NIST Cybersecurity Framework (CSF) 2.0

Національний інститут стандартів і технологій
Ця публікація доступна безкоштовно за посиланням:

https://doi.org/10.6028/NIST.CSWP.29 26 лютого 2024 року

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Анотація

NIST Cybersecurity Framework (CSF) 2.0 надає рекомендації для промисловості, урядових установ та інших організацій щодо управління ризиками кібербезпеки. Вона пропонує таксономію результатів кібербезпеки високого рівня, які можуть бути використані будь-якою організацією - незалежно від її розміру, сектору або зрілості - для кращого розуміння, оцінки, визначення пріоритетів та інформування про свої зусилля з кібербезпеки. CSF не визначає, як саме мають бути досягнуті результати. Замість цього вона містить посилання на онлайн-ресурси, які надають додаткові вказівки щодо практик і заходів контролю, які можуть бути використані для досягнення цих результатів. Цей документ описує CSF 2.0, її компоненти та деякі з багатьох способів її використання.

Ключові слова

кібербезпека; рамка кібербезпеки (CSF); управління ризиками кібербезпеки; управління ризиками кібербезпеки; управління ризиками підприємства; Профілі; Рівні.

Аудиторія

Основною аудиторією CSF є особи, відповідальні за розробку та керівництво програмами з кібербезпеки. CSF також можуть використовувати інші особи, які беруть участь в управлінні ризиками - в тому числі керівники, ради директорів, фахівці з придбання, технологічні фахівці, ризик-менеджери, юристи, фахівці з управління персоналом, а також аудитори з кібербезпеки та управління ризиками - для прийняття рішень, пов'язаних з кібербезпекою. Крім того, CSF може бути корисним для тих, хто формує політику і впливає на неї (наприклад, асоціації, професійні організації, регуляторні органи), які визначають і повідомляють про пріоритети в управлінні ризиками кібербезпеки.

Додатковий вміст

NIST продовжуватиме створювати і розміщувати додаткові ресурси, які допоможуть організаціям впроваджувати CSF, в тому числі Посібники для початківців і Профілі громад. Всі ресурси знаходяться у відкритому доступі на вебсайті CSF NIST. Пропозиції щодо додаткових ресурсів для розміщення на вебсайті CSF NIST завжди можна надсилати до NIST за адресою: cyberframework@nist.gov.

До уваги читачів

Якщо не зазначено інше, документи, що цитуються, на які є посилання або уривки з яких містяться в цій публікації, не є повністю включеними до неї.

До версії 2.0 Рамкова концепція кібербезпеки називалася "Рамкова концепція вдосконалення кібербезпеки критичної інфраструктури". Ця назва не використовується для CSF 2.0.

Подяки

CSF є результатом багаторічних спільних зусиль промисловості, академічних кіл та урядів США і всього світу. NICT висловлює подяку всім, хто зробив свій внесок у розробку цієї нової редакції CSF. Інформацію про процес розробки CSF можна знайти на вебсайті NIST CSF. Уроками, отриманими під час використання CSF, завжди можна поділитися з NIST за адресою cyberframework@nist.gov.

Зміст

Перелік рисунків

Передмова

Cybersecurity Framework (CSF) 2.0 розроблена, щоб допомогти організаціям усіх розмірів і секторів - включаючи промисловість, уряд, наукові установи та некомерційні організації - для управління та зменшення ризиків кібербезпеки. Вона корисна незалежно від рівня зрілості та технічної складності програм кібербезпеки організації. З усім тим, CSF не передбачає універсального підходу. Кожна організація має як спільні, так і унікальні ризики, а також різні апетити до ризику та толерантність до нього, специфічні місії та цілі для досягнення цих місій. За необхідності, способи впровадження CSF в організаціях будуть відрізнятися.

В ідеалі, CSF буде використовуватися для подолання ризиків кібербезпеки поряд з іншими ризиками підприємства, в тому числі фінансовими, приватності, ланцюга постачання, репутаційними, технологічними або фізичними за своєю природою.

CSF *описує* бажані результати, які мають бути зрозумілими широкій аудиторії, включаючи керівників, менеджерів і фахівців-практиків, незалежно від їхнього досвіду в галузі кібербезпеки. Оскільки ці результати не залежать від сектору, країни та технології, вони надають організаціям гнучкість, необхідну для подолання їхніх унікальних ризиків, технологій та місії. Результати безпосередньо пов'язані з переліком потенційних заходів контролю безпеки для негайного розгляду з метою зменшення ризиків кібербезпеки.

Хоча CSF не є директивним документом, він допомагає користувачам дізнатися про конкретні результати і вибрати їх. Пропозиції щодо того, як можна досягти конкретних результатів, містяться в розширювальному наборі онлайн-ресурсів, які доповнюють CSF, включаючи серію Посібників для швидкого старту (QSG). Крім того, різні інструменти пропонують завантажувані формати, щоб допомогти організаціям, які вирішили автоматизувати деякі зі своїх процесів. QSG пропонують початкові способи використання CSF і запрошують читача вивчити CSF і пов'язані з ним ресурси більш глибоко. Доступні на вебсайті NIST CSF, CSF і ці додаткові ресурси від NIST та інших організацій слід розглядати як "портфоліо CSF", що допомагає управляти ризиками і знижувати їх. Незалежно від способу застосування, CSF спонукає користувачів розглянути свою позицію щодо кібербезпеки в контексті, а потім адаптувати CSF до своїх конкретних потреб.

Ґрунтуючись на попередніх версіях, CSF 2.0 містить нові функції, які підкреслюють важливість *управління* та *ланцюгів постачання*. Особлива увага приділяється QSGs, щоб гарантувати, що CSF є актуальним і легкодоступним як для менших організацій, так і для їхніх більших партнерів. Наразі NIST надає *приклади впровадження* та *інформаційні посилання,* які доступні в Інтернеті та регулярно оновлюються. Створення поточних і цільових *організаційних профілів* допомагає організаціям порівнювати їхній поточний стан з тим, де вони хочуть або повинні бути, а також дозволяє їм швидше впроваджувати і оцінювати засоби контролю безпеки.

Ризики кібербезпеки постійно зростають, і управління ними має бути безперервним процесом. Це справедливо незалежно від того, чи організація тільки починає протистояти викликам кібербезпеки, чи вже багато років має досвідчену, добре забезпечену ресурсами команду з кібербезпеки. CSF розроблений таким чином, щоб бути цінним для організацій будь-якого типу, і очікується, що він буде слугувати належним керівництвом протягом тривалого часу.

1. Огляд Рамкової програми з кібербезпеки (CSF)

Цей документ є версією 2.0 Рамкової програми NIST з кібербезпеки (*Рамкова програма* або *CSF)*. Він включає наступні компоненти:

- **Ядро CSF**, яке є таксономією результатів кібербезпеки високого рівня, що може допомогти будь-якій організації в управлінні ризиками кібербезпеки. Компоненти Ядра CSF - це ієрархія функцій, категорій та підкатегорій, які деталізують кожен результат. Ці результати можуть бути зрозумілі широкій аудиторії, включаючи керівників, менеджерів і фахівців-практиків, незалежно від їхнього досвіду в галузі кібербезпеки. Оскільки результати не залежать від сектору, країни та технології, вони надають організації гнучкість, необхідну для вирішення її унікальних ризиків, технологій та місії.
- ***Організаційні профілі CSF,*** які є механізмом опису поточного та/або цільового стану кібербезпеки організації з точки зору результатів Ядра CSF.
- ***Рівні*** CSF, які можуть бути застосовані до організаційних профілів CSF, щоб охарактеризувати суворість практик управління ризиками кібербезпеки в організації. Рівні також можуть надати контекст того, як організація розглядає ризики кібербезпеки та наявні процеси управління цими ризиками.

Цей документ описує бажані результати, до яких може прагнути організація. Він не встановлює результатів і не *описує, як* їх можна досягти. Опис того, *як* організація може досягти цих результатів, міститься в наборі онлайн-ресурсів, які доповнюють CSF і доступні на веб-сайті CSF NIST. Ці ресурси пропонують додаткові вказівки щодо практик і заходів контролю, які можуть бути використані для досягнення результатів, і призначені для того, щоб допомогти організації зрозуміти, прийняти і використовувати CSF. Вони включають в себе

- *Інформаційні посилання*, які вказують на джерела інформації щодо кожного результату з наявний світових стандартів, керівних принципів, рамкових умов, нормативних актів, політик тощо.
- *Приклади реалізації*, що ілюструють потенційні шляхи досягнення кожного результату
- *Посібники зі швидкого старту,* які надають практичні рекомендації щодо використання CSF та її онлайн-ресурсів, включаючи перехід з попередніх версій CSF на версію 2.0
- *Профілі спільнот та шаблони профілів організацій*, які допомагають організаціям впроваджувати CSF на практиці та визначати пріоритети в управлінні ризиками кібербезпеки

Організація може використовувати Ядро, Профілі та Рівні CSF разом з додатковими ресурсами для розуміння, оцінки, визначення пріоритетів та інформування про ризики кібербезпеки.

- **Зрозуміти та оцінити:** Описати поточну або цільову позицію кібербезпеки частини або всієї організації, визначити прогалини та

оцінити прогрес у їх усуненні.

- **Визначити пріоритети:** Визначте, організуйте та визначте пріоритетність заходів з управління ризиками кібербезпеки, які відповідають місії організації, законодавчим та нормативним вимогам, а також очікуванням щодо управління ризиками та керівництва.
- **Спілкування:** Забезпечити спільну мову для спілкування всередині та поза межами організації щодо ризиків, можливостей, потреб та очікувань у сфері кібербезпеки.

CSF призначений для використання організаціями всіх розмірів і секторів, включаючи промисловість, уряд, наукові установи та неприбуткові організації, незалежно від рівня зрілості їхніх програм з кібербезпеки. CSF є основоположним ресурсом, який може бути прийнятий на добровільних засадах, а також в рамках урядової політики та мандатів. Таксономія CSF та стандарти, керівні принципи і практики, на які він посилається, не прив'язані до конкретної країни, а попередні версії CSF успішно використовувалися багатьма урядами та іншими організаціями як у США, так і за їх межами.

CSF слід використовувати разом з іншими ресурсами (наприклад, рамками, стандартами, настановами, провідними практиками) для кращого управління ризиками кібербезпеки та інформування про загальне управління ризиками інформаційно-комунікаційних технологій (ICT) на рівні підприємства. CSF - це гнучка структура, яка призначена для використання усіма організаціями незалежно від розміру. Організації й надалі матимуть унікальні ризики - включаючи різні загрози та вразливості - і толерантність до ризиків, а також унікальні цілі та вимоги до місії. Таким чином, підходи організацій до управління ризиками та впровадження ними CSF будуть відрізнятися.

Решта цього документу має наступну структуру:

- Розділ 2 пояснює основи ядра CSF: функції, категорії та підкатегорії.
- Розділ 3 визначає поняття профілів та рівнів CSF.
- Розділ 4 містить огляд окремих компонентів набору онлайн-ресурсів CSF: інформаційні посилання, приклади впровадження та короткі посібники.
- У Розділі 5 обговорюється, як організація може інтегрувати CSF з іншими програмами управління ризиками.
- Додаток А - Ядро CSF.
- Додаток Б містить умовну ілюстрацію рівнів CSF.
- Додаток С - глосарій термінів, пов'язаних з CSF.

2. Вступ до ядра CSF

У Додатку А наведено Ядро CSF - набір результатів кібербезпеки, розташованих за функціями, потім за категоріями і, нарешті, за підкатегоріями, як показано на рис. 1. Ці результати не є контрольним переліком дій, які необхідно виконати; конкретні дії, що вживаються для досягнення результату, будуть відрізнятися залежно від організації та варіанту використання, так само як і особа, відповідальна за ці дії. Крім того, порядок і розмір функцій, категорій і підкатегорій в Основі не означає послідовність або важливість їх досягнення. Структура ядра призначена для того, щоб найбільше відповідати тим, хто відповідає за впровадження управління ризиками в організації.

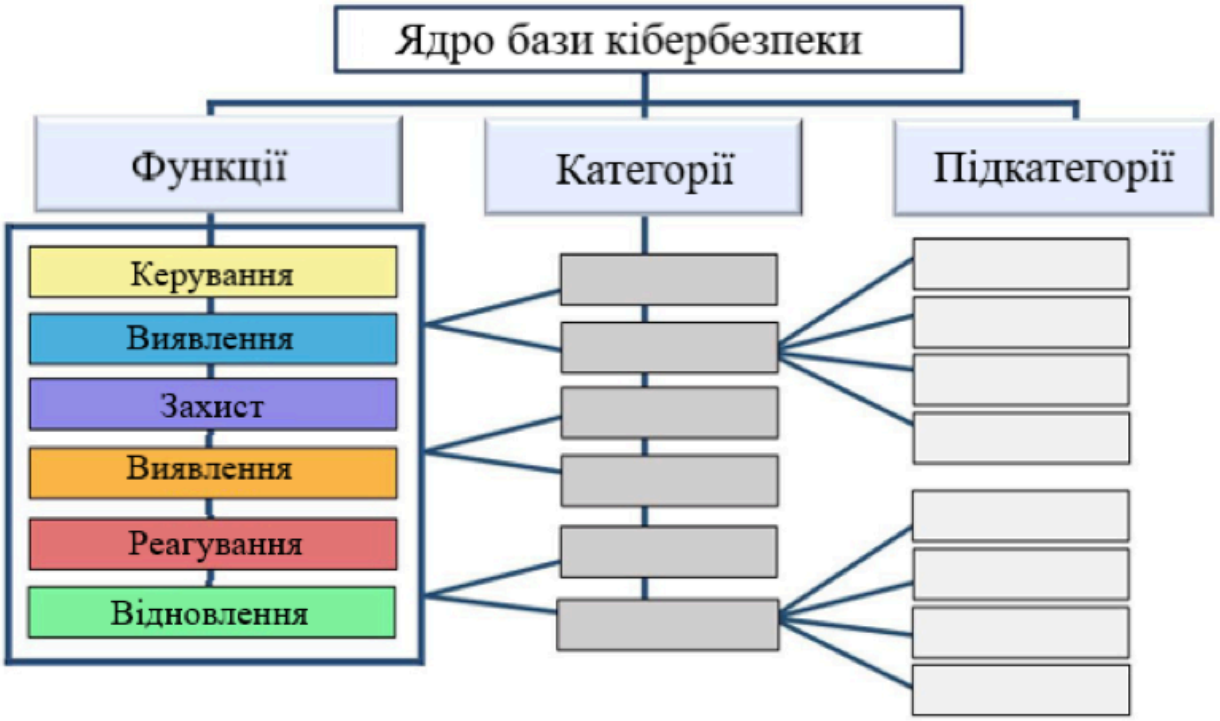

Рис. 1. Структура ядра CSF

Основні функції CSF - УПРАВЛІННЯ, ІДЕНТИФІКАЦІЯ, ЗАХИСТ, ВИЯВЛЕННЯ, РЕАГУВАННЯ та ВІДНОВЛЕННЯ - організовують результати кібербезпеки на найвищому рівні.

- **УПРАВЛІННЯ (GV)** - *стратегія, очікування та політика організації щодо управління ризиками кібербезпеки встановлюються, доводяться до відома та контролюються.* Функція управління забезпечує результати, які інформують про те, що організація може зробити для досягнення та визначення пріоритетності результатів інших п'яти функцій в контексті її місії та очікувань зацікавлених сторін. Діяльність з управління має вирішальне значення для включення кібербезпеки в ширшу стратегію управління ризиками організації (ERM).Управління охоплює розуміння організаційного контексту; розробку стратегії кібербезпеки та управління ризиками кібербезпеки ланцюга постачання; ролі, обов'язки та повноваження; політику; та нагляд за стратегією кібербезпеки.

- **Ідентифікація (ID)** - *розуміння поточних ризиків кібербезпеки організації.* Розуміння активів організації (наприклад, даних, обладнання, програмного забезпечення, систем, засобів, послуг, людей), постачальників та пов'язаних з ними ризиків кібербезпеки дозволяє організації визначити пріоритети своїх зусиль відповідно до стратегії управління ризиками та потреб місії, визначених в рамках функції "Врядування" (GV). Ця функція також включає визначення можливості вдосконалення політик, планів, процесів, процедур і практик організації, які підтримують управління ризиками кібербезпеки, з метою інформування про зусилля за всіма шістьма функціями.
- **ЗАХИСТ(PR)** - *використовуються засоби захисту для управління ризиками кібербезпеки організації. Після того, як* активи та ризики визначені та пріоритезовані, PROTECT підтримує здатність захистити ці активи, щоб запобігти або зменшити ймовірність та вплив несприятливих подій у сфері кібербезпеки, а також збільшити ймовірність та вплив використання переваг, що відкриваються. Результати, які охоплює ця функція, включають управління ідентифікацією, аутентифікацією та контролем доступу; обізнаність та навчання; безпеку даних; безпеку платформи (тобто, захист апаратного, програмного забезпечення та послуг фізичних та віртуальних платформ); та стійкість технологічної інфраструктури.
- **ВИЯВЛЕННЯ (DE)** - виявлення *та аналіз можливих атак на кібербезпеку та компрометації.* DETECT дозволяє своєчасно виявляти та аналізувати аномалії, індикатори компрометації та інші потенційно несприятливі події, які можуть вказувати на те, що відбуваються атаки та інциденти кібербезпеки. Ця функція підтримує успішне реагування на інциденти та заходи з відновлення.
- **РЕАГУВАННЯ (RS)** - *Вживаються заходи щодо виявленого інциденту кібербезпеки. Функція* РЕАГУВАННЯ підтримує здатність стримувати наслідки інцидентів кібербезпеки. Результати в рамках цієї функції охоплюють управління інцидентами, аналіз, пом'якшення наслідків, звітування та комунікацію.
- **ВІДНОВЛЕННЯ (RC)** - *відновлення активів та операцій, що постраждали від інциденту кібербезпеки.* Воно підтримує своєчасне відновлення нормальної роботи, щоб зменшити наслідки інцидентів кібербезпеки та забезпечити належну комунікацію під час відновлювальних робіт.

Хоча багато заходів з управління ризиками кібербезпеки зосереджені на запобіганні негативним подіям, вони також можуть сприяти використанню позитивних можливостей. Заходи зі зниження ризиків кібербезпеки можуть принести користь організації в інший спосіб, наприклад, збільшити дохід (наприклад, спочатку запропонувати комерційному хостинг-провайдеру надлишкову площу для розміщення власних дата-центрів і дата-центрів інших організацій, а потім перенести основну фінансову систему з власного дата-центру організації до хостинг-провайдера, щоб знизити ризики кібербезпеки).

На рисунку 2 функції CSF функції зображені у вигляді колеса, оскільки всі функції пов'язані одна з одною. Наприклад, організація класифікує активи в рамках функції ідентифікації та вживає заходів для захисту цих активів в рамках функції захисту. Інвестиції в планування і тестування функцій керування та ідентифікації сприятимуть своєчасному виявленню неочікуваних подій у функції виявлення, а також забезпеченню реагування на інциденти та відновлення після інцидентів кібербезпеки у функціях відповіді та відновлення. Функція керування знаходиться в центрі колеса, оскільки вона інформує про те, як організація буде впроваджувати інші п'ять функцій.

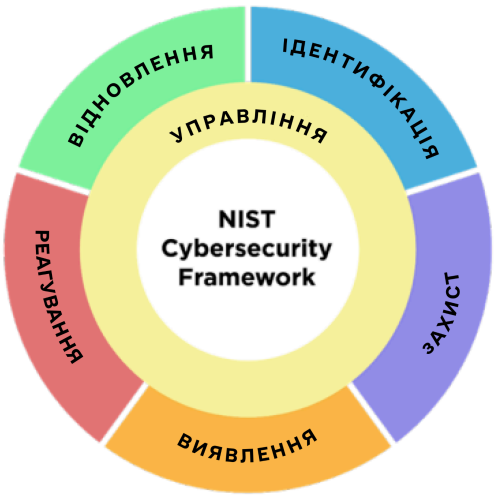

Рис. 2. Функції CSF

Функції повинні виконуватись одночасно. Дії, що підтримують керування, ідентифікацію, захист і виявлення, повинні відбуватися безперервно, а дії, що підтримують реагування і відновлення, повинні бути готовими в будь-який час і здійснюватися в разі виникнення інцидентів кібербезпеки. Усі функції відіграють життєво важливу роль у реагуванні на інциденти кібербезпеки. Результати керування, ідентифікація та захист допомагають запобігати інцидентам і готуватися до них, тоді як результати керування, виявлення, реагування та відновлення допомагають виявляти інциденти та управляти ними.

Кожна функція названа дієсловом, яке узагальнює її зміст. Кожна функція поділяється на *категорії,* які є пов'язаними результатами кібербезпеки, що в сукупності складають функцію. *Підкатегорії* поділяють кожну категорію на більш конкретні результати технічної та управлінської діяльності. Підкатегорії не є

вичерпними, але вони описують детальні результати, які підтримують кожну категорію.

Функції, категорії та підкатегорії застосовуються до всіх ІКТ, що використовуються в організації, включаючи інформаційні технології (IT), Інтернет речей (IoT) та операційні технології (OT). Вони також застосовуються до всіх типів технологічних середовищ, включаючи хмарні, мобільні та системи штучного інтелекту. Ядро CSF орієнтоване на перспективу і призначене для застосування до майбутніх змін у технологіях і середовищах.

3. Вступ до профілів та рівнів CSF

Цей розділ визначає поняття профілів та рівнів CSF.

3.1. Профілі CSF

Організаційний профіль CSF описує поточну та/або цільову позицію організації в сфері кібербезпеки з точки зору результатів Базового компонента. Організаційні профілі використовуються для розуміння, адаптації, оцінки, визначення пріоритетів та інформування про результати, враховуючи цілі місії організації, очікування зацікавлених сторін, ландшафт загроз та вимоги. Після цього організація може визначити пріоритетність своїх дій для досягнення конкретних результатів і донести цю інформацію до зацікавлених сторін.

Кожен Організаційний профіль включає один або обидва з перелічених нижче пунктів:

1. *Поточний профіль* визначає основні результати, яких організація наразі досягає (або намагається досягти), і характеризує, як і в якій мірі досягається кожен результат.
2. *Цільовий профіль* визначає бажані результати, які організація обрала та визначила як пріоритетні для досягнення своїх цілей з управління ризиками кібербезпеки. Цільовий профіль враховує очікувані зміни в системі кібербезпеки організації, такі як нові вимоги, впровадження нових технологій і тенденції в розвідці загроз.

> *Профіль спільноти* - це базовий перелік результатів ФГС, який створюється та публікується для того, щоб врахувати спільні інтереси та цілі низки організацій. Профіль спільноти зазвичай розробляється для певного сектору, підсектору, технології, типу загрози або іншого варіанту використання. Організація може використовувати Профіль спільноти як основу для власного Цільового профілю.
> Приклади Профілів спільнот можна знайти на веб-сайті NIST CSF.

Кроки, показані на рис. 3 і підсумовані нижче, ілюструють один із способів, у який організація може використовувати Організаційний профіль для сприяння постійному вдосконаленню своєї кібербезпеки.

Рис. 3. Етапи створення та використання профілю організації CSF

1. **Визначте сферу застосування організаційного профілю.** Задокументуйте факти та припущення високого рівня, на яких базуватиметься профіль, щоб визначити сферу його застосування. Організація може мати стільки організаційних профілів, скільки бажає, кожен з яких має різну сферу застосування. Наприклад, профіль може стосуватися всієї організації або обмежуватися фінансовими системами організації чи протидією загрозам програм-вимагачів і реагуванням на інциденти, пов'язані з цими фінансовими системами.
2. **Зберіть інформацію, необхідну для підготовки організаційного профілю.** Прикладами такої інформації можуть бути організаційні політики, пріоритети та ресурси управління ризиками, профілі ризиків підприємства, реєстри аналізу впливу на бізнес (BIA), вимоги та стандарти кібербезпеки, яких дотримується організація, практики та інструменти (наприклад, процедури та запобіжні заходи), а також робочі ролі.
3. **Створіть профіль організації.** Визначте, яку інформацію слід включити до профілю для обраних результатів CSF, і задокументуйте необхідну інформацію. Розгляньте наслідки ризиків Поточного профілю для планування та визначення пріоритетів Цільового профілю. Крім того, розгляньте можливість використання Профілю громади як основи для Цільового профілю.
4. **Проаналізувати розбіжності між поточним і цільовим профілями та розробити план дій.** Провести аналіз прогалин, щоб виявити та проаналізувати відмінності між поточним та цільовим профілями, а також розробити пріоритетний план дій (наприклад, реєстр ризиків, детальний звіт про ризики, план дій та етапи [POA&M]) для усунення цих прогалин.
5. **Впроваджуйте план дій та оновлюйте профіль організації.** Дотримуйтесь плану дій, щоб усунути прогалини та наблизити організацію до Цільового профілю. План дій може мати загальний дедлайн або бути безперервним.

Враховуючи важливість постійного вдосконалення, організація може повторювати ці кроки так часто, як це необхідно.

Організаційні профілі можуть мати й інші застосування. Наприклад, Поточний

профіль можна використовувати для документування та інформування зовнішніх зацікавлених сторін, таких як ділові партнери або потенційні клієнти, про спроможності організації у сфері кібербезпеки та відомі можливості для вдосконалення. Крім того, Цільовий профіль може допомогти висловити вимоги та очікування організації щодо управління ризиками кібербезпеки постачальникам, партнерам та іншим третім сторонам як мету, якої вони повинні досягти.

3.2. Рівні CSF

Організація може використовувати Рівні для формування Поточного та Цільового профілів. *Рівні* характеризують суворість практик управління ризиками кібербезпеки в організації, а також надають контекст того, як організація розглядає ризики кібербезпеки та процеси, що застосовуються для управління цими ризиками. Рівні, як показано на Рис. 4 та умовно проілюстровано в Додатку B, відображають практики організації з управління ризиками кібербезпеки як часткові (Рівень 1), ризикоорієнтовані (Рівень 2), повторювані (Рівень 3) та адаптивні (Рівень 4). Рівні описують перехід від неформальних, ситуативних заходів реагування до підходів, які є гнучкими, заснованими на оцінці ризиків та постійно вдосконалюється. Вибір рівнів допомагає задати загальний тон тому, як організація керуватиме ризиками кібербезпеки.

Рис. 4. Рівні CSF для управління та контролю ризиками кібербезпеки

Рівні повинні доповнювати методологію управління ризиками кібербезпеки організації, а не змінювати її. Наприклад, організація може використовувати рівні для внутрішньої комунікації як орієнтир для загальноорганізаційного [1] підходу до управління ризиками кібербезпеки. Перехід до вищих рівнів заохочується, коли ризики або завдання стають більшими або коли аналіз витрат і вигод вказує на можливе та економічно ефективне зниження негативних ризиків кібербезпеки.

Вебсайт NIST CSF надає додаткову інформацію про використання профілів і рівнів. Він містить посилання на шаблони організаційних профілів, розміщені на сайті NIST, а також репозиторій профілів спільнот у різних машинозчитуваних і зручних для людини форматах.

[1] У цьому документі терміни "в масштабах організації" та "підприємство" мають однакове значення.

4. Вступ до онлайн-ресурсів, які доповнюють CSF

NIST та інші організації розробили низку онлайн-ресурсів, які допомагають організаціям зрозуміти, впровадити і використовувати CSF. Оскільки вони розміщені в Інтернеті, ці додаткові ресурси можуть оновлюватися частіше, ніж цей документ, який оновлюється нечасто, щоб забезпечити стабільність для користувачів, і бути доступними в машинозчитуваних форматах. Цей розділ містить огляд трьох типів онлайн-ресурсів: Інформаційні посилання, Приклади впровадження та Посібники швидкого старту.

Інформаційні посилання - це схеми, які вказують на зв'язок між Основними положеннями та різними стандартами, настановами, правилами та іншим контентом. Інформаційні посилання допомагають зрозуміти, як організація може досягти результатів, визначених у ядрі. Інформаційні посилання можуть бути галузевими або технологічними. Вони можуть бути підготовлені NIST або іншою організацією. Деякі інформаційні посилання вужчі за обсягом, ніж підкатегорії. Наприклад, конкретний засіб контролю з SP 800-53 "Засоби *контролю безпеки та конфіденційності для інформаційних систем та організацій*" може бути одним з багатьох джерел, необхідних для досягнення результату, описаного в одній з підкатегорій. Інші інформативні посилання можуть бути вищого рівня, наприклад, вимоги політики, які частково стосуються багатьох підкатегорій. Використовуючи CSF, організація може визначити найбільш релевантні інформаційні посилання.

Приклади реалізації надають умовні приклади стислих, орієнтованих на дії кроків, які допоможуть досягти результатів підкатегорій. Дієслова, що використовуються для вираження Прикладів, включають: ділитися, документувати, розробляти, виконувати, моніторити, аналізувати, оцінювати та здійснювати. Приклади не є вичерпним переліком усіх дій, які можуть бути здійснені організацією для досягнення результату, а також не є базовим переліком необхідних дій для подолання ризиків кібербезпеки.

Посібники зі швидкого старту (QSG) - це короткі документи на конкретні теми, пов'язані з CSF, які часто адаптовані для конкретної аудиторії. Посібники можуть допомогти організації впровадити QSG, оскільки вони перетворюють окремі частини QSG на практичні "перші кроки", які організація може розглянути на шляху до покращення свого стану кібербезпеки та управління пов'язаними з нею ризиками. Посібники переглядаються у встановлені терміни, а нові посібники додаються за потреби.

Пропозиції щодо нових інформативних посилань для CSF 2.0 завжди можна надсилати до NIST за адресою olir@nist.gov. Пропозиції щодо інших ресурсів, на які можна посилатися на вебсайті CSF NIST, включаючи додаткові теми QSG, слід надсилати на адресу cyberframework@nist.gov.

5. Покращення комунікації та інтеграції ризиків кібербезпеки

Використання CSF буде залежати від унікальної місії організації та її ризиків. Розуміючи очікування зацікавлених сторін, апетит до ризику та толерантність до нього (як зазначено в керуванні), організація може визначити пріоритети діяльності з кібербезпеки для прийняття обґрунтованих рішень щодо витрат та заходів з кібербезпеки. Організація може обрати один або декілька способів управління ризиками, включаючи пом'якшення, передачу, уникнення або прийняття негативних ризиків, а також реалізацію, розподіл, посилення або прийняття позитивних ризиків, залежно від потенційних наслідків та ймовірності їх виникнення. Важливо, що організація може використовувати CSF як всередині для управління своїми можливостями кібербезпеки, так і зовні для нагляду або комунікації з третіми сторонами.

Незалежно від способу застосування CSF's, організація може отримати користь від використання CSF як керівництва, що допоможе їй зрозуміти, оцінити, визначити пріоритети і повідомити про ризики кібербезпеки та заходи, які допоможуть управляти цими ризиками. Вибрані результати можуть бути використані для зосередження уваги на стратегічних рішеннях, спрямованих на покращення стану кібербезпеки та підтримання безперервності важливих для місії функцій, з урахуванням пріоритетів та наявних ресурсів, а також для їх реалізації.

5.1. Покращення комунікації з управління ризиками

CSF забезпечує основу для покращення комунікації щодо очікувань, планування та ресурсів у сфері кібербезпеки. CSF сприяє двосторонньому потоку інформації (як показано у верхній частині рис. 5) між керівниками, які зосереджені на пріоритетах і стратегічному напрямку діяльності організації, та менеджерами, які управляють конкретними ризиками кібербезпеки, що можуть вплинути на досягнення цих пріоритетів. CSF також підтримує подібний потік (як показано в нижній частині рис. 5) між керівниками і фахівцями-практиками, які впроваджують та експлуатують технології. Ліва частина рисунка вказує на важливість того, щоб фахівці-практики ділилися своїми новинами, думками та проблемами з менеджерами та керівниками.

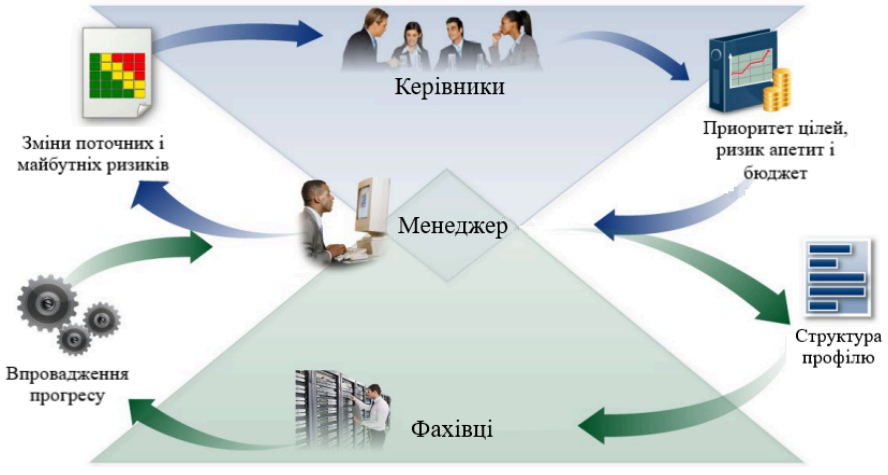

Рис. 5. Використання CSF для покращення комунікації з управління ризиками

Підготовка до створення та використання організаційних профілів передбачає збір інформації про організаторські пріоритети, ресурси та напрямки ризиків від керівників. Потім керівники співпрацюють з фахівцями, щоб повідомити про бізнес-потреби і створити організаційні профілі, що враховують ризики. Заходи, спрямовані на усунення розбіжностей між поточним і цільовим профілями, здійснюються менеджерами і фахівцями-практиками і стануть ключовим внеском у плани системного рівня. Оскільки кінцевий стан досягається в рамках всієї організації - в тому числі за допомогою заходів контролю і моніторингу, що застосовуються на системному рівні, - оновлені результати можуть поширюватися через реєстри ризиків і звіти про хід виконання робіт. В рамках постійного оцінювання менеджери отримують інформацію для внесення змін, які зменшують потенційну шкоду та збільшують потенційні переваги.

Функція GOVERN підтримує комунікацію з **керівниками щодо** ризиків організації. Обговорення з керівництвом стосуються стратегії, зокрема того, як невизначеності, пов'язані з кібербезпекою, можуть вплинути на досягнення цілей організації. Ці дискусії, щодо управління сприяють діалогу та досягненню згоди щодо стратегій управління ризиками (включно з ризиками кібербезпеки ланцюгів постачання); ролей, обов'язків та повноважень; політик; та контролю. Коли керівники визначають пріоритети та цілі кібербезпеки на основі цих потреб, вони повідомляють про свої очікування щодо схильності до ризику, відповідальності та ресурсів. Керівники також відповідають за інтеграцію управління ризиками кібербезпеки з програмами ERM та програмами управління ризиками нижчого рівня (див. Розділ 5.2). Комунікації, відображені у верхній частині рис. 5, можуть включати аспекти щодо ERM та програм нижчого рівня і, таким чином, інформувати керівників і фахівців.

Загальні цілі кібербезпеки, які встановлюють керівники, доводяться до відома **менеджерів**. У комерційній установі вони можуть стосуватися напряму діяльності або операційного підрозділу. Для державних організацій це можуть бути міркування на рівні підрозділу або філії. Під час впровадження CSF керівники зосереджуватимуться на тому, як досягти цільових показників ризику за допомогою загальних послуг, заходів контролю та співпраці, як зазначено в цільовому профілі та вдосконалено за допомогою дій, які відстежуються в плані дій (наприклад, реєстр ризиків, докладний звіт про ризики, POA&M).

Фахівці зосереджуються на впровадженні цільового стану та визначенні змін операційного ризику, щоб допомогти планувати, здійснювати та контролювати конкретні заходи з кібербезпеки. У міру впровадження заходів контролю для управління ризиками на прийнятному рівні, фахівці надають менеджерам і керівникам інформацію (наприклад, ключові показники ефективності, ключові показники ризику), необхідну для розуміння стану кібербезпеки організації, прийняття обґрунтованих рішень, а також підтримання або відповідного корегування стратегії управління ризиками. Керівники також можуть поєднувати ці дані про ризики кібербезпеки з інформацією про інші види ризиків в організації. Оновлення очікувань і пріоритетів включаються в оновлені організаційні профілі, коли процес повторюється.

5.2. Покращення інтеграції з іншими програмами управління ризиками

Кожна організація стикається з численними видами ІКТ-ризиків (наприклад, конфіденційність, ланцюжок постачання, штучний інтелект) і може використовувати системи та інструменти управління, специфічні для кожного ризику. Деякі організації інтегрують ІКТ та всі інші зусилля з управління ризиками на високому рівні, використовуючи ERM, тоді як інші розділяють ці зусилля, щоб забезпечити належну увагу до кожного з них. Невеликі Організації за своєю природою можуть здійснювати моніторинг ризиків на рівні підприємства, тоді як більші компанії можуть вести окрему роботу з управління ризиками, інтегровану в ERM. Організації можуть використовувати ERM підхід, щоб збалансувати *портфоліо* міркувань щодо ризиків, включаючи кібербезпеку, і приймати обґрунтовані рішення. Керівники отримують важливу інформацію про поточну та заплановану діяльність, пов'язану з ризиками, оскільки вони інтегрують стратегії управління та управління ризиками з результатами попереднього використання CSF. CSF допомагає організаціям перекласти свою термінологію з кібербезпеки та управління ризиками кібербезпеки на загальну мову управління ризиками, зрозумілу керівництву.

Ресурси NIST, які описують взаємозв'язок між управлінням ризиками кібербезпеки та ERM, включають:

- *NIST Cybersecurity Framework 2.0* - *Короткий посібник з управління ризиками на підприємстві*
- NIST Interagency Report (IR) 8286, *Інтеграція кібербезпеки та управління ризиками підприємства (ERM)*
- IR 8286A, *Ідентифікація та оцінка ризиків кібербезпеки для управління ризиками підприємства*
- IR 8286B, *Пріоритетність ризику кібербезпеки для управління ризиками підприємства*
- IR 8286C, *Визначення ризиків кібербезпеки для корпоративного управління ризиками та нагляду з боку керівництва*
- IR 8286D, *Використання аналізу впливу на бізнес для визначення пріоритетів та реагування на ризики*
- SP 800-221, *Вплив ризиків інформаційно-комунікаційних технологій на підприємство: керівництво та управління програмами управління ризиками ІКТ в рамках портфеля ризиків підприємства*
- SP 800-221A, *Результати оцінки ризиків інформаційно-комунікаційних технологій (ІКТ): Інтеграція програм управління ризиками ІКТ з портфоліо ризиків підприємства*

Організація також може вважати CSF корисним для інтеграції управління ризиками кібербезпеки з окремими програмами управління ризиками ІКТ, такими як:

- **Управління та оцінка ризиків кібербезпеки:** CSF можна інтегрувати з існуючими програмами управління та оцінки ризиків кібербезпеки, такими як SP 800-37 "*Система управління ризиками для інформаційних систем та організацій*" та SP 800-30 "*Посібник з проведення оцінювання ризиків* на основі системи управління ризиками NIST (RMF)". Для організацій, які

використовують RMF NIST та її набір публікацій, CSF можна використовувати як доповнення до підходу RMF щодо вибору та визначення пріоритетності заходів контролю з SP 800-53 "Засоби *контролю безпеки та конфіденційності для інформаційних систем та організацій"*.

- **Ризики для приватності:** Хоча кібербезпека і конфіденційність є незалежними поняттями, за певних обставин їхні цілі перетинаються, як показано на рис. 6.

Рис. 6. Взаємозв'язок між кібербезпекою та конфіденційністю

Управління ризиками кібербезпеки має важливе значення для конфіденційності, пов'язаних із втратою конфіденційності, цілісності та доступності персональних даних. Наприклад, витік даних може призвести до крадіжки особистих даних. Однак ризики для конфіденційності можуть також виникати через причини, не пов'язані з кіберінцидентами.

Організація обробляє дані для досягнення цілей, що іноді може призвести до *подій, пов'язаних* з конфіденційністю, в результаті яких окремі особи можуть зіткнутися з проблемами, пов'язаними з обробкою даних. Ці проблеми можуть виражатися по-різному, але NIST описує їх як такі, що варіюються від впливу на гідність (наприклад, збентеження або стигматизація) до більш відчутної шкоди (наприклад, дискримінація, економічні збитки або фізична шкода). Рамкова основа конфіденційності NIST та Рамкова основа кібербезпеки можуть використовуватися разом для вирішення різних аспектів ризиків кібербезпеки та конфіденційності. Крім того, Методологія NIST з оцінки ризиків конфіденційності (PRAM) містить каталог прикладів проблем для використання в оцінці ризиків конфіденційності.

- **Ризики в ланцюгах постачання:** Організація може використовувати CSF для посилення нагляду за ризиками кібербезпеки та комунікації із зацікавленими сторонами в ланцюгах постачання. Всі види технологій покладаються на складну, глобально розподілену, розгалужену та взаємопов'язану екосистему ланцюгів постачання з географічно

різноманітними маршрутами та багаторівневим аутсорсингом. Ця екосистема складається з суб'єктів державного та приватного секторів (наприклад, покупців, постачальників, розробників, системних інтеграторів, зовнішніх постачальників системних послуг та інших постачальники послуг, пов'язаних з технологіями), які взаємодіють з метою дослідження, розробки, проєктування, виробництва, придбання, доставки, інтеграції, експлуатації, обслуговування, утилізації та іншого використання або управління технологічними продуктами та послугами. Ця взаємодія формується під впливом технологій, законів, політик, процедур і практик.

З огляду на складні та пов'язані відносини в цій екосистемі, управління ризиками ланцюгів постачання (SCRM) є критично важливим для організацій. SCRM кібербезпеки (C-SCRM) - це систематичний процес управління ризиками кібербезпеки в ланцюгах постачання і розробки відповідних стратегій, політик, процесів і процедур реагування. Підкатегорії в рамках категорії CSF C-SCRM [GV.SC] забезпечують зв'язок між результатами, які зосереджені виключно на кібербезпеці, і тими, які зосереджені на C-SCRM. SP 800-161r1 (редакція 1), *Практика управління ризиками кібербезпеки ланцюгів постачання для систем і організацій*, надає детальну інформацію про C-SCRM.

- **Ризики від нових технологій: З появою** нових технологій і сфер їх застосування стають зрозумілими нові ризики. Сучасним прикладом є штучний інтелект (ШІ), який несе в собі ризики кібербезпеки і конфіденційності, а також багато інших видів ризиків. Система управління ризиками штучного інтелекту NIST (AI RMF) була розроблена для того, щоб допомогти впоратися з цими ризиками. Розгляд ризиків, пов'язаних зі штучним інтелектом, разом з іншими ризиками підприємства (наприклад, фінансовими, ризиками кібербезпеки, репутаційними та конфіденційними) дасть більш інтегрований результат і підвищить організаційну ефективність. Міркування та підходи до управління ризиками кібербезпеки та конфіденційності застосовуються до проєктування, розробки, розгортання, оцінки та використання систем штучного інтелекту. Ядро RMF AI використовує функції, категорії та підкатегорії для опису результатів ШІ і допомагає управляти ризиками, пов'язаними зі штучним інтелектом.

Додаток A. Ядро CSF

Цей додаток описує функції, категорії та підкатегорії ядра CSF. У Таблиці 1 наведені назви функцій і категорій ядра CSF 2.0 та їхні унікальні літерні ідентифікатори. Кожна назва функції в таблиці пов'язана з відповідною частиною додатка. Порядок функцій, категорій та підкатегорій ядра не є алфавітним; він призначений для того, щоб найбільше мати відповідність з тим, хто відповідає за впровадження управління ризиками в організації.

Таблиця 1. Назви та ідентифікатори основних функцій і категорій CSF 2.0

Функція	Категорія	Ідентифікатор категорії
Управління (GV)	Організаційний контекст	GV.OC
	Стратегія управління ризиками	GV.RM
	Ролі, обов'язки та повноваження	GV.RR
	Політика	GV.PO
	Нагляд	GV.OV
	Управління ризиками кібербезпеки в ланцюгу поставок	GV.SC
Ідентифікація (ID)	Управління активами	ID.AM
	Оцінка ризиків	ID.RA
	Покращення	ID.IM
Захист (PR)	Управління ідентифікацією, автентифікація та контролем доступу	PR.AA
	Інформування та навчання	PR.AT
	Безпека даних	PR.DS
	Безпека платформи	PR.PS
	Стійкість технологічної інфраструктури	PR.IR
Виявлення (DE)	Постійний моніторинг	DE.CM
	Аналіз несприятливих подій	DE.AE
Реагування (RS)	Управління інцидентами	RS.MA
	Аналіз інцидентів	RS.AN
	Реагування на інциденти, звітування та комунікація	RS.CO
	Пом'якшення наслідків інцидентів	RS.MI
Відновлення (RC)	Виконання плану відновлення після інциденту	RC.RP
	Комунікація з відновлення після інциденту	RC.CO

Ядро CSF, інформаційні довідники та приклади впровадження доступні на вебсайті CSF 2.0 та за допомогою довідкового інструменту CSF 2.0, який дозволяє користувачам вивчати їх та експортувати у форматах, придатних для читання людиною та машиною. Ядро CSF 2.0 також доступне у застарілому форматі, подібному до формату CSF 1.1.

КЕРУВАННЯ (GV): Стратегія, очікування та політика організації щодо управління ризиками кібербезпеки визначені, доведені до відома та відстежуються

- **Організаційний контекст (GV.OC):** Обставини - місії, очікувань зацікавлених сторін, залежностей, а також правових, регуляторних та договірних вимог - які оточують рішення організації щодо управління ризиками кібербезпеки.
  - **GV.OC-01:** Місія організації зрозуміла та використовується в управлінні ризиками кібербезпеки
  - **GV.OC-02:** Внутрішні та зовнішні зацікавлені сторони зрозумілі, а їхні потреби та очікування щодо управління ризиками кібербезпеки зрозумілі та враховані
  - **GV.OC-03:** Правові, регуляторні та договірні вимоги щодо кібербезпеки - включно із зобов'язаннями щодо захисту приватності та громадянських свобод - розуміються та виконуються.
  - **GV.OC-04:** Ключові цілі, можливості та послуги, від яких залежать зовнішні зацікавлені сторони або які вони очікують від організації, зрозумілі та доведені до відома.
  - **GV.OC-05:** Результати, можливості та послуги, від яких залежить організація, зрозумілі та повідомлені

- **Стратегія управління ризиками (GV.RM):** Пріоритети, обмеження, толерування ризику та апетит організації, а також припущення встановлюються, доводяться до відома та використовуються для підтримки рішень щодо операційних ризиків
  - **GV.RM-01:** Цілі управління ризиками встановлюються та узгоджуються зацікавленими сторонами організації
  - **GV.RM-02:** Встановлення, доведення до відома та підтримання в робочому стані заяв про апетит до ризику та толерантність до ризику
  - **GV.RM-03:** Діяльність та результати управління ризиками кібербезпеки включені до процесів управління ризиками підприємства
  - **GV.RM-04:** Розроблено та доведено до відома стратегічний напрямок, який описує відповідні варіанти реагування на ризики
  - **GV.RM-05:** В організації встановлені лінії комунікації щодо ризиків кібербезпеки, в тому числі ризиків з боку постачальників та третіх сторін
  - **GV.RM-06:** Створено та поширено стандартизований метод розрахунку, документування, категоризації та визначення пріоритетності ризиків кібербезпеки
  - **GV.RM-07:** Стратегічні можливості (тобто позитивні ризики) охарактеризовані та включені в обговорення ризиків кібербезпеки організації

- **Ролі, обов'язки та повноваження (GV.RR):** Визначені та доведені до відома ролі, обов'язки та повноваження у сфері кібербезпеки для сприяння відповідальності, оцінці ефективності та постійному вдосконаленню
  - **GV.RR-01:** Керівництво організації несе відповідальність та підзвітність ризиків кібербезпеки та сприяє формуванню культури, яка враховує ризики, є етичною та постійно вдосконалюється
  - **GV.RR-02:** Ролі, обов'язки та повноваження, пов'язані з управлінням ризиками кібербезпеки, визначені, доведені до відома, зрозумілі та впроваджені
  - **GV.RR-03:** Виділено достатні ресурси, що відповідають стратегії управління ризиками кібербезпеки, ролям, обов'язкам та політиці у сфері кібербезпеки
  - **GV.RR-04:** Кібербезпека включена до кадрових практик
- **Політика (GV.PO):** Організаційна політика кібербезпеки встановлена, доведена до відома та впроваджена
  - **GV.PO-01:** Політика управління ризиками кібербезпеки розроблена на основі організаційного контексту, стратегії та пріоритетів кібербезпеки, доведена до відома та впроваджена
  - **GV.PO-02:** Політика управління ризиками кібербезпеки переглядається, оновлюється, доводиться до відома та впроваджується з урахуванням змін у вимогах, загрозах, технологіях та цілей організації
- **Контроль (GV.OV):** Результати діяльності з управління ризиками кібербезпеки в масштабах всієї організації використовуються для інформування, вдосконалення та корегування стратегії управління ризиками
  - **GV.OV-01:** Результати стратегії управління ризиками кібербезпеки переглядаються з метою інформування та корегування стратегії та напрямів діяльності
  - **GV.OV-02:** Стратегія управління ризиками кібербезпеки переглядається та коригується для забезпечення покриття організаційних потреб та ризиків
  - **GV.OV-03:** Ефективність управління ризиками кібербезпеки організації оцінюється та аналізується на предмет необхідних коригувань
- **Управління ризиками кібербезпеки ланцюга постачання (GV.SC):** Процеси управління кібер ризиками ланцюга постачання визначаються, встановлюються, управляються, контролюються та вдосконалюються зацікавленими сторонами організації
  - **GV.SC-01:** Програма, стратегія, цілі, політики та процеси управління ризиками в сфері кібербезпеки ланцюга постачання розроблені та узгоджені зацікавленими сторонами організації
  - **GV.SC-02:** Ролі та обов'язки з кібербезпеки постачальників, клієнтів та партнерів визначені, доведені до відома та скоординовані на внутрішньому та зовнішньому рівнях

- **GV.SC-03:** Управління ризиками кібербезпеки ланцюга постачання інтегровано в процеси управління кібербезпекою та ризиками підприємства, оцінки та вдосконалення ризиків
- **GV.SC-04:** Постачальники відомі та пріоритезовані за ступенем важливості
- **GV.SC-05:** Вимоги щодо управління ризиками кібербезпеки в ланцюгах постачання визначені, пріоритезовані та інтегровані в контракти та інші види угод з постачальниками та іншими відповідними третіми сторонами
- **GV.SC-06:** Планування та комплексна перевірка здійснюються з метою зниження ризиків до вступу в офіційні відносини з постачальниками або іншими третіми сторонами
- **GV.SC-07:** Ризики, пов'язані з постачальником, його продукцією та послугами, а також іншими третіми сторонами, розуміються, фіксуються, визначаються пріоритети, оцінюються, на них реагують та відстежуються протягом усього періоду взаємовідносин.
- **GV.SC-08:** Відповідні постачальники та інші треті сторони залучені до планування, реагування та відновлення після інцидентів
- **GV.SC-09:** Практики безпеки ланцюгів постачання інтегровані в програми кібербезпеки та управління ризиками підприємства, а їх ефективність контролюється протягом усього життєвого циклу технологічних продуктів та послуг
- **GV.SC-10:** Плани управління ризиками кібербезпеки ланцюга постачання включають положення щодо діяльності, яка відбувається після укладення договору про партнерство або договору про надання послуг.

ІДЕНТИФІКАЦІЯ (ID): Розуміння поточних ризиків кібербезпеки організації

- **Управління активами (ID.AM):** Активи (наприклад, дані, обладнання, програмне забезпечення, системи, споруди, послуги, люди), які дозволяють організації досягати бізнес-цілей, визначаються та управляються відповідно до їх відносної важливості для цілей організації та стратегії управління ризиками організації.
  - **ID.AM-01:** Ведеться інвентаризація обладнання, яким керує організація
  - **ID.AM-02:** Ведеться інвентаризація програмного забезпечення, послуг та систем, якими керує організація
  - **ID.AM-03:** Підтримуються уявлення про авторизовану мережеву комунікацію організації та внутрішні і зовнішні мережеві потоки даних
  - **ID.AM-04:** Ведеться облік послуг, що надаються постачальниками
  - **ID.AM-05:** Пріоритетність активів визначається на основі класифікації, критичності, ресурсів та впливу на місію
  - **ID.AM-07:** Ведеться інвентаризація даних та відповідних метаданих для визначених типів даних
  - **ID.AM-08:** Управління системами, обладнанням, програмним

забезпеченням, послугами та даними протягом їх життєвого циклу

- **Оцінка ризиків (ID.RA):** Організація розуміє ризик кібербезпеки для організації, активів та окремих осіб
  - **ID.RA-01:** Вразливості активів виявлено, підтверджено та зафіксовано
  - **ID.RA-02:** Розвіддані про кіберзагрози отримуються з форумів та джерел обміну інформацією
  - **ID.RA-03:** Внутрішні та зовнішні загрози для організації визначені та зафіксовані
  - **ID.RA-04:** Визначено та зафіксовано потенційні наслідки та ймовірність загроз, що використовують вразливості
  - **ID.RA-05:** Загрози, вразливості, ймовірності та наслідки використовуються для розуміння притаманних ризиків та визначення пріоритетів реагування на ризики
  - **ID.RA-06:** Реакції на ризики обираються, визначаються пріоритети, плануються, відстежуються та комунікуються
  - **ID.RA-07:** Зміни та винятки управляються, оцінюються на предмет впливу на ризики, реєструються та відстежуються
  - **ID.RA-08:** Запроваджено процеси отримання, аналізу та реагування на розкриття вразливостей
  - **ID.RA-09:** Автентичність та цілісність апаратного та програмного забезпечення оцінюються перед придбанням та використанням
  - **ID.RA-10:** Критичні постачальники оцінюються перед придбання

- **Удосконалення (ID.IM):** Удосконалення процесів, процедур та заходів з управління ризиками кібербезпеки організації визначено в усіх функціях CSF
  - **ID.IM-01:** За результатами оцінювання визначено шляхи вдосконалення
  - **ID.IM-02:** Покращення визначаються на основі тестів та навчань з безпеки, в тому числі у співпраці з постачальниками та відповідними третіми сторонами
  - **ID.IM-03:** Виявлено покращення в результаті виконання операційних процесів, процедур та заходів
  - **ID.IM-04:** Плани реагування на інциденти та інші плани з кібербезпеки, що впливають на операції, розроблені, доведені до відома, підтримуються та вдосконалюються

PROTECT (PR): Використовуються засоби захисту для управління ризиками кібербезпеки організації

- **Управління ідентифікацією, автентифікацією та контролем доступу (PR.AA):** Доступ до фізичних та логічних активів обмежується авторизованими користувачами, службами та обладнанням і управляється

відповідно до оціненого ризику несанкціонованого доступу.

- **PR.AA-01:** Організація управляє ідентифікацією та обліковими даними авторизованих користувачів, послуг та обладнання.
- **PR.AA-02:** Ідентифікаційні дані підтверджуються та прив'язуються до облікових даних на основі контексту взаємодії
- **PR.AA-03:** Користувачі, сервіси та обладнання автентифіковані
- **PR.AA-04:** Захист, передача та перевірка ідентифікаційних даних
- **PR.AA-05:** Дозволи на доступ, права та повноваження визначені в політиці, управляються, застосовуються та переглядаються, а також включають принципи найменших привілеїв та розподілу обов'язків
- **PR.AA-06:** Фізичний доступ до активів управляється, контролюється та забезпечується відповідно до ризиків

- **Інформування та навчання (PR.AT):** Персонал організації отримує інформацію та навчання з питань кібербезпеки, щоб вони могли виконувати свої завдання, пов'язані з кібербезпекою.
  - **PR.AT-01:** Персонал проінформований та навчений таким чином, щоб володіти знаннями та навичками для виконання загальних завдань з урахуванням ризиків кібербезпеки
  - **PR.AT-02:** Особи, які виконують спеціалізовані функції, проінформовані та навчені таким чином, щоб вони володіли знаннями та навичками для виконання відповідних завдань з урахуванням ризиків кібербезпеки

- **Безпека даних (PR.DS):** Управління даними здійснюється відповідно до стратегії управління ризиками організації для захисту конфіденційності, цілісності та доступності інформації
  - **PR.DS-01:** Конфіденційність, цілісність та доступність даних у стані спокою захищені
  - **PR.DS-02:** Конфіденційність, цілісність та доступність даних у дорозі захищені
  - **PR.DS-10:** Конфіденційність, цілісність та доступність даних, що використовуються, захищені
  - **PR.DS-11:** Резервні копії даних створюються, захищаються, підтримуються та тестуються

- **Безпека платформи (PR.PS):** Управління обладнанням, програмним забезпеченням (наприклад, мікропрограмами, операційними системами, додатками) та послугами фізичних та віртуальних платформ здійснюється відповідно до стратегії управління ризиками організації для захисту їх конфіденційності, цілісності та доступності.
  - **PR.PS-01:** Впроваджені та застосовуються практики управління конфігурацією
  - **PR.PS-02:** Програмне забезпечення підтримується, замінюється та видаляється відповідно до ризиків
  - **PR.PS-03:** Обслуговування, заміна та демонтаж обладнання здійснюється відповідно до рівня ризику
  - **PR.PS-04:** Записи журналів створюються та доступні для постійного моніторингу
  - **PR.PS-05:** Запобігання встановленню та виконанню несанкціонованого програмного

забезпечення

- **PR.PS-06:** Інтегровані безпечні практики розробки програмного забезпечення, а їх ефективність відстежується протягом усього життєвого циклу розробки програмного забезпечення

- **Стійкість технологічної інфраструктури (PR.IR):** Управління архітектурою безпеки здійснюється відповідно до стратегії управління ризиками організації для захисту конфіденційності, цілісності та доступності активів, а також організаційної стійкості.
  - **PR.IR-01:** Мережі та середовища захищені від несанкціонованого логічного доступу та використання
  - **PR.IR-02:** Технологічні активи організації захищені від екологічних загроз
  - **PR.IR-03:** Впроваджено механізми для досягнення вимог до стійкості в нормальних та несприятливих ситуаціях
  - **PR.IR-04:** Належний ресурсний потенціал для забезпечення доступності

ВИЯВЛЕННЯ (DE): Виявлення та аналіз можливих атак та компрометації кібербезпеки

- **Безперервний моніторинг (DE.CM):** Активи відстежуються для виявлення аномалій, індикаторів компрометації та інших потенційно несприятливих подій
  - **DE.CM-01:** Моніторинг мереж та мережевих послуг з метою виявлення потенційно несприятливих подій
  - **DE.CM-02:** Здійснюється моніторинг фізичного середовища з метою виявлення потенційно несприятливих подій
  - **DE.CM-03:** Діяльність персоналу та використання технологій контролюється з метою виявлення потенційно несприятливих подій
  - **DE.CM-06:** Діяльність та послуги зовнішніх постачальників послуг контролюються з метою виявлення потенційно несприятливих подій
  - **DE.CM-09:** Обчислювальне обладнання та програмне забезпечення, середовища виконання та їх дані контролюються для виявлення потенцій

- **Аналіз несприятливих подій (DE.AE):** Аномалії, індикатори компрометації та інші потенційно несприятливі події аналізуються для характеристики подій та виявлення інцидентів кібербезпеки
  - **DE.AE-02:** Потенційно несприятливі події аналізуються для кращого розуміння пов'язаної з ними діяльності
  - **DE.AE-03:** Інформація співвідноситься з декількох джерел
  - **DE.AE-04:** Очікуваний вплив та масштаби несприятливих подій є зрозумілими
  - **DE.AE-06:** Інформація про небажані явища надається уповноваженому персоналу

та інструментарію

- **DE.AE-07:** Розвід дані про кіберзагрози та інша контекстна інформація інтегрована в аналіз
- **DE.AE-08:** Інциденти оголошуються, коли несприятливі події відповідають визначеним критеріям інциденту

РЕАГУВАННЯ (RS): Вживаються заходи щодо виявленого інциденту кібербезпеки

- **Управління інцидентами (RS.MA):** Управління реагуванням на виявлені інциденти кібербезпеки
  - **RS.MA-01:** План реагування на інцидент виконується у координації з відповідними третіми сторонами після оголошення інциденту
  - **RS.MA-02:** Звіти про інциденти сортуються та перевіряються
  - **RS.MA-03:** Інциденти класифікуються за категоріями та пріоритетами
  - **RS.MA-04:** Ескалація або підвищення рівня інцидентів за необхідності
  - **RS.MA-05:** Застосовано критерії для ініціювання відновлення після інциденту
- **Аналіз інцидентів (RS.AN):** Розслідування проводяться для забезпечення ефективного реагування та підтримки судово-медичної експертизи і заходів з відновлення
  - **RS.AN-03:** Проводиться аналіз для встановлення того, що відбулося під час інциденту та першопричини інциденту
  - **RS.AN-06:** Дії, що виконуються під час розслідування, фіксуються, а цілісність та джерело записів зберігаються
  - **RS.AN-07:** Дані про інциденти та метадані збираються, а їх цілісність та джерело зберігаються
  - **RS.AN-08:** Масштаб інциденту оцінено та підтверджено
- **Звітування та комунікація щодо реагування на інциденти (RS.CO):** Діяльність з реагування координується з внутрішніми та зовнішніми зацікавленими сторонами відповідно до вимог законів, нормативних актів або політик
  - **RS.CO-02:** Внутрішні та зовнішні зацікавлені сторони повідомляються про інциденти
  - **RS.CO-03:** Обмін інформацією з визначеними внутрішніми та зовнішніми зацікавленими сторонами
- **Ліквідація наслідків інциденту (RS.MI):** Діяльність, спрямована на запобігання поширенню події та пом'якшення її наслідків
  - **RS.MI-01:** Інциденти локалізовано
  - **RS.MI-02:** Інциденти усунуто

ВІДНОВЛЕННЯ (RC): Активи та операції, що постраждали від інциденту кібербезпеки, відновлюються

- **Виконання плану відновлення після інциденту (RC.RP):** Відновлювальні заходи проводяться для забезпечення операційної доступності систем і сервісів, що постраждали від інцидентів кібербезпеки
  - **RC.RP-01:** Частина плану реагування на інцидент, що стосується відновлення, виконується після початку процесу реагування на інцидент
  - **RC.RP-02:** Відбір, визначення обсягу, пріоритетності та виконання заходів з відновлення
  - **RC.RP-03:** Цілісність резервних копій та інших засобів відновлення перевіряється перед використанням їх для відновлення
  - **RC.RP-04:** Важливі функції місії та управління ризиками кібербезпеки розглядаються для встановлення оперативних норм після інцидентів
  - **RC.RP-05:** Перевірено цілісність відновлених активів, відновлено системи та послуги, підтверджено нормальний робочий стан
  - **RC.RP-06:** Кінець відновлення інциденту оголошується на основі критеріїв, а документація, пов'язана з інцидентом, завершується

- **Комунікація з відновлення після інциденту (RC.CO):** Відновлювальні заходи координуються з внутрішніми та зовнішніми сторонами
  - **RC.CO-03:** Заходи з відновлення та прогрес у відновленні операційної спроможності повідомляються визначеним внутрішнім та зовнішнім зацікавленим сторонам
  - **RC.CO-04:** Публічні оновлення щодо відновлення після інцидентів поширюються з використанням затверджених методів та повідомлень

Додаток Б. Рівні CSF

Таблиця 2 містить умовну ілюстрацію рівнів CSF, про які йшлося в Розділі 3. Рівні характеризують практики управління ризиками кібербезпеки в організації (GOVERN) та практик управління ризиками кібербезпеки (IDENTIFICATE, PROTECT, DETECT, RESPONSE, and RECOVER).

Таблиця 2. Умовна ілюстрація рівнів CSF

Ярус	Управління та контроль ризиками кібербезпеки	Управління ризиками кібербезпеки
Рівень 1: Частковий	Управління застосуванням організаційної стратегії управління ризиками кібербезпеки здійснюється на індивідуальній основі. Пріоритети визначаються ситуаційно і формально не ґрунтуються на цілях або середовищі загроз.	Інформованість про ризики кібербезпеки на організаційному рівні є обмеженою. Організація впроваджує управління ризиками кібербезпеки на нерегулярній, індивідуальній основі. Організація може не мати процесів, які дозволяють обмінюватися інформацією про кібербезпеку всередині організації. Організація, як правило, не знає про ризики кібербезпеки, пов'язані з її постачальниками, продуктами та послугами, які вона купує та використовує.
Рівень 2: Інформований про ризики	Практики управління ризиками затверджуються керівництвом, але не можуть бути встановлені як загально-організаційна політика. Визначення пріоритетності заходів з кібербезпеки та потреб у захисті безпосередньо залежить від цілей організації щодо ризиків, середовища загроз або вимог бізнесу/місії.	На організаційному рівні існує усвідомлення ризиків кібербезпеки, але загально організаційний підхід до управління ризиками кібербезпеки ще не запроваджено. Врахування кібербезпеки в організаційних цілях і програмах, може відбуватися на деяких але не на всіх рівнях організації. Оцінка кібер ризиків організаційних та зовнішніх активів відбувається але, як правило, не повторюється і не є регулярною. Обмін інформацією про кібербезпеку в організації відбувається на неформальній основі. Організація усвідомлює ризики кібербезпеки, пов'язані з її постачальниками, продуктами та послугами, які вона купує та використовує, але вона не діє послідовно або формально у

		відповідь на ці ризики.
Рівень 3: Повторювальний	Практики управління ризиками організації офіційно затверджені та виражені у вигляді політики. Політики, процеси та процедури, що враховують ризики, визначаються, впроваджуються відповідно до намірів та переглядаються. Організаційні практики кібербезпеки регулярно оновлюються на основі застосування процесів управління ризиками з урахуванням змін у вимогах бізнесу/місії, загрозах та технологічному ландшафті.	Існує загально організаційний підхід до управління ризиками кібербезпеки. Інформація про кібербезпеку регулярно поширюється по всій організації. Існують послідовні методи для ефективного реагування на зміни в ризиках. Персонал володіє знаннями та навичками для виконання своїх функцій та обов'язків. Організація послідовно і точно відстежує ризики кібербезпеки активів. Керівники вищого рівня, відповідальні за кібербезпеку, та керівники, які не відповідають за кібербезпеку, регулярно спілкуються щодо ризиків кібербезпеки. Керівники забезпечують врахування питань кібербезпеки в усіх напрямках діяльності організації.

Ярус	**Управління та контроль ризиками кібербезпеки**	**Управління ризиками кібербезпеки**
		Стратегія управління ризиками організації ґрунтується на ризиках кібербезпеки, пов'язаних з її постачальниками, продуктами та послугами, які вона купує та використовує. Персонал офіційно реагує на ці ризики за допомогою таких механізмів, як письмові угоди, що визначають базові вимоги, структури управління (наприклад, ради з управління ризиками), а також впровадження та моніторинг політики. Ці дії здійснюються послідовно і відповідно до намірів, а також постійно контролюються і переглядаються.

Рівень 4: Адаптивний	Існує загально організаційний підхід до управління ризиками кібербезпеки, який використовує політики, процеси та процедури, що враховують ризики, для реагування на потенційні події кібербезпеки. Взаємозв'язок між ризиками кібербезпеки та цілями організації чітко зрозумілий та враховується при прийнятті рішень. Керівники відстежують ризики кібербезпеки в тому ж контексті, що й фінансові та інші організаційні ризики. Бюджет організації базується на розумінні поточного та прогнозованого середовища ризиків та толерантності до ризиків. Бізнес-підрозділи впроваджують бачення керівництва та аналізують ризики системного рівня в контексті організаційних толерантностей до ризиків. Управління ризиками кібербезпеки є частиною організаційної культури. Воно розвивається з усвідомлення попередньої діяльності та постійної обізнаності про діяльність в організаційних системах та мережах. Організація може швидко та ефективно враховувати зміни в бізнес-цілях/цілях місії в тому, як підходити до ризиків та інформувати про них.	Організація адаптує свої практики кібербезпеки на основі попередніх та поточних заходів з кібербезпеки, включаючи отримані уроки та прогнозні показники. Завдяки процесу постійного вдосконалення, який включає передові технології та практики кібербезпеки, організація активно адаптується до мінливого технологічного ландшафту і своєчасно та ефективно реагує на нові, складні загрози. Організація використовує інформацію в режимі реального або близькому до реального часу, щоб розуміти ризики кібербезпеки, пов'язані з її постачальниками, продуктами та послугами, які вона купує та використовує, і послідовно реагувати на них. Інформація про кібербезпеку постійно поширюється по всій організації та з уповноваженими третіми сторонами.

Додаток С. Глосарій

Категорія CSF
Група взаємопов'язаних результатів у сфері кібербезпеки, які в сукупності складають функцію CSF.

Профіль спільноти CSF
Базовий перелік результатів CSF, який створюється та публікується для задоволення спільних інтересів та цілей низки організацій. Профіль спільноти зазвичай розробляється для певного сектору, підсектору, технології, типу загрози або іншого варіанту використання. Організація може використовувати Профіль спільноти як основу для власного Цільового профілю.

Ядро CSF
Таксономія результатів кібербезпеки високого рівня, яка може допомогти будь-якій організації управляти ризиками кібербезпеки. Її компонентами є ієрархія функцій, категорій та підкатегорій, які деталізують кожен результат.

Поточний профіль CSF
Частина організаційного профілю, яка визначає основні результати, яких організація наразі досягає (або намагається досягти), і характеризує, як і в якій мірі досягається кожен результат.

Функція CSF
Найвищий рівень організації для досягнення результатів у сфері кібербезпеки. Існує шість функцій CSF: Управління, Ідентифікація, Захист, Виявлення, Реагування та Відновлення.

Приклад реалізації CSF
Стисла, орієнтована на дію, умовна ілюстрація способу досягнення основних результатів CSF.

Інформаційна довідка CSF
Відображення, яке вказує на зв'язок між основними результатами CSF та існуючими стандартами, настановами, положеннями чи іншим змістом.

Організаційний профіль CSF
Механізм опису поточного та/або цільового стану кібербезпеки організації в термінах результатів Ядра CSF.

Посібник з швидкого початку роботи з CSF
Додатковий ресурс, що містить короткі, практичні рекомендації з конкретних питань, пов'язаних з CSF.

Підкатегорія CSF
Група більш конкретних результатів технічної та управлінської діяльності з кібербезпеки, які складають категорію CSF.

Цільовий профіль CSF

Частина організаційного профілю, що визначає бажані основні результати, які організація обрала та визначила пріоритетними для досягнення своїх цілей з управління ризиками кібербезпеки.

Рівень CSF
Характеристика суворості управління ризиками кібербезпеки в організації та практики управління ними. Існує чотири рівні: Частковий (Рівень 1), інформований про ризики (Рівень 2), повторюваний (Рівень 3) та адаптивний (Рівень 4).

Певне комерційне обладнання, прилади, програмне забезпечення або матеріали, комерційні або некомерційні, згадуються в цій статті для того, щоб адекватно описати експериментальну процедуру. Така ідентифікація не означає рекомендацію або схвалення будь-якого продукту або послуги з боку NIST, а також не означає, що вказані матеріали або обладнання обов'язково є найкращими з доступних для даної мети.

Політика NIST щодо технічних серій
Заяви про авторське право, використання та ліцензування
Ідентифікатор публікації NIST Technical Series Синтаксис ідентифікатора публікації

Як цитувати цю публікацію NIST Technical Series:
Національний інститут стандартів і технологій (2024) Рамкова основа кібербезпеки NIST (CSF) 2.0. (Національний інститут стандартів і технологій, Гейтерсбург, штат Меріленд), Біла книга з кібербезпеки NIST (CSWP) NIST CSWP 29. https://doi.org/10.6028/NIST.CSWP.29

Контактна інформація
cyberframework@nist.gov

Національний інститут стандартів і технологій
Кому: Відділ прикладної кібербезпеки,
Лабораторія інформаційних технологій 100 Bureau
Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

Всі коментарі підлягають оприлюдненню відповідно до Закону про свободу інформації (FOIA).