
- Постачальники послуг, які надають послуги організації, пов'язані з кібербезпекою, інформуються про застосовні політики конфіденційності організації.

Виявлення аномальної діяльності та моніторинг систем та активів

- Впроваджено процес для проведення перевірки конфіденційності аномальної діяльності організації та моніторингу кібербезпеки.

Заходи реагування, включаючи обмін інформацією або інші заходи щодо пом'якшення наслідків

- Впроваджено процес для оцінки та вирішення питання про те, чи, коли, як і в якій мірі

персональна інформація поширюється поза межами організації як частина діяльності по обміну інформацією у рамках кібербезпеки.

- Впроваджено процес для перегляду конфіденційності зусиль організації з кібербезпеки, спрямованих на пом'якшення.

4.0 Самооцінка ризику для кібербезпеки за допомогою Платформи

Платформа кібербезпеки призначена для зниження ризику шляхом покращення управління ризиком для кібербезпеки для цілей організації. В ідеалі, організації, які використовують Платформу, зможуть виміряти та приписати свої ризики разом із вартістю та перевагами заходів, спрямованих на зменшення ризику до прийнятного рівня. Чим краще організація зможе виміряти свій ризик, витрати та переваги стратегій і кроків з кібербезпеки, тим більш раціональним, ефективним і цінним буде її підхід до кібербезпеки та інвестицій.

З часом самооцінка та вимірювання повинні вдосконалити прийняття рішень щодо інвестиційних пріоритетів. Наприклад, вимірювання - або, принаймні, характеристика - аспектів стану кібербезпеки організації та тенденції можуть з часом допомогти такій організації зрозуміти та передати суттєву інформацію про ризик залежним об’єктам, постачальникам, покупцям та іншим сторонам. Організація може виконати це внутрішньо або залучити для оцінки сторонню організацію. Якщо це виконується належним чином і з урахуванням обмежень, ці виміри можуть слугувати базою для надійних довірених відносин як всередині організації, так і поза її межами.

Щоб перевірити ефективність інвестицій, організація спочатку повинна мати чітке розуміння своїх організаційних цілей, взаємозв'язку між цими цілями та підтримуючими результатами кібербезпеки, а також як ці дискретні результати кібербезпеки реалізуються та управляються. Хоча вимірювання всіх цих предметів виходять за межі Платформи, результати Основи платформи кібербезпеки підтримують самооцінку ефективності інвестицій та діяльності з кібербезпеки у наступних напрямках:

- Вибір того, як різні частини операції з кібербезпеки повинні впливати на вибір Цільових рівнів впровадження,
- Оцінка підходу організації до управління ризиками для кібербезпеки шляхом визначення Поточних рівнів впровадження,
- Визначення пріоритетів результатів з кібербезпеки шляхом розробки Цільових профілів,
- Визначення ступеня досягнення конкретними заходами з кібербезпеки бажаних результатів з кібербезпеки шляхом оцінки Поточних профілів та
- Вимірювання ступеня впровадження для каталогів контролю або технічного керівництва, вказаних як Інформаційні посилання.

Розробка показників ефективності кібербезпеки розвивається. Організації повинні бути розважливими, креативними та обережними щодо способів, якими вони застосовують вимірювання для оптимізації використання, уникаючи при цьому використання штучних показників поточного стану та прогресу у вдосконаленні управління ризиком для кібербезпеки. Судження про кібер-ризики вимагає дисципліни, і його слід періодично переглядати. Будь-які вимірювання часу використовуються як частина процесу Платформи, і організаціям рекомендується чітко визначити та знати, чому ці вимірювання є важливими та

як вони сприятимуть загальному управлінню ризиком для кібербезпеки. Вони також повинні чітко розуміти обмеження вимірювань, які використовуються.

Наприклад, відстеження заходів безпеки та бізнес-результатів може дати суттєве уявлення про те, як зміни в засобах управління модульністю безпеки впливають на досягнення організаційних цілей. Перевірка досягнення певних організаційних цілей вимагає аналізу даних лише *після* досягнення цієї цілі. Цей тип відстаючого вимірювання є більш абсолютним. Однак часто важливіше передбачити чи *може* бути ризик для кібербезпеки та який вплив він *може* мати, використовуючи запобіжний захід.

Організаціям рекомендується впроваджувати інновації та налаштовувати під себе способи включення вимірювань в застосування ними Платформи, з повним розумінням їх корисності та обмежень.

Додаток А: Основа платформи

У цьому додатку представлена Основа платформи: перелік Функцій, Категорій, Підкатегорій та Інформаційних посилань, що описують конкретні види діяльності з кібербезпеки, що є загальними для всіх секторів критично важливих інфраструктур. Обраний формат презентації Основи платформи не пропонує конкретного порядку виконання та не має на увазі ступінь важливості Категорій, Підкатегорій та Інформаційних посилань. Основа платформи, представлена в цьому додатку, являє собою загальний набір заходів для управління ризиком для кібербезпеки. Хоча Платформа не є вичерпною, вона розширювана, що дозволяє організаціям, секторам та іншим суб’єктам використовувати Підкатегорії та Інформаційні посилання, які є економічно ефективними та дієвими та дозволяють їм керувати ризиком для кібербезпеки. Заходи можна обрати з Основи платформи під час процесу створення Профілю, а до Профілю можна додати додаткові Категорії, Підкатегорії та Інформаційні посилання. Процеси управління ризиком, правові/регуляторні вимоги, цілі бізнесу/місії організації та організаційні обмеження керують вибором цих заходів під час створення Профілю. Персональні дані вважаються компонентом даних або активів, на які посилаються Категорії, при оцінці ризиків та методів захисту безпеки.

Хоча очікувані результати, визначені в Функціях, Категоріях та Підкатегоріях, однакові для IT та ICS, операційні середовища та міркування для IT та ICS відрізняються. ICS мають прямий вплив на фізичний світ, включаючи потенційні ризики для здоров'я та безпеки людей і вплив на навколишнє середовище. Крім того, ICS мають унікальні вимоги до продуктивності та надійності в порівнянні з IT, а цілі безпеки та ефективності повинні бути враховані при впровадженні заходів кібербезпеки.

Для полегшення використання кожному компоненту Основи платформи надається унікальний ідентифікатор. Функції та Категорії мають унікальний алфавітний ідентифікатор, як показано в Таблиці 1. Посилання на Підкатегорії в кожній Категорії наводяться чисельно; унікальний ідентифікатор для кожної Підкатегорії включений у Таблицю 2.

Додатковий допоміжний матеріал, включаючи Інформаційні посилання, що стосуються Платформи, можна знайти на веб-сайті NIST за адресою http://www.nist.gov/cyberframework/.

Таблиця 1: Унікальні ідентифікатори функцій та Категорій

Унікальний ідентифікатор Функції	Функція	Унікальний ідентифікатор Категорії	Категорія
ID	**Ідентифікація**	**ID.AM**	**Управління активами**
		ID.BE	**Бізнес-середовище**
		ID.GV	**Врядування**
		ID.RA	**Оцінка ризиків**
		ID.RM	**Стратегія управління ризиками**
		ID.SC	**Управління ризиками ланцюжків поставок**
PR	**Захист**	**PR.AC**	**Управління ідентифікацією та контроль доступу**
		PR.AT	**Усвідомлення та підготовка**
		PR.DS	**Безпека даних**
		PR.IP	**Процеси та процедури захисту інформації**
		PR.MA	**Технічне обслуговування**
		PR.PT	**Захисні технології**
DE	**Виявлення**	**DE.AE**	**Аномалії та події**
		DE.CM	**Безперервний моніторинг безпеки**
		DE.DP	**Процеси виявлення**
RS	**Реагування**	**RS.RP**	**Планування реагування**
		RS.CO	**Комунікації**
		RS.AN	**Аналіз**
		RS.MI	**Пом'якшення наслідків**
		RS.IM	**Вдосконалення**
RC	**Відновлення**	**RC.RP**	**Планування відновлення**
		RC.IM	**Вдосконалення**
		RC.CO	**Комунікації**

Таблиця 2: Основа Платформи

Функція	Категорія	Підкатегорія	Інформаційні посилання
ІДЕНТИФІКАЦІЯ (ID)	**Управління активами (ID.AM):** Дані, персонал, пристрої, системи та засоби, що дозволяють організації досягти комерційних цілей, визначаються та управляються відповідно до їх відносної важливості для цілей організації та стратегії ризику організації.	**ID.AM-1:** Фізичні пристрої та системи всередині організації інвентаризовано	**CIS CSC 1** **COBIT 5 BAI09.01, BAI09.02** **ISA 62443-2-1:2009 4.2.3.4** **ISA 62443-3-3:2013 SR 7.8** **ISO/IEC 27001:2013 A.8.1.1, A.8.1.2** **NIST SP 800-53 Ред. 4 CM-8, PM-5**
		ID.AM-2: Програмні платформи та програми в межах організації інвентаризовано	**CIS CSC 2** **COBIT 5 BAI09.01, BAI09.02, BAI09.05** **ISA 62443-2-1:2009 4.2.3.4** **ISA 62443-3-3:2013 SR 7.8** **ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1** **NIST SP 800-53 Ред. 4 CM-8, PM-5**
		ID.AM-3: Комунікації та потоки даних в організації структуровано	**CIS CSC 12** **COBIT 5 DSS05.02** **ISA 62443-2-1:2009 4.2.3.4** **ISO/IEC 27001:2013 A.13.2.1, A.13.2.2** **NIST SP 800-53 Ред. 4 AC-4, CA-3, CA-9, PL-8**
		ID.AM-4: Зовнішні інформаційні системи каталогізовано	**CIS CSC 12** **COBIT 5 AP002.02, AP010.04, DSS01.02** **ISO/IEC 27001:2013 A.11.2.6** **NIST SP 800-53 Ред. 4 AC-20, SA-9**
		ID.AM-5: Ресурси (наприклад, апаратне забезпечення, пристрої, дані, час, персонал та програмне забезпечення) пріоритизовано на підставі їх класифікації, критичності та вартості для бізнесу	**CIS CSC 13, 14** **COBIT 5 AP003.03, AP003.04, AP012.01, BAI04.02, BAI09.02** **ISA 62443-2-1:2009 4.2.3.6** **ISO/IEC 27001:2013 A.8.2.1** **NIST SP 800-53 Ред. 4 CP-2, RA-2, SA-14, SC-6**
		ID.AM-6: Роль і обов'язки з кібербезпеки для всієї робочої сили та сторонніх зацікавлених сторін (постачальників, клієнтів, партнерів) визначено	**CIS CSC 17, 19** **COBIT 5 AP001.02, AP007.06, AP013.01, DSS06.03** **ISA 62443-2-1:2009 4.3.2.3.3** **ISO/IEC 27001:2013 A.6.1.1** **NIST SP 800-53 Ред. 4 CP-2, PS-7, PM-11**

Функція	Категорія	Підкатегорія	Інформаційні посилання
	Бізнес-середовище (ID.BE): Місія, цілі, зацікавлені сторони та діяльність організації зрозумілі та пріоритизовані; ця інформація використовується для інформування ролей, відповідальності та рішень щодо управління ризиком для	**ID.BE-1:** Роль організації в ланцюжку поставок визначено та повідомлено	**COBIT 5 APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05** **ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2** **NIST SP 800-53 Ред. 4 CP-2, SA-12**
		ID.BE-2: Місце організації в критично важливій інфраструктурі та її секторі промисловості визначено та повідомлено	**COBIT 5 APO02.06, APO03.01** **ISO/IEC 27001:2013 пункт 4.1** **NIST SP 800-53 Ред. 4 PM-8**
		ID.BE-3: Пріоритети організаційної місії, цілей та заходів встановлено та повідомлено	**COBIT 5 APO02.01, APO02.06, APO03.01** **ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6** **NIST SP 800-53 Ред. 4 PM-11, SA-14**
		ID.BE-4: Залежності та критично важливі функції для надання критично важливих послуг встановлено	**COBIT 5 APO10.01, BAI04.02, BAI09.02** **ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3** **NIST SP 800-53 Ред. 4 CP-8, PE-9, PE-11, PM-8, SA-14**
		ID.BE-5: Вимоги стійкості для підтримки надання критично важливих послуг для всіх операційних станів (наприклад, під примусом/ атакою, під час відновлення, звичайних операцій) встановлено	**COBIT 5 BAI03.02, DSS04.02** **ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1** **NIST SP 800-53 Ред. 4 CP-2, CP-11, SA-13, SA- 14**
	Врядування (ID.GV): Політика, процедури та процеси управління та моніторингу регуляторних, правових, ризикових, екологічних та операційних вимог організації розуміються керівництвом та інформують його про ризик для кібербезпеки.	**ID.GV-1:** Організаційну політику з кібербезпеки встановлено та повідомлено	**CIS CSC 19** **COBIT 5 APO01.03, APO13.01, EDM01.01, EDM01.02** **ISA 62443-2-1:2009 4.3.2.6** **ISO/IEC 27001:2013 A.5.1.1** **NIST SP 800-53 Ред. 4 -1 засоби контролю зі всіх груп контролю безпеки**

Функція	Категорія	Підкатегорія	Інформаційні посилання
		ID.GV-2: Ролі та обов'язки з кібербезпеки координуються та узгоджуються з внутрішніми ролями та зовнішніми партнерами	**CIS CSC 19** **COBIT 5 APO01.02, APO10.03, APO13.02, DSS05.04** **ISA 62443-2-1:2009 4.3.2.3.3** **ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.15.1.1** **NIST SP 800-53 Ред. 4 PS-7, PM-1, PM-2**
		ID.GV-3: Законодавчі та нормативні вимоги щодо кібербезпеки, включаючи зобов'язання щодо конфіденційності та громадянських свобод, розуміються, та управління ними здійснюється	**CIS CSC 19** **COBIT 5 BAI02.01, MEA03.01, MEA03.04** **ISA 62443-2-1:2009 4.4.3.7** **ISO/IEC 27001:2013 A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5** **NIST SP 800-53 Ред. 4 -1 засоби контролю зі всіх груп контролю**
		ID.GV-4: Процеси врядування та управління ризиками усувають ризики для кібербезпеки	**COBIT 5 EDM03.02, APO12.02, APO12.05, DSS04.02** **ISA 62443-2-1:2009 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3** **ISO/IEC 27001:2013 пункт 6** **NIST SP 800-53 Ред. 4 SA-2, PM-3, PM-7, PM- 9, PM-10, PM-11**
	Оцінка ризиків (ID.RA): Організація розуміє ризик для кібербезпеки для організаційних операцій (включаючи місію, функції, імідж чи репутацію), організаційних ресурсів та окремих осіб.	**ID.RA-1:** Вразливості об'єктів визначені та задокументовані	**CIS CSC 4** **COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02** **ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12** **ISO/IEC 27001:2013 A.12.6.1, A.18.2.3** **NIST SP 800-53 Ред. 4 CA-2, CA-7, CA-8, RA- 3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5**
		ID.RA-2: Розвідувальна інформація про кібер-загрози отримується з форумів та джерел обміну інформацією	**CIS CSC 4** **COBIT 5 BAI08.01** **ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12** **ISO/IEC 27001:2013 A.6.1.4** **NIST SP 800-53 Ред. 4 SI-5, PM-15, PM-16**

Функція	Категорія	Підкатегорія	Інформаційні посилання
		ID.RA-3: Загрози, як внутрішні, так і зовнішні, ідентифіковано та документовано	**CIS CSC 4** **COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04** **ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12** **ISO/IEC 27001:2013 пункт 6.1.2** **NIST SP 800-53 Ред. 4 RA-3, SI-5, PM-12, PM- 16**
		ID.RA-4: Визначено потенційні ділові наслідки та ймовірності	**CIS CSC 4** **COBIT 5 DSS04.02** **ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12** **ISO/IEC 27001:2013 A.16.1.6, пункт 6.1.2** **NIST SP 800-53 Ред. 4 RA-2, RA-3, SA-14, PM- 9, PM-11**
		ID.RA-5: Для визначення ризику використовуються загрози, вразливості, вірогідність та наслідки	**CIS CSC 4** **COBIT 5 APO12.02** **ISO/IEC 27001:2013 A.12.6.1** **NIST SP 800-53 Ред. 4 RA-2, RA-3, PM-16**
		ID.RA-6: Реагування на ризик ідентифіковано та пріоритизовано	**CIS CSC 4** **COBIT 5 APO12.05, APO13.02** **ISO/IEC 27001:2013 пункт 6.1.3** **NIST SP 800-53 Ред. 4 PM-4, PM-9**
	Стратегія управління ризиками (ID.RM): пріоритети , обмеження, стійкість до ризику та припущення організації визначаються та використовуються для підтримки операційних	**ID.RM-1:** Процеси управління ризиками встановлені, керовані та узгоджені із зацікавленими сторонами організації	**CIS CSC 4** **COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02** **ISA 62443-2-1:2009 4.3.4.2** **ISO/IEC 27001:2013 пункт 6.1.3, пункт 8.3, пункт 9.3** **NIST SP 800-53 Ред. 4 PM-9**
		ID.RM-2: Стійкість організації до ризику визначена та чітко виражена	**COBIT 5 APO12.06** **ISA 62443-2-1:2009 4.3.2.6.5** **ISO/IEC 27001:2013 пункт 6.1.3, пункт 8.3** **NIST SP 800-53 Ред. 4 PM-9**

Функція	Категорія	Підкатегорія	Інформаційні посилання
		ID.RM-3: Визначення організацією стійкості до ризику визначається її роллю у критично важливій інфраструктурі та аналізом конкретних ризиків, пов'язаних із сектором	**COBIT 5 APO12.02** **ISO/IEC 27001:2013 пункт 6.1.3, пункт 8.3** **NIST SP 800-53 Ред. 4 SA-14, PM-8, PM-9, PM- 11**
	Управління ризиками системи поставок (ID.SC): Пріоритети організації, обмеження, стійкість до ризику та припущення визначаються та використовуються для підтримки рішень щодо ризику, пов'язаних з управлінням ризиком систем поставок. Організація створила та впровадила процеси визначення, оцінки та управління ризиками поставок.	**ID.SC-1:** Процеси управління кібер-ризиками для ланцюжків поставок визначено, встановлено, оцінено, керовано та узгоджено з зацікавленими сторонами організації	**CIS CSC 4** **COBIT 5 APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02** **ISA 62443-2-1:2009 4.3.4.2** **ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2** **NIST SP 800-53 Ред. 4 SA-9, SA-12, PM-9**
		ID.SC-2: Постачальники та сторонні партнери інформаційних систем, компонентів та послуг ідентифіковані, пріоритизовані та оцінені за допомогою процесу оцінювання кібер-ризику для ланцюжків поставок	**COBIT 5 APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03** **ISA 62443-2-1:2009 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14** **ISO/IEC 27001:2013 A.15.2.1, A.15.2.2** **NIST SP 800-53 Ред. 4 RA-2, RA-3, SA-12, SA- 14, SA-15, PM-9**
		ID.SC-3: Контракти з постачальниками та сторонніми партнерами використовуються для здійснення відповідних заходів, спрямованих на досягнення цілей програми кібербезпеки організації та Плану управління кібер-ризиками ланцюжків поставок	**COBIT 5 APO10.01, APO10.02, APO10.03, APO10.04, APO10.05** **ISA 62443-2-1:2009 4.3.2.6.4, 4.3.2.6.7** **ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3** **NIST SP 800-53 Ред. 4 SA-9, SA-11, SA-12, PM- 9**
		ID.SC-4: Постачальники та сторонні партнери регулярно оцінюються за допомогою аудитів, результатів тестів або інших форм оцінок, щоб підтвердити, що вони виконують свої договірні зобов'язання.	**COBIT 5 APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05** **ISA 62443-2-1:2009 4.3.2.6.7** **ISA 62443-3-3:2013 SR 6.1** **ISO/IEC 27001:2013 A.15.2.1, A.15.2.2**

Функція	Категорія	Підкатегорія	Інформаційні посилання
			NIST SP 800-53 Ред. 4 AU-2, AU-6, AU-12, AU- 16, PS-7, SA-9, SA-12
		ID.SC-5: Планування та перевірка реагування та відновлення проводяться з постачальниками та сторонніми провайдерами	**CIS CSC 19, 20** **COBIT 5 DSS04.04** **ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11** **ISA 62443-3-3:2013 SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4** **ISO/IEC 27001:2013 A.17.1.3** **NIST SP 800-53 Ред. 4 CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9**
ЗАХИСТ (PR)	**Управління ідентифікацією, аутентифікацією та контроль доступу (PR.AC):** Доступ до фізичних та логічних ресурсів та пов'язаних з ними пристроїв обмежений авторизованими користувачами, процесами та пристроями та управляється відповідно до оціненого ризику несанкціонованого доступу до дозволених видів діяльності та операцій.	**PR.AC-1:** Засоби індивідуалізації та дані для встановлення аутентичності видаються, керуються, верифікуються, відкликаються та перевіряються аудитом для авторизованих пристроїв, користувачів та процесів	**CIS CSC 1, 5, 15, 16** **COBIT 5 DSS05.04, DSS06.03** **ISA 62443-2-1:2009 4.3.3.5.1** **ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9** **ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3** **NIST SP 800-53 Ред. 4 AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11**
		PR.AC-2: Фізичний доступ до активів керується та захищений	**COBIT 5 DSS01.04, DSS05.05** **ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8** **ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8** **NIST SP 800-53 Ред. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-8**
		PR.AC-3: Віддалений доступ керується	**CIS CSC 12** **COBIT 5 AP013.01, DSS01.04, DSS05.03** **ISA 62443-2-1:2009 4.3.3.6.6** **ISA 62443-3-3:2013 SR 1.13, SR 2.6** **ISO/IEC 27001:2013 A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1**

Функція	Категорія	Підкатегорія	Інформаційні посилання
			NIST SP 800-53 Ред. 4 AC-1, AC-17, AC-19, AC-20, SC-15
		PR.AC-4: Дозволи та права доступу керуються, використовуючи принципи найменших повноважень та розподілу обов'язків	**CIS CSC 3, 5, 12, 14, 15, 16, 18** **COBIT 5 DSS05.04** **ISA 62443-2-1:2009 4.3.3.7.3** **ISA 62443-3-3:2013 SR 2.1** **ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5** **NIST SP 800-53 Ред. 4 AC-1, AC-2, AC-3, AC- 5, AC-6, AC-14, AC-16, AC-24**
		PR.AC-5: Цільність мережі захищена (наприклад, сегрегація мережі, сегментація мережі).	**CIS CSC 9, 14, 15, 18** **COBIT 5 DSS01.05, DSS05.02** **ISA 62443-2-1:2009 4.3.3.4** **ISA 62443-3-3:2013 SR 3.1, SR 3.8** **ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3** **NIST SP 800-53 Ред. 4 AC-4, AC-10, SC-7**
		PR.AC-6: Особистості перевірені та пов'язані з даними для встановлення аутентичності та підтверджуються у взаємодіях	**CIS CSC, 16** **COBIT 5 DSS05.04, DSS05.05, DSS05.07, DSS06.03** **ISA 62443-2-1:2009 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4** **ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1** **ISO/IEC 27001:2013, A.7.1.1, A.9.2.1** **NIST SP 800-53 Ред. 4 AC-1, AC-2, AC-3, AC- 16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3**
		PR.AC-7: Користувачі, пристрої та інші активи аутентифіковані (наприклад, однофакторний, багатофакторний) у відповідності до ризиків операції (наприклад, ризики для безпеки та конфіденційності приватних осіб та інші організаційні ризики)	**CIS CSC 1, 12, 15, 16** **COBIT 5 DSS05.04, DSS05.10, DSS06.10** **ISA 62443-2-1:2009 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9**

Функція	Категорія	Підкатегорія	Інформаційні посилання
			ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 **ISO/IEC 27001:2013 A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4** **NIST SP 800-53 Ред. 4 AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11**
	Усвідомлення та підготовка (PR.AT). Співробітники та партнери організації отримують освіту для підвищення обізнаності з кібербезпеки та вчаться виконувати свої обов'язки, пов'язані з кібербезпекою, відповідно до релевантної політики, процедур та угод.	**PR.AT-1:** Усі користувачі поінформовані та пройшли підготовку	**CIS CSC 17, 18** **COBIT 5 AP007.03, BAI05.07** **ISA 62443-2-1:2009 4.3.2.4.2** **ISO/IEC 27001:2013 A.7.2.2, A.12.2.1** **NIST SP 800-53 Ред. 4 AT-2, PM-13**
		PR.AT-2: Привілейовані користувачі розуміють їх ролі та обов'язки	**CIS CSC 5, 17, 18** **COBIT 5 AP007.02, DSS05.04, DSS06.03** **ISA 62443-2-1:2009 4.3.2.4.2, 4.3.2.4.3** **ISO/IEC 27001:2013 A.6.1.1, A.7.2.2** **NIST SP 800-53 Ред. 4 AT-3, PM-13**
		PR.AT-3: Зацікавлені треті сторони (наприклад, постачальники, клієнти, партнери) розуміють їхні ролі та обов'язки	**CIS CSC 17** **COBIT 5 AP007.03, AP007.06, AP010.04, AP010.05** **ISA 62443-2-1:2009 4.3.2.4.2** **ISO/IEC 27001:2013 A.6.1.1, A.7.2.1, A.7.2.2** **NIST SP 800-53 Ред. 4 PS-7, SA-9, SA-16**
		PR.AT-4: Вищі керівники розуміють їх ролі та обов'язки	**CIS CSC 17, 19** **COBIT 5 EDM01.01, AP001.02, AP007.03** **ISA 62443-2-1:2009 4.3.2.4.2** **ISO/IEC 27001:2013 A.6.1.1, A.7.2.2** **NIST SP 800-53 Ред. 4 AT-3, PM-13**
		PR.AT-5: Персонал з питань фізичної та кібербезпеки розуміє свої ролі та обов'язки	**CIS CSC 17** **COBIT 5 AP007.03** **ISA 62443-2-1:2009 4.3.2.4.2** **ISO/IEC 27001:2013 A.6.1.1, A.7.2.2**

Функція	Категорія	Підкатегорія	Інформаційні посилання
			NIST SP 800-53 Ред. 4 AT-3, IR-2, PM-13
	Безпека даних (PR.DS): Інформація та записи (дані) управляються відповідно до стратегії управління ризиками організації для захисту конфіденційності, цілісності та доступності інформації.	**PR.DS-1:** Дані, що знаходяться на зберіганні, захищені	**CIS CSC 13, 14** **COBIT 5 AP001.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06** **ISA 62443-3-3:2013 SR 3.4, SR 4.1** **ISO/IEC 27001:2013 A.8.2.3** **NIST SP 800-53 Ред. 4 MP-8, SC-12, SC-28**
		PR.DS-2: Дані, що передаються, захищені	**CIS CSC 13, 14** **COBIT 5 AP001.06, DSS05.02, DSS06.06** **ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2** **ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3** **NIST SP 800-53 Ред. 4 SC-8, SC-11, SC-12**
		PR.DS-3: Здійснюється формальне управління активами під час видалення, передачі та ліквідації	**CIS CSC 1** **COBIT 5 BAI09.03** **ISA 62443-2-1:2009 4.3.3.3.9, 4.3.4.4.1** **ISA 62443-3-3:2013 SR 4.2** **ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7** **NIST SP 800-53 Ред. 4 CM-8, MP-6, PE-16**
		PR.DS-4: Підтримується достатня здатність забезпечити доступність	**CIS CSC 1, 2, 13** **COBIT 5 AP013.01, BAI04.04** **ISA 62443-3-3:2013 SR 7.1, SR 7.2** **ISO/IEC 27001:2013 A.12.1.3, A.17.2.1** **NIST SP 800-53 Ред. 4 AU-4, CP-2, SC-5**
		PR.DS-5: Захист від витоків даних впроваджено	**CIS CSC 13** **COBIT 5 AP001.06, DSS05.04, DSS05.07, DSS06.02** **ISA 62443-3-3:2013 SR 5.2** **ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4,**

Функція	Категорія	Підкатегорія	Інформаційні посилання
			A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 **NIST SP 800-53 Ред. 4 AC-4, AC-5, AC-6, PE- 19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4**
		PR.DS-6: Механізми перевірки цілісності використовуються для перевірки цілісності програмного забезпечення, прошивки та інформації	**CIS CSC 2, 3** **COBIT 5 AP001.06, BAI06.01, DSS06.02** **ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4, SR 3.8** **ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4** **NIST SP 800-53 Ред. 4 SC-16, SI-7**
		PR.DS-7: Середовище(а) розробки та тестування відокремлене(і) від виробничого середовища	**CIS CSC 18, 20** **COBIT 5 BAI03.08, BAI07.04** **ISO/IEC 27001:2013 A.12.1.4** **NIST SP 800-53 Ред. 4 CM-2**
		PR.DS-8: Механізми перевірки цілісності використовуються для перевірки цілісності апаратного забезпечення	**COBIT 5 BAI03.05** **ISA 62443-2-1:2009 4.3.4.4.4** **ISO/IEC 27001:2013 A.11.2.4** **NIST SP 800-53 Ред. 4 SA-10, SI-7**
	Процеси та процедури захисту інформації (PR.IP): Політика безпеки (яка стосується цілей, обсягу, ролей, обов'язків, зобов'язань керівництва та координації між організаціями), процеси та процедури підтримуються та використовуються для управління	**PR.IP-1:** Базова конфігурація інформаційних технологій/промислових систем управління створюється та підтримується з урахуванням принципів безпеки (наприклад, концепція найменшої функціональності)	**CIS CSC 3, 9, 11** **COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05** **ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3** **ISA 62443-3-3:2013 SR 7.6** **ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4** **NIST SP 800-53 Ред. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10**
		PR.IP-2: Впроваджено Життєвий цикл розвитку Системи для управління системами	**CIS CSC 18** **COBIT 5 AP013.01, BAI03.01, BAI03.02, BAI03.03** **ISA 62443-2-1:2009 4.3.4.3.3**

Функція	Категорія	Підкатегорія	Інформаційні посилання
			ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 **NIST SP 800-53 Ред. 4 PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI- 13, SI-14, SI-16, SI-17**
		PR.IP-3: Впроваджено процеси контролю змін конфігурації	**CIS CSC 3, 11** **COBIT 5 BAI01.06, BAI06.01** **ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3** **ISA 62443-3-3:2013 SR 7.6** **ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4** **NIST SP 800-53 Ред. 4 CM-3, CM-4, SA-10**
		PR.IP-4: Резервне копіювання інформації ведеться, підтримується та тестується	**CIS CSC 10** **COBIT 5 AP013.01, DSS01.01, DSS04.07** **ISA 62443-2-1:2009 4.3.4.3.9** **ISA 62443-3-3:2013 SR 7.3, SR 7.4** **ISO/IEC 27001:2013 A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3** **NIST SP 800-53 Ред. 4 CP-4, CP-6, CP-9**
		PR.IP-5: Політика та нормативні акти щодо фізичного робочого середовища для активів організації виконуються	**COBIT 5 DSS01.04, DSS05.05** **ISA 62443-2-1:2009 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6** **ISO/IEC 27001:2013 A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3** **NIST SP 800-53 Ред. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18**
		PR.IP-6: Дані знищуються відповідно до політики	**COBIT 5 BAI09.03, DSS05.06** **ISA 62443-2-1:2009 4.3.4.4.4** **ISA 62443-3-3:2013 SR 4.2** **ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7** **NIST SP 800-53 Ред. 4 MP-6**

Функція	Категорія	Підкатегорія	Інформаційні посилання
		PR.IP-7: Покращено процеси захисту	**COBIT 5 APO11.06, APO12.06, DSS04.05** **ISA 62443-2-1:2009 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8** **ISO/IEC 27001:2013 A.16.1.6, пункт 9, пункт 10** **NIST SP 800-53 Ред. 4 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6**
		PR.IP-8: Інформація про ефективність технологій захисту розподіляється	**COBIT 5 BAI08.04, DSS03.04** **ISO/IEC 27001:2013 A.16.1.6** **NIST SP 800-53 Ред. 4 AC-21, CA-7, SI-4**
		PR.IP-9: Плани реагування (Реагування на інциденти та безперервність бізнесу) та плани (Відновлення після інцидентів та відновлення після аварій) впроваджені та управляються	**CIS CSC 19** **COBIT 5 APO12.06, DSS04.03** **ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1** **ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3** **NIST SP 800-53 Ред. 4 CP-2, CP-7, CP-12, CP- 13, IR-7, IR-8, IR-9, PE-17**
		PR.IP-10: Плани реагування та відновлення перевіряються	**CIS CSC 19, 20** **COBIT 5 DSS04.04** **ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11** **ISA 62443-3-3:2013 SR 3.3** **ISO/IEC 27001:2013 A.17.1.3** **NIST SP 800-53 Ред. 4 CP-4, IR-3, PM-14**
		PR.IP-11: Кібербезпеку включено в практику персоналу (наприклад, відклик, скринінг персоналу)	**CIS CSC 5, 16** **COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05** **ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3** **ISO/IEC 27001:2013 A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4** **NIST SP 800-53 Ред. 4 PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21**

Функція	Категорія	Підкатегорія	Інформаційні посилання
		PR.IP-12: Розроблено та впроваджено план управління вразливостями	**CIS CSC 4, 18, 20** **COBIT 5 BAI03.10, DSS05.01, DSS05.02** **ISO/IEC 27001:2013 A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3** **NIST SP 800-53 Ред. 4 RA-3, RA-5, SI-2**
	Технічне обслуговування (PR.MA): Обслуговування та ремонт компонентів промислової системи контролю та інформаційної системи виконуються відповідно до правил та процедур.	**PR.MA-1:** Технічне обслуговування та ремонт організаційних активів виконуються та реєструються за допомогою затверджених та контрольованих інструментів	**COBIT 5 BAI03.10, BAI09.02, BAI09.03, DSS01.05** **ISA 62443-2-1:2009 4.3.3.3.7** **ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6** **NIST SP 800-53 Ред. 4 MA-2, MA-3, MA-5, MA-6**
		PR.MA-2: Віддалене обслуговування організаційних ресурсів затверджується, реєструється та виконується таким чином, що запобігає несанкціонованому доступу	**CIS CSC 3, 5** **COBIT 5 DSS05.04** **ISA 62443-2-1:2009 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8** **ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1** **NIST SP 800-53 Ред. 4 MA-4**
	Захисна технологія (PR.PT):Технічні рішення безпеки управляються для забезпечення безпеки та стійкості систем та активів відповідно до відповідних політик, процедур та угод.	**PR.PT-1:** Аудит/записи в журналі визначаються, документуються, впроваджуються та переглядаються відповідно до політики	**CIS CSC 1, 3, 5, 6, 14, 15, 16** **COBIT 5 AP011.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01** **ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4** **ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12** **ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1** **NIST SP 800-53 Ред. 4 AU Група (Family)**
		PR.PT-2: Змінні носії захищені та використовуються з обмеженнями відповідно до політики	**CIS CSC 8, 13** **COBIT 5 AP013.01, DSS05.02, DSS05.06** **ISA 62443-3-3:2013 SR 2.3** **ISO/IEC 27001:2013 A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9**

Функція	Категорія	Підкатегорія	Інформаційні посилання
			NIST SP 800-53 Ред. 4 MP-2, MP-3, MP-4, MP- 5, MP-7, MP-8
		PR.PT-3: Принцип найменшої функціональності враховується шляхом налаштування систем для забезпечення лише істотних можливостей	**CIS CSC 3, 11, 14** **COBIT 5 DSS05.02, DSS05.05, DSS06.06 ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4** **ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7** **ISO/IEC 27001:2013 A.9.1.2** **NIST SP 800-53 Ред. 4 AC-3, CM-7**
		PR.PT-4: Мережі зв'язку та управління захищені	**CIS CSC 8, 12, 15** **COBIT 5 DSS05.02, AP013.01** **ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6** **ISO/IEC 27001:2013 A.13.1.1, A.13.2.1, A.14.1.3** **NIST SP 800-53 Ред. 4 AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC- 38, SC-39, SC-40, SC-41, SC-43**
		PR.PT-5: Механізми (наприклад, безвідмовна робота, балансування навантаження, гаряча заміна) впроваджуються для досягнення вимог до стійкості в нормальних та несприятливих ситуаціях.	**COBIT 5 BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05** **ISA 62443-2-1:2009 4.3.2.5.2** **ISA 62443-3-3:2013 SR 7.1, SR 7.2** **ISO/IEC 27001:2013 A.17.1.2, A.17.2.1** **NIST SP 800-53 Ред. 4 CP-7, CP-8, CP-11, CP- 13, PL-8, SA-14, SC-6**

Функція	Категорія	Підкатегорія	Інформаційні посилання
ВИЯВЛЕННЯ (DE)	**Аномалії та події (DE.AE):** Виявляється аномальна активність і розуміється потенційний вплив подій.	**DE.AE-1:** Встановлюється та керується базовий рівень операцій мережі та очікуваних потоків даних для користувачів і систем	**CIS CSC 1, 4, 6, 12, 13, 15, 16** **COBIT 5 DSS03.01** **ISA 62443-2-1:2009 4.4.3.3** **ISO/IEC 27001:2013 A.12.1.1, A.12.1.2, A.13.1.1,A.13.1.2** **NIST SP 800-53 Ред. 4 AC-4, CA-3, CM-2, SI-4**
		DE.AE-2: Виявлені події аналізуються для розуміння цілей атаки та методів	**CIS CSC 3, 6, 13, 15** **COBIT 5 DSS05.07** **ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8** **ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2** **ISO/IEC 27001:2013 A.12.4.1, A.16.1.1, A.16.1.4** **NIST SP 800-53 Ред. 4 AU-6, CA-7, IR-4, SI-4**
		DE.AE-3: Дані про події збираються та корелюються з кількох джерел та датчиків	**CIS CSC 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16** **COBIT 5 BAI08.02** **ISA 62443-3-3:2013 SR 6.1** **ISO/IEC 27001:2013 A.12.4.1, A.16.1.7** **NIST SP 800-53 Ред. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4**
		DE.AE-4: Визначено вплив подій	**CIS CSC 4, 6** **COBIT 5 AP012.06, DSS03.01** **ISO/IEC 27001:2013 A.16.1.4** **NIST SP 800-53 Ред. 4 CP-2, IR-4, RA-3, SI-4**
		DE.AE-5: Порогові значення попередження про події встановлено	**CIS CSC 6, 19** **COBIT 5 AP012.06, DSS03.01** **ISA 62443-2-1:2009 4.2.3.10** **ISO/IEC 27001:2013 A.16.1.4** **NIST SP 800-53 Ред. 4 IR-4, IR-5, IR-8**
	Безперервний моніторинг безпеки (DE.CM): Інформаційна система та активи контролюються для виявлення подій, пов'язаних із кібербезпекою, та перевірки	**DE.CM-1:** Проводиться моніторинг мережі для виявлення можливих подій, пов'язаних із кібербезпекою	**CIS CSC 1, 7, 8, 12, 13, 15, 16** **COBIT 5 DSS01.03, DSS03.05, DSS05.07** **ISA 62443-3-3:2013 SR 6.2** **NIST SP 800-53 Ред. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4**

Функція	Категорія	Підкатегорія	Інформаційні посилання
		DE.CM-2: Фізичне середовище контролюється для виявлення можливих подій, пов'язаних із кібербезпекою	**COBIT 5 DSS01.04, DSS01.05** **ISA 62443-2-1:2009 4.3.3.3.8** **ISO/IEC 27001:2013 A.11.1.1, A.11.1.2** **NIST SP 800-53 Ред. 4 CA-7, PE-3, PE-6, PE-20**
		DE.CM-3: Моніторинг діяльності персоналу визначає можливі події, пов'язані з кібербезпекою	**CIS CSC 5, 7, 14, 16** **COBIT 5 DSS05.07** **ISA 62443-3-3:2013 SR 6.2** **ISO/IEC 27001:2013 A.12.4.1, A.12.4.3** **NIST SP 800-53 Ред. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11**
		DE.CM-4: Виявлено шкідливий код	**CIS CSC 4, 7, 8, 12** **COBIT 5 DSS05.01** **ISA 62443-2-1:2009 4.3.4.3.8** **ISA 62443-3-3:2013 SR 3.2** **ISO/IEC 27001:2013 A.12.2.1** **NIST SP 800-53 Ред. 4 SI-3, SI-8**
		DE.CM-5: Виявлено неавторизований мобільний код	**CIS CSC 7, 8** **COBIT 5 DSS05.01** **ISA 62443-3-3:2013 SR 2.4** **ISO/IEC 27001:2013 A.12.5.1, A.12.6.2** **NIST SP 800-53 Ред. 4 SC-18, SI-4, SC-44**
		DE.CM-6: Здійснюється моніторинг діяльності зовнішнього постачальника послуг для виявлення потенційних подій, пов'язаних із кібербезпекою	**COBIT 5 APO07.06, APO10.05** **ISO/IEC 27001:2013 A.14.2.7, A.15.2.1** **NIST SP 800-53 Ред. 4 CA-7, PS-7, SA-4, SA-9, SI-4**
		DE.CM-7: Моніторинг неавторизованого персоналу, підключень, пристроїв та програмного забезпечення	**CIS CSC 1, 2, 3, 5, 9, 12, 13, 15, 16** **COBIT 5 DSS05.02, DSS05.05** **ISO/IEC 27001:2013 A.12.4.1, A.14.2.7, A.15.2.1** **NIST SP 800-53 Ред. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4**
		DE.CM-8: Виконується сканування вразливостей	**CIS CSC 4, 20**

Функція	Категорія	Підкатегорія	Інформаційні посилання
			COBIT 5 BAI03.10, DSS05.01 **ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7** **ISO/IEC 27001:2013 A.12.6.1** **NIST SP 800-53 Ред. 4 RA-5**
	Процеси виявлення (DE.DP): Процеси та процедури виявлення підтримуються та перевіряються для забезпечення обізнаності про аномальні події.	**DE.DP-1:** Ролі та обов'язки щодо виявлення добре визначені для забезпечення відповідальності	**CIS CSC 19** **COBIT 5 APO01.02, DSS05.01, DSS06.03** **ISA 62443-2-1:2009 4.4.3.1** **ISO/IEC 27001:2013 A.6.1.1, A.7.2.2** **NIST SP 800-53 Ред. 4 CA-2, CA-7, PM-14**
		DE.DP-2: Заходи з виявлення відповідають всім застосовним вимогам	**COBIT 5 DSS06.01, MEA03.03, MEA03.04** **ISA 62443-2-1:2009 4.4.3.2** **ISO/IEC 27001:2013 A.18.1.4, A.18.2.2, A.18.2.3** **NIST SP 800-53 Ред. 4 AC-25, CA-2, CA-7, SA-18, SI-4, PM-14**
		DE.DP-3: Протестовано процеси виявлення	**COBIT 5 APO13.02, DSS05.02** **ISA 62443-2-1:2009 4.4.3.2** **ISA 62443-3-3:2013 SR 3.3** **ISO/IEC 27001:2013 A.14.2.8** **NIST SP 800-53 Ред. 4 CA-2, CA-7, PE-3, SI-3, SI-4, PM-14**
		DE.DP-4: Інформація про виявлення подій повідомляється	**CIS CSC 19** **COBIT 5 APO08.04, APO12.06, DSS02.05** **ISA 62443-2-1:2009 4.3.4.5.9** **ISA 62443-3-3:2013 SR 6.1** **ISO/IEC 27001:2013 A.16.1.2, A.16.1.3** **NIST SP 800-53 Ред. 4 AU-6, CA-2, CA-7, RA-5, SI-4**
		DE.DP-5: Процеси виявлення постійно вдосконалюються	**COBIT 5 APO11.06, APO12.06, DSS04.05** **ISA 62443-2-1:2009 4.4.3.4** **ISO/IEC 27001:2013 A.16.1.6** **NIST SP 800-53 Ред. 4, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14**

Функція	Категорія	Підкатегорія	Інформаційні посилання
РЕАГУВАННЯ (RS)	**Планування реагування (RS.RP):** Процеси та процедури реагування виконуються та підтримуються, щоб забезпечити реагування на виявлені випадки, пов'язані з кібербезпекою.	**RS.RP-1:** План реагування виконується під час або після інциденту	**CIS CSC 19** **COBIT 5 APO12.06, BAI01.10** **ISA 62443-2-1:2009 4.3.4.5 1** **ISO/IEC 27001:2013 A.16.1.5** **NIST SP 800-53 Ред. 4 CP-2, CP-10, IR-4, IR-8**
	Комунікації (RS.CO): Відповідні дії координуються з внутрішніми та зовнішніми зацікавленими сторонами (наприклад, зовнішня підтримка від правоохоронних органів).	**RS.CO-1:** Персонал знає свої функції та порядок операцій, коли потрібне реагування	**CIS CSC 19** **COBIT 5 EDM03.02, APO01.02, APO12.03** **ISA 62443-2-1:2009 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4** **ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, A.16.1.1** **NIST SP 800-53 Ред. 4 CP-2, CP-3, IR-3, IR-8**
		RS.CO-2: Інформація про інциденти повідомляється відповідно до встановлених критеріїв	**CIS CSC 19** **COBIT 5 DSS01.03** **ISA 62443-2-1:2009 4.3.4.5.5** **ISO/IEC 27001:2013 A.6.1.3, A.16.1.2** **NIST SP 800-53 Ред. 4 AU-6, IR-6, IR-8**
		RS.CO-3: Інформація поширюються відповідно до планів реагування	**CIS CSC 19** **COBIT 5 DSS03.04** **ISA 62443-2-1:2009 4.3.4.5.2** **ISO/IEC 27001:2013 A.16.1.2, пункт 7.4, пункт 16.1.2** **NIST SP 800-53 Ред. 4 CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4**
		RS.CO-4: Координування з зацікавленими сторонами відбувається відповідно до планів реагування	**CIS CSC 19** **COBIT 5 DSS03.04** **ISA 62443-2-1:2009 4.3.4.5.5** **ISO/IEC 27001:2013 пункт 7.4** **NIST SP 800-53 Ред. 4 CP-2, IR-4, IR-8**
		RS.CO-5: Добровільний обмін інформацією відбувається з зовнішніми зацікавленими сторонами для досягнення більш широкої обізнаності про ситуацію з кібербезпеки	**CIS CSC 19** **COBIT 5 BAI08.04** **ISO/IEC 27001:2013 A.6.1.4** **NIST SP 800-53 Ред. 4 SI-5, PM-15**

Функція	Категорія	Підкатегорія	Інформаційні посилання
	Аналіз (RS.AN): Аналіз **проводиться** для забезпечення ефективного реагування та підтримки відновлення діяльності.	**RS.AN-1:** Вивчаються повідомлення від систем виявлення	**CIS CSC 4, 6, 8, 19** **COBIT 5 DSS02.04, DSS02.07** **ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8** **ISA 62443-3-3:2013 SR 6.1** **ISO/IEC 27001:2013 A.12.4.1, A.12.4.3, A.16.1.5** **NIST SP 800-53 Ред. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4**
		RS.AN-2: Вплив інцидентів зрозумілий	**COBIT 5 DSS02.02** **ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8** **ISO/IEC 27001:2013 A.16.1.4, A.16.1.6** **NIST SP 800-53 Ред. 4 CP-2, IR-4**
		RS.AN-3: Проводиться експертиза	**COBIT 5 AP012.06, DSS03.02, DSS05.07** **ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1** **ISO/IEC 27001:2013 A.16.1.7** **NIST SP 800-53 Ред. 4 AU-7, IR-4**
		RS.AN-4: Інциденти класифікуються відповідно до планів реагування	**CIS CSC 19** **COBIT 5 DSS02.02** **ISA 62443-2-1:2009 4.3.4.5.6** **ISO/IEC 27001:2013 A.16.1.4** **NIST SP 800-53 Ред. 4 CP-2, IR-4, IR-5, IR-8**
		RS.AN-5: Створені процеси отримання, аналізу та реагування на вразливі елементи, що розкриваються для організації з внутрішніх та зовнішніх джерел (наприклад, внутрішні тести, бюлетені з безпеки або дослідники проблем безпеки).	**CIS CSC 4, 19** **COBIT 5 EDM03.02, DSS05.07** **NIST SP 800-53 Ред. 4 SI-5, PM-15**
	Пом'якшення наслідків (RS.MI): Проводяться заходи для запобігання розширенню події, пом'якшення її наслідків та усунення інциденту.	**RS.MI-1:** Інциденти обмежено	**CIS CSC 19** **COBIT 5 AP012.06** **ISA 62443-2-1:2009 4.3.4.5.6** **ISA 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4** **ISO/IEC 27001:2013 A.12.2.1, A.16.1.5**

Функція	Категорія	Підкатегорія	Інформаційні посилання
			NIST SP 800-53 Ред. 4 IR-4
		RS.MI-2: Наслідки інцидентів зменшено	**CIS CSC 4, 19** **COBIT 5 APO12.06** **ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10** **ISO/IEC 27001:2013 A.12.2.1, A.16.1.5** **NIST SP 800-53 Ред. 4 IR-4**
		RS.MI-3: Наслідки нової визначеної вразливості пом'якшені або задокументовані як прийняті ризики	**CIS CSC 4** **COBIT 5 APO12.06** **ISO/IEC 27001:2013 A.12.6.1** **NIST SP 800-53 Ред. 4 CA-7, RA-3, RA-5**
	Вдосконалення (RS.IM): Організаційні заходи з реагування вдосконалюються шляхом включення досвіду, отриманого з поточної та попередньої діяльності з виявлення/реагування.	**RS.IM-1:** Плани реагування містять отриманий досвід	**COBIT 5 BAI01.13** **ISA 62443-2-1:2009 4.3.4.5.10, 4.4.3.4** **ISO/IEC 27001:2013 A.16.1.6, пункт 10** **NIST SP 800-53 Ред. 4 CP-2, IR-4, IR-8**
		RS.IM-2: Стратегії реагування оновлюються	**COBIT 5 BAI01.13, DSS04.08** **ISO/IEC 27001:2013 A.16.1.6, пункт 10** **NIST SP 800-53 Ред. 4 CP-2, IR-4, IR-8**
ВІДНОВЛЕННЯ (RC)	**Планування відновлення (RC.RP):** Процеси та процедури відновлення виконуються та підтримуються для забезпечення відновлення систем або активів, що постраждали від інцидентів, пов'язаних із кібербезпекою.	**RC.RP-1:** План відновлення виконується під час або після інциденту, пов’язаного з кібербезпекою	**CIS CSC 10** **COBIT 5 APO12.06, DSS02.05, DSS03.04** **ISO/IEC 27001:2013 A.16.1.5** **NIST SP 800-53 Ред. 4 CP-10, IR-4, IR-8**
	Вдосконалення (RC.IM): Планування та процеси відновлення вдосконалюються завдяки включенню отриманого досвіду у майбутні заходи.	**RC.IM-1:** Плани відновлення включають отриманий досвід	**COBIT 5 APO12.06, BAI05.07, DSS04.08** **ISA 62443-2-1:2009 4.4.3.4** **ISO/IEC 27001:2013 A.16.1.6, пункт 10** **NIST SP 800-53 Ред. 4 CP-2, IR-4, IR-8**
		RC.IM-2: Стратегії відновлення оновлюються	**COBIT 5 APO12.06, BAI07.08** **ISO/IEC 27001:2013 A.16.1.6, пункт 10** **NIST SP 800-53 Ред. 4 CP-2, IR-4, IR-8**

Функція	Категорія	Підкатегорія	Інформаційні посилання
	Комунікації (RC.CO): Відновлювальні заходи координуються з внутрішніми та зовнішніми сторонами (наприклад, координуючими центрами, постачальниками Інтернет-послуг, власниками атакуючих систем, жертвами, іншими групами реагування на інциденти, пов'язані з кібербезпекою та постачальниками).	**RC.CO-1:** Здійснюється управління зв'язками з громадськістю	**COBIT 5 EDM03.02** **ISO/IEC 27001:2013 A.6.1.4, пункт 7.4**
		RC.CO-2: Репутація відновлена після інциденту	**COBIT 5 MEA03.02** **ISO/IEC 27001:2013 пункт 7.4**
		RC.CO-3: Відновлювальні заходи передаються внутрішнім та зовнішнім зацікавленим сторонам, а також виконавчим і керівним командам	**COBIT 5 APO12.06** **ISO/IEC 27001:2013 пункт 7.4** **NIST SP 800-53 Ред. 4 CP-2, IR-4**

Інформацію про Інформаційні посилання, описані в Додатку А, можна бути знайти за наступними адресами:

- Цілі контролю за інформаційними та суміжними технологіями (COBIT): http://www.isaca.org/COBIT/Pages/default.aspx
- Засоби контролю критичної безпеки CIS для ефективного кіберзахисту (Засоби контролю CIS): https://www.cisecurity.org
- Американський національний інститут стандартів / Міжнародне товариство автоматизації (ANSI/ISA)-62443-2-1 (99.02.01)-2009, *Безпека для промислової автоматизації та систем управління: створення програми безпеки промислової автоматики та систем управління:* https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116731
- ANSI/ISA-62443-3-3 (99.03.03)-2013, *Безпека для промислової автоматизації та систем керування: вимоги до безпеки системи та рівні безпеки:* https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116785
- ISO/IEC 27001, *Інформаційні технології -- Технології безпеки -- Системи управління інформаційною безпекою -- Вимоги:* https://www.iso.org/standard/54534.html
- NIST SP 800-53 Ред. 4 - Спеціальна публікація NIST 800-53 Редакція 4, *Контроль безпеки та конфіденційності для федеральних інформаційних систем та організацій,* квітень 2013 р. (включаючи оновлення від 22 січня 2015 року). https://doi.org/10.6028/NIST.SP.800-53r4. Інформативні посилання структуруються лише для контрольного рівня, хоча будь-яке вдосконалення керування може бути корисним для досягнення результату Підкатегорії.

Структурування між Підкатегоріями Основи Платформи та зазначеними розділами в Інформаційних посиланнях не призначене для остаточного визначення, чи вказані розділи в Інформаційних посиланнях забезпечують бажаний результат для Підкатегорії.

Інформативні посилання не є вичерпними, тому що не кожен елемент (наприклад, контроль, вимога) даного Інформаційного посилання структурований в Підкатегоріях Основи Платформи.

Додаток B: Словник термінів

Цей додаток визначає вибрані терміни, що використовуються в публікації.

Таблиця 3: Словник термінів Платформи

Покупець	Люди або організації, які споживають певний товар чи послугу.
Категорія	Розподіл Функції на групи результатів з кібербезпеки, тісно пов'язаних з програмними потребами та окремими видами діяльності. Приклади Категорій включають "Управління активами", "Управління ідентифікацією та контроль доступу" та "Процеси виявлення".
Критично важлива інфраструктура	Системи та активи, фізичні або віртуальні, настільки важливі для Сполучених Штатів, що недієздатність або знищення таких систем та активів матиме виснажливий вплив на кібербезпеку, національну економічну безпеку, національну охорону здоров'я чи безпеку чи будь-яке поєднання цих сфер.
Кібербезпека	Процес захисту інформації шляхом попередження, виявлення та реагування на атаки.
Подія, пов’язана з кібербезпекою	Зміна в кібербезпеці, яка може вплинути на організаційні операції (включаючи місію, можливості чи репутацію).
Інцидент з кібербезпеки	Події, пов'язані з кібербезпекою, які визначаються для того, щоб вплинути на організацію, що створює необхідність реагування та відновлення.
Виявлення (функція)	Розробка та здійснення відповідних заходів, щоб визначити появу події, пов’язаної з кібербезпекою.
Платформа	Підхід, що базується на оцінці ризику для зменшення ризику для кібербезпеки, складається з трьох частин: Основа Платформи, Профіль Платформи та Рівень впровадження Платформи. Також відома як "Платформа для кібербезпеки".
Основа Платформи	Набір заходів щодо для кібербезпеки та посилань, що є загальними в галузях критично важливих інфраструктур та організовані за певними підсумками. Основа Платформи містить чотири типи елементів: Функції, Категорії, Підкатегорії та Інформаційні посилання.
Рівень впровадження Платформи	Призма, через яку можна переглянути характеристики підходу організації до управління ризиками, як організація розглядає ризик для кібербезпеки та процеси, які використовуються для управління цим ризиком.

Профіль Платформи	Представлення результатів, обраних певною системою або організацією з Категорій та Підкатегорій Платформи.
Функція	Один з основних складових Платформи. Функції забезпечують найвищий рівень структури для організації основних заходів з для кібербезпеки у Категоріях та Підкатегоріях. П'ять функцій - Визначення, Захист, Виявлення, Реагування та Відновлення.
Визначення (функція)	Розробка організаційного розуміння для управління ризиком для кібербезпеки для систем, активів, даних та можливостей.
Інформаційне посилання	Конкретний розділ стандартів, керівних принципів та практик, що є спільним серед секторів критично важливих інфраструктур, який ілюструє метод досягнення результатів, пов'язаних із кожною Підкатегорією. Прикладом інформаційного посилання є ISO/IEC 27001 Control A.10.8.3, який підтримує Підкатегорію "Дані при передачі захищено" в Категорії "Безпека даних" в функції "Захист".
Мобільний код	Програма (наприклад, скрипт, макрос або інша портативна інструкція), яку можна доставити без змін до гетерогенної колекції платформ і виконати з ідентичною семантикою.
Захист (функція)	Розробка та впровадження відповідних гарантій для забезпечення надання послуг критично важливих інфраструктур.
Привілейований користувач	користувач, який уповноважений (і, отже, якому довіряють), виконує функції, пов’язані з безпекою, які звичайні користувачі не мають права виконувати.
Відновлення (функція)	Розробка та впровадження відповідних заходів для підтримки планів стійкості та відновлення будь-яких можливостей або послуг, які були порушені внаслідок події, пов'язаної з кібербезпекою.
Реагування (функція)	Розробка та впровадження відповідних заходів для вжиття заходів щодо виявленої події, пов'язаної з кібербезпекою .
Ризик	Вимірювання того, якою мірою суб'єкту господарювання загрожує потенційна обставина або подія, і зазвичай є функцією: (i) несприятливого впливу, що виникне, якщо така обставина або подія відбудеться; і (ii) вірогідність виникнення.
Управління ризиками	Процес визначення, оцінки та реагування на ризик.
Підкатегорія	Поділ Категорії на конкретні результати технічної та/або управлінської діяльності. Приклади Підкатегорій включають в себе "Зовнішні інформаційні системи каталогізовані", "Дані, що зберігаються, захищені" та "Повідомлення від систем виявлення вивчаються".

Постачальник	Постачальники продукції та послуг використовуються для внутрішніх цілей організації (наприклад, IT-інфраструктури) або інтегровані в продукти послуг, наданих Покупцям цієї організації.
Таксономія	Схема класифікації .

Додаток C: Акроніми

Цей додаток визначає вибрані акроніми, що використовуються в цій публікації.

ANSI	Американський національний інститут стандартизації
CEA	Закон про підвищення ефективності для кібербезпеки від 2014 року
CIS	Центр Інтернет-безпеки
COBIT	Цілі контролю за інформаційними та суміжними технологіями
CPS	Кібер-фізичні системи
CSC	Критичний контроль безпеки
DHS	Міністерство національної безпеки
EO	Указ
ICS	Промислові системи управління
IEC	Міжнародна електротехнічна комісія
IoT	Інтернет речей
IR	Міжвідомчий звіт
ISA	Міжнародне товариство автоматизації
ISAC	Центр обміну та аналізу інформації
ISAO	Організація обміну та аналізу інформації
ISO	Міжнародна організація стандартизації
IT	Інформаційна технологія
NIST	Національний інститут стандартів і технологій
OT	Операційні технології
PII	Особисті ідентифікаційні дані
RFI	Запит інформації
RMP	Процес управління ризиками
SCRM	Управління ризиками ланцюжків поставок
SP	Спеціальна публікація