УДК 004.056.53
DOI: 10.31673/2409-7292.2025.030936

Іваночко Т. А., Семенюк С. А.

УПРАВЛІННЯ РИЗИКАМИ КІБЕРБЕЗПЕКИ З ВИКОРИСТАННЯМ NIST CSF 2.0

У статті розглядається питання управління ризиками кібербезпеки з використанням фреймворку NIST Cybersecurity Framework (CSF), який є одним із найпоширеніших і найгнучкіших інструментів у сфері кіберзахисту. Актуальність дослідження зумовлена стрімким зростанням складності та частоти кібератак, що загрожують безперервності бізнесу, безпеці персональних даних та національній безпеці. У сучасних умовах організації стикаються з викликами адаптації до нових типів загроз, таких як атаки на ланцюжки постачання, зловживання технологіями штучного інтелекту, а також хронічним дефіцитом кваліфікованих кадрів. Запропоновано системний підхід до управління ризиками, що базується на фреймворку NIST CSF версії 2.0, який охоплює шість функціональних доменів: від ідентифікації активів і вразливостей до стратегічного управління кібербезпекою. На основі критерію зрілості організацій та рівня критичності контрольних заходів представлено спосіб побудови профілю кібербезпеки, що дозволяє виявити прогалини та визначити пріоритети для вдосконалення. Дослідження підкреслює переваги NIST CSF як адаптивного, універсального і масштабованого інструменту, що підходить для різних типів та розмірів компаній. Практична значущість результатів полягає у можливості їх застосування в українських компаніях з обмеженими ресурсами, які потребують ефективного механізму виявлення вразливостей, побудови політик кіберзахисту та досягнення відповідності міжнародним стандартам. Запропоновані рекомендації спрямовані на підвищення стійкості до кіберзагроз та зниження впливу цифрових загроз на критично важливі процеси організації.

Ключові слова: інформаційна безпека, система управління ризиками, стандарт, NIST CSF, заходи безпеки.

Вступ і формулювання проблеми.

У сучасну епоху, що характеризується глибокою цифровізацією бізнесу, державного управління та повсякденного життя, питання кібербезпеки набуло першочергового значення. Прогнозовані втрати від кіберзлочинності на глобальному рівні сягають 24 трильйонів доларів до 2027 року, а лише у 2024 році понад 72% малих і середніх підприємств у Канаді та 65% у Мексиці стали жертвами кібератак[1]. Така статистика свідчить про критичну вразливість організацій різного масштабу та про необхідність створення структурованих, адаптивних підходів до управління ризиками у сфері кіберзахисту.

Важливим інструментом у цій площині став Cybersecurity Framework (CSF), що був розроблений Національним інститутом стандартів і технологій США (NIST) [2]. Його друга версія, представлена у 2024 році [3], передбачає інтеграцію шести ключових функцій фреймворку від ідентифікації загроз до стратегічного управління кібербезпекою (Govern). Він пропонує гнучку модель оцінки, планування та вдосконалення безпекової інфраструктури організацій.

Попри наявність фреймворків, таких як ISO/IEC 27001 [4], ISO/IEC 27002 [5], COBIT [6] чи CIS Controls [7], у практиці багатьох компаній, особливо малих і середніх, спостерігається відсутність комплексного підходу до впровадження стандартів кіберзахисту. Причинами цього є як обмежені ресурси, так і недостатній рівень зрілості внутрішніх процесів. Крім того, постійна еволюція кібератак, у тому числі з використанням штучного інтелекту, створює нові виклики для традиційних моделей управління ризиками.

Метою даної статті є дослідження можливостей застосування NIST CSF для практичного управління ризиками кібербезпеки в умовах обмежених ресурсів. У межах цього дослідження виконано:

- порівняльний аналіз провідних фреймворків кібербезпеки;
- дослідження функціональної структури та логіки роботи NIST CSF 2.0;
- адаптацію моделі зрілості фреймворку до умов малого і середнього бізнесу;
- аналіз реального кейсу з ідентифікацією типових вразливостей організаційної інфраструктури;

- формулювання практичних рекомендацій щодо підвищення ефективності управління ризиками кіберзагроз.

Аналіз існуючих досліджень

Управління ризиками кібербезпеки є предметом інтенсивного міждисциплінарного дослідження, що охоплює як технічні, так і організаційні аспекти забезпечення інформаційної безпеки. У науковій літературі сформовано декілька парадигм управління кіберризиками: інженерна (технічні засоби та архітектури), організаційна (управління процесами), нормативна (відповідність стандартам), а також гібридна - з урахуванням бізнес-контексту та стратегічних цілей. У цьому контексті фреймворки кібербезпеки слугують методологічною основою для гармонізації технічного і процесного управління ризиками.

ISO/IEC 27001 є найпоширенішим міжнародним стандартом, орієнтованим на створення, впровадження та вдосконалення системи управління інформаційною безпекою (ISMS). Як показано у [8], стандарт забезпечує системність, проте часто є надто об'ємним для малих і середніх підприємств через необхідність формальної сертифікації, витрат на аудит та складну документацію.

COBIT, розроблений ISACA, фокусується на управлінні IT та корпоративному контролі. В літературі його часто позиціонують як інструмент для інтеграції кібербезпеки у бізнес-процеси [9]. Попри стратегічну глибину, COBIT має високу вартість впровадження та потребує значної зрілості IT-губернансу, що обмежує його доступність для організацій з невеликим IT-відділом.

CIS Controls, у свою чергу, акцентують на практичних кроках для захисту від поширених загроз. Дослідження [10] відзначають їхню ефективність у швидкому підвищенні базового рівня кіберзахисту. Однак CIS орієнтовані переважно на технічний рівень і не покривають в достатній мірі управлінські чи стратегічні аспекти.

Фреймворк NIST CSF, оприлюднений у 2014 році та оновлений до версії 2.0 у 2024 році, вирізняється гнучкістю, масштабованістю та орієнтацією на управління ризиками в динамічному цифровому середовищі. Його функціональна структура (Identify, Protect, Detect, Respond, Recover, Govern) дозволяє адаптувати підхід до потреб організацій різного рівня зрілості. Як зазначається у [11], NIST CSF особливо цінний для міжгалузевого впровадження та не вимагає формальної сертифікації. Дослідження [12] демонструють успішні кейси його застосування в охороні здоров'я, фінансовій сфері та державному управлінні.

Однак в академічному дискурсі відсутні достатньо опрацьовані підходи до адаптації NIST CSF для малого і середнього бізнесу в країнах, що розвиваються, а також бракує прикладних моделей інтеграції нової функції Govern стратегічного управління кібербезпекою. Залишається відкритим також питання ефективної оцінки рівня зрілості контролів в умовах обмежених ресурсів.

Таким чином, наявна література створює сильне теоретичне підґрунтя для вивчення фреймворку NIST CSF, проте вимагає подальшого розвитку в напрямі його локалізації та практичного впровадження.

Методологія

Методологічною основою дослідження є фреймворк кібербезпеки NIST CSF версії 2.0, що дозволяє системно аналізувати поточний стан безпеки, визначати прогалини та формувати пріоритети для вдосконалення. Для досягнення мети дослідження використано поєднання аналітичних, порівняльних і прикладних методів, що охоплюють як теоретичне моделювання, так і практичну оцінку. NIST CSF обрано як базову модель оцінювання через його адаптивну структуру, відсутність вимог до сертифікації, підтримку стратегічного підходу та сумісність з іншими міжнародними стандартами (ISO/IEC 27001, COBIT). Оцінювання здійснюється за шістьма функціями: Identify, Protect, Detect, Respond, Recover та Govern. Кожна з них поділяється на категорії та підкатегорії, що відображають ключові напрямки забезпечення безпеки.

© Іваночко Т. А., Семенюк С. А. (2025) Управління ризиками кібербезпеки з використанням NIST CSF 2.0. Сучасний захист інформації, 3(63), 75–82.
https://doi.org/10.31673/2409-7292.2025.030936

Методологія оцінки починається з функції Identify, яка зосереджена на розумінні інформаційного середовища організації. Це передбачає інвентаризацію активів, таких як апаратне забезпечення, програмне забезпечення, дані та мережі, а також ідентифікацію потенційних ризиків і вразливостей. Наприклад, організація може використовувати інструменти сканування мережі, щоб виявити незахищені пристрої, або проводити оцінку ризиків для визначення критичних даних. В Україні, де малі підприємства часто мають обмежені ресурси, цей етап може включати базовий аудит із використанням відкритих інструментів, таких як Nmap. Оцінка за цією функцією дозволяє створити основу для подальшого аналізу, визначаючи, що саме потребує захисту.

Функція Protect спрямована на оцінку заходів безпеки, які запобігають кіберінцидентам. Методологія включає аналіз наявних засобів захисту, таких як шифрування, контроль доступу, антивірусне програмне забезпечення чи політики безпеки. Наприклад, організація може перевірити, чи використовується двохфакторна автентифікація для доступу до критичних систем, або оцінити рівень обізнаності персоналу через симуляцію фішингових атак. В українському контексті, де фішинг є поширеною загрозою, оцінка може фокусуватися на навчанні працівників і впровадженні базових технічних засобів, таких як спам-фільтри. Цей етап допомагає виявити слабкі місця в захисті та оцінити їхню ефективність проти актуальних загроз.

Detect передбачає оцінку здатності організації своєчасно виявляти кіберінциденти. Методологія охоплює аналіз систем моніторингу, таких як системи виявлення вторгнень (IDS) або журнали подій, а також процедур реагування на аномалії. Наприклад, організація може перевірити, чи здатна її система SIEM (Security Information and Event Management) виявляти підозрілу активність, або оцінити частоту оновлення сигнатур антивірусу. Для українських організацій, які часто стикаються з обмеженим бюджетом, можуть застосовуватися безкоштовні інструменти, такі як OSSEC, для базового моніторингу. Оцінка за цією функцією дозволяє визначити, наскільки швидко організація може виявити атаку, що є критично важливим для мінімізації збитків.

Функція Respond зосереджена на оцінці готовності організації реагувати на кіберінциденти. Методологія включає аналіз планів реагування, процедур ізоляції заражених систем і комунікаційних стратегій. Наприклад, організація може провести симуляцію атаки ransomware, щоб перевірити, чи здатна команда швидко локалізувати загрозу та повідомити стейкхолдерів. В Україні, де державні установи та підприємства часто є мішенню складних атак, оцінка може включати перевірку координації з національними центрами, такими як CERT-UA. Цей етап допомагає оцінити ефективність реагування та виявити прогалини в підготовці.

Recover завершує цикл оцінки, фокусуючись на здатності організації відновлюватися після інцидентів. Методологія передбачає аналіз планів відновлення, резервного копіювання даних і процедур повернення до нормальної роботи. Наприклад, організація може перевірити, чи регулярно тестуються резервні копії, або оцінити час, необхідний для відновлення критичних систем. Для українських організацій, які стикаються з атаками на кшталт NotPetya, цей етап є особливо важливим, оскільки швидке відновлення може запобігти значним збиткам. Оцінка за цією функцією визначає, наскільки організація готова повернутися до операційної діяльності після атаки.

Функція Govern підкреслює стратегічне управління кібербезпекою, включаючи координацію політик і залучення керівництва.

Застосовано модель профільного порівняння, що передбачає визначення:

- поточного профілю організації, тобто стану реалізації кожної функції/категорії безпеки відповідно до фактичного рівня зрілості;
- цільового профілю як бажаного рівня реалізації кожного елемента відповідно до критичності бізнес-процесів;

© Іваночко Т. А., Семенюк С. А. (2025) Управління ризиками кібербезпеки з використанням NIST CSF 2.0. Сучасний захист інформації, 3(63), 75–82.
https://doi.org/10.31673/2409-7292.2025.030936

- дельта-профілю як різниці між поточним і цільовим рівнями, що слугує основою для побудови дорожньої карти покращень.

Для побудови поточного профілю можна використовувати:

- внутрішню документацію компанії (політики, процедури, інструкції);
- результати технічного аудиту IT-інфраструктури;
- інтерв'ю зі стейкхолдерами (менеджмент, IT-фахівці);
- спостереження за процесами управління активами, інцидентами, доступом і резервним копіюванням.

Модель зрілості кібербезпеки (Cybersecurity Maturity Model) є ефективним інструментом для оцінки рівня кібербезпеки організації через аналіз трьох ключових компонентів: людей, процесів і технологій. Вона базується на п'яти рівнях зрілості, які дозволяють оцінити, наскільки системно організація підходить до управління ризиками, і визначити напрями для вдосконалення. У контексті NIST Cybersecurity Framework (NIST CSF) ця модель гармонізується з рівнями впровадження (Implementation Tiers), надаючи структурований підхід до оцінки зрілості кібербезпеки.

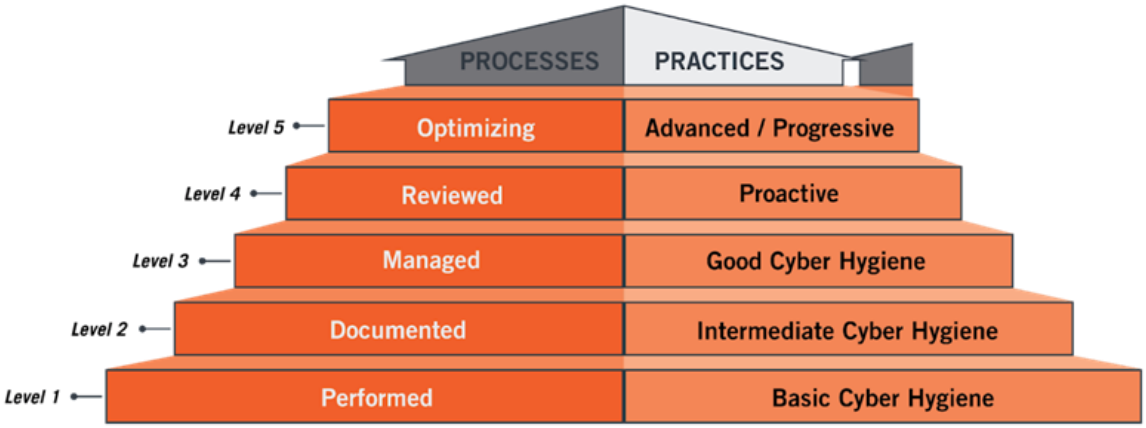

Рис. 1. Модель зрілості кібербезпеки

Модель зрілості (рис.1) включає п'ять рівнів, кожен із яких відображає прогрес у розвитку кібербезпеки. На початковому рівні (Level 1) кібербезпека є реактивною, а заходи вживаються хаотично, без формалізованих процесів. Люди, як правило, не мають достатньої підготовки, процеси є неструктурованими, а технології використовуються фрагментарно, наприклад, лише базові антивіруси. Для українських малих підприємств цей рівень є типовим через брак ресурсів і експертизи. Оцінка на цьому етапі передбачає аналіз наявності будь-яких заходів безпеки, таких як паролі чи оновлення програмного забезпечення, і виявлення критичних прогалин, наприклад, відсутності навчання персоналу.

На формуючому рівні (Level 2) організація починає впроваджувати базові процеси та політики. Люди отримують початкове навчання, наприклад, щодо розпізнавання фішингових листів, процеси частково документовані, як-от правила резервного копіювання, а технології включають прості засоби захисту, такі як брандмауери. Методологія оцінки на цьому рівні зосереджена на перевірці наявності документації, наприклад, політик безпеки, і тестуванні базових технічних засобів. В Україні підприємства на цьому рівні, наприклад, у роздрібній торгівлі, можуть оцінювати, чи є у них чіткі інструкції для реагування на інциденти, і чи застосовуються оновлення безпеки.

Керований рівень (Level 3) характеризується формалізованими процесами та системним підходом. Люди регулярно проходять тренінги, процеси чітко визначені й документовані, наприклад, плани реагування на інциденти, а технології включають системи моніторингу, як-от SIEM. Оцінка передбачає аудит процедур, аналіз метрик, таких як частота інцидентів, і

© Іваночко Т. А., Семенюк С. А. (2025) Управління ризиками кібербезпеки з використанням NIST CSF 2.0. Сучасний захист інформації, 3(63), 75–82.
https://doi.org/10.31673/2409-7292.2025.030936

перевірку інтеграції технологій у робочі процеси. Для українських організацій, таких як банки чи енергетичні компанії, цей рівень є актуальним, оскільки вони прагнуть відповідати регуляторним вимогам. Оцінка може включати симуляцію атак для перевірки ефективності виявлення та реагування.

На оптимізованому рівні (Level 4) кібербезпека є проактивною, з акцентом на безперервне вдосконалення. Люди беруть участь у розширених тренінгах, включаючи симуляції складних атак, процеси регулярно переглядаються та оптимізуються, а технології включають автоматизовані інструменти, такі як SOAR. Методологія оцінки на цьому рівні охоплює аналіз ключових показників ефективності (KPI), наприклад, середнього часу виявлення інцидентів, і оцінку адаптивності до нових загроз. В Україні цей рівень є досяжним для великих корпорацій, таких як телекомунікаційні компанії, які використовують NIST CSF для оцінки зрілості кібербезпеки, аналізуючи відповідність функціям Identify, Protect, Detect, Respond і Recover.

Адаптивний рівень (Level 5) є найвищим, де кібербезпека повністю інтегрована в організаційну культуру та бізнес-процеси. Працівники демонструють високу обізнаність і беруть активну участь у формуванні кібербезпеки, процеси автоматизовані та постійно вдосконалюються. Також технології використовують передові рішення, такі як штучний інтелект для аналізу загроз. Оцінка на цьому рівні передбачає комплексний аналіз, включаючи стрес-тестування систем, оцінку інновацій у кібербезпеці та співпрацю з зовнішніми партнерами, наприклад, CERT-UA. В Україні цей рівень є рідкісним, але може бути досягнутий у секторах із високими вимогами до безпеки, таких як фінансовий.

Об'єкт і контекст дослідження

Як приклад аналізу розглянемо IT-компанію середнього масштабу. Аудит охоплює період активних інфраструктурних змін, що створювало додаткові ризики для конфіденційності, доступності та цілісності критичних даних. Особливу увагу зосереджено на процесах доступу, резервування, моніторингу та ізоляції середовищ, які виявилися найбільш уразливими.

Результати дослідження

Оцінювання системи кібербезпеки об'єкта дослідження здійснювалося на основі фреймворку NIST CSF 2.0 за допомогою профільного підходу. Було визначено поточний рівень реалізації контрольних заходів, а також розриви порівняно з цільовим профілем.

Аналіз показав, що більшість категорій безпеки реалізовано на низькому рівні зрілості (0–1). Особливо критичні недоліки виявлено у таких доменах (табл. 2).

Таблиця 2

Виявлені недоліки по доменах

Домен	Недолік
Asset Management (ID.AM)	відсутність повного обліку активів, недостатня інвентаризація IT-інфраструктури
Risk Assessment (ID.RA)	неформалізований підхід до аналізу загроз і вразливостей
Data Security (PR.DS)	відсутні засоби шифрування, механізми запобігання витоку даних, захист API
Incident Response (RS.CO, RS.AN)	відсутність плану реагування на інциденти, формальних процедур і тренінгів
Governance (GV)	політики безпеки існують, але не донесені до відповідального персоналу і не реалізовані на практиці

Усі функціональні домени фреймворку (за винятком окремих аспектів функції Protect) мають оцінку на рівні 0 або 1. Жодна категорія не досягла рівня 2 (керованої реалізації). Це свідчить про незрілість практик кіберзахисту та високу ймовірність інцидентів. На основі технічного аудиту і документального аналізу ідентифіковано такі найважливіші вразливості:

- об'єднання розробницького, тестового та продуктивного середовищ в одну мережу без сегментації;

© Іваночко Т. А., Семенюк С. А. (2025) Управління ризиками кібербезпеки з використанням NIST CSF 2.0. Сучасний захист інформації, 3(63), 75–82.
https://doi.org/10.31673/2409-7292.2025.030936

- відсутність автентифікації для доступу до критичних сервісів (SSH, API, бази даних);
- відсутність централізованого моніторингу подій безпеки і журналів;
- відсутність ізольованої інфраструктури для забезпечення безперервності бізнесу;
- відсутність навчання співробітників щодо фішингу та реагування на загрози.

Для візуалізації результатів було побудовано радарну діаграму (рис.2), що демонструє поточний рівень зрілості в межах 22 категорій фреймворку NIST CSF. Діаграма виявляє сильну асиметрію між бажаним і фактичним станом: більшість показників у межах 0–1 із цільовим рівнем 4–5. Це підкреслює масштаб розриву та необхідність термінових заходів.

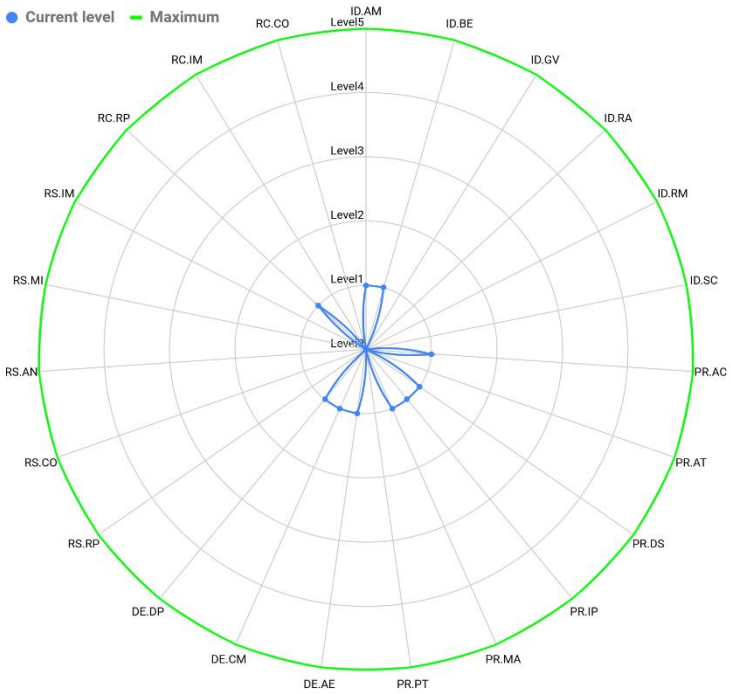

Рис 2. Діаграма зрілості згідно NIST CSF

Оцінка за рівнями критичності (від 1 до 5) показала, що понад 60% контрольних заходів мають високу або критичну важливість для цілей кібербезпеки організації. Зокрема, функції Identify, Protect і Respond містять найбільшу частку контролів критичного рівня.

Таблиця 2

Результати аудиту за категоріями (фрагмент)

Функція	Категорія	Поточний рівень	Цільовий рівень	Критичність
Identify	ID.AM	1	5	5
Identify	ID.RA	0	5	5
Protect	PR.DS	1	5	5
Respond	RS.CO	0	5	5
Recover	RC.RP	1	5	4
Govern	GV	0	5	5

Результати оцінювання свідчать про критично низький рівень зрілості системи кібербезпеки досліджуваної організації. Незважаючи на наявність загальних політик безпеки, їх практична імплементація виявилася майже повністю відсутньою. Ключові функції фреймворку NIST CSF – зокрема Identify, Protect та Respond – реалізовані фрагментарно або не реалізовані зовсім. Це створює широкий простір для потенційних інцидентів, включно з

втратою конфіденційної інформації, компрометацією внутрішніх сервісів та перервою в роботі критичних систем.

Одним із найбільш тривожних виявів є відсутність розмежування середовищ розробки і виробництва, що суперечить базовим принципам безпеки. Така архітектура уможливлює ланцюгову ескалацію доступу в разі компрометації окремих вузлів. Відсутність систем журналювання, реагування на інциденти та моніторингу позбавляє організацію можливості своєчасно виявляти порушення або проводити розслідування заднім числом.

Крім технічних аспектів, виявлено відсутність кібербезпекової культури на рівні персоналу та менеджменту. Співробітники не проходили спеціального навчання, а управлінська ланка не володіє достатньою обізнаністю щодо актуальних ризиків. Нововведена функція Govern, яка у фреймворку CSF 2.0 відповідає за стратегічне управління безпекою, фактично відсутня в організаційній структурі.

Ці знахідки підтверджують важливість адаптації NIST CSF саме до реалій малого та середнього бізнесу, де часто бракує ресурсів для повноцінного впровадження комплексних рішень. У такому контексті фреймворк може виконувати роль навігатора, що дозволяє встановити пріоритети на основі критичності бізнес-процесів.

Пропоновані рекомендації

У результаті проведення аудиту запропоновано впровадити наступні рекомендації:

- терміново впровадити базову сегментацію мережі: ізоляція середовищ розробки, тестування і продуктивної системи;
- розгорнути систему моніторингу подій безпеки (SIEM або її легкі альтернативи) та налаштувати централізовані журнали;
- актуалізувати та формалізувати політики кібербезпеки, забезпечивши їх розповсюдження серед технічного персоналу;
- почати побудову функції Govern, створивши окрему роль або відділ, відповідальний за стратегічне управління ризиками;
- провести базове навчання персоналу щодо фішингу, політик доступу, захисту даних;
- побудувати покрокову дорожню карту вдосконалень згідно з пріоритетами, визначеними дельта-профілем.

Порівняння з літературними джерелами [10, 11] демонструє, що більшість викликів малого бізнесу пов’язані не з відсутністю технічних рішень, а з недооцінкою процесного та управлінського компонентів. У цьому контексті особливу роль відіграє нова функція Govern, що має бути визнана як базовий пріоритет для організацій, які прагнуть до підвищення кіберстійкості.

Висновки

У статті досліджено можливості та ефективність застосування фреймворку NIST Cybersecurity Framework (CSF) версії 2.0 для управління ризиками кібербезпеки в умовах обмежених ресурсів. Проведене оцінювання реальної організації продемонструвало, що навіть при наявності загальних політик безпеки, відсутність їх практичного впровадження створює критичні вразливості, які підвищують ймовірність інцидентів та загрожують безперервності бізнесу.

Аналіз виявив, що більшість функцій NIST CSF реалізовані на рівні 0–1 за шкалою зрілості, тоді як цільові значення становлять 4–5. Найгостріші проблеми зосереджені в таких сферах, як управління активами, оцінка ризиків, сегментація середовищ, моніторинг подій, реагування на інциденти та стратегічне управління (Govern).

Практичне застосування фреймворку дозволило:

- систематизувати виявлення вразливостей у бізнес-процесах;
- сформувати поточний профіль кібербезпеки організації;
- встановити пріоритети вдосконалення за критичністю контрольних заходів;

© Іваночко Т. А., Семенюк С. А. (2025) Управління ризиками кібербезпеки з використанням NIST CSF 2.0. Сучасний захист інформації, 3(63), 75–82.
https://doi.org/10.31673/2409-7292.2025.030936

- розробити базові рекомендації, релевантні до українських реалій малого та середнього бізнесу.

Фреймворк NIST CSF підтвердив свою гнучкість і адаптивність, а також придатність до поетапного впровадження навіть у компаніях без спеціалізованих команд безпеки. Водночас результати засвідчують необхідність активної підтримки з боку керівництва, послідовної реалізації функції стратегічного управління безпекою (Govern) і створення культури відповідального ставлення до цифрової безпеки.

У подальших дослідженнях доцільно зосередитись на розробці практичних інструментів локалізації фреймворку NIST CSF для різних галузей, інтеграції з іншими стандартами (зокрема, ISO/IEC 27001) та створенні доступних метрик для оцінювання прогресу впровадження в умовах обмеженого бюджету.

Перелік посилань

1. Global Cybersecurity Outlook 2025 URL: https://www.weforum.org/publications/global-cybersecurity-outlook-2025.

2. NIST Cybersecurity Framework // National Institute of Standards and Technology. URL: https://www.nist.gov/cyberframework

3. NIST Cybersecurity Framework Version 2.0 // National Institute of Standards and Technology. URL: https://www.nist.gov/news-events/news/2024/02/nist-releases-draft-update-cybersecurity-framework-version-20.

4. ISO/IEC 27001: Information Security Management // International Organization for Standardization URL: https://www.iso.org/isoiec-27001-information-security.html.

5. Кухарська Н.П., Семенюк С.А., Полотай О. І. (2025). Ключові аспекти оновленого стандарту ISO/IEC 27002:2022. Сучасний захист інформації, №2, https://doi.org/10.31673/2409-7292.2025.023969.

6. COBIT Framework // ISACA. URL: https://www.isaca.org/resources/cobit.

7. CIS Controls // Center for Internet Security. URL: https://www.cisecurity.org/controls.

8. Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2023). The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector. Sustainability, 15(7), 5828. https://doi.org/10.3390/su15075828

9. Utomo, D., Wijaya, M., Suzanna, S., Efendi, E., & Sagala, N. T. M. (2022). Leveraging COBIT 2019 to Implement IT Governance in SME Context: A Case Study of Higher Education in Campus A. CommIT (Communication and Information Technology) Journal, 16(2), 129–141. https://doi.org/10.21512/commit.v16i2.8172.

10. Edwards, J. (2024). Critical security controls for effective cyber defense. In Apress eBooks. https://doi.org/10.1007/979-8-8688-0506-6.

11. Alshar'e, M. (2023). Cyber security framework selection: comparison of NIST and ISO 27001. Applied Computing Journal, 3(1), 245-255. https://doi.org/10.52098/acj.202364.

12. Udroiu, A. M., Dumitrache, M., & Sandu, I. (2022, June). Improving the cybersecurity of medical systems by applying the NIST framework. In 2022 14th International Conference on Electronics, Computers and Artificial Intelligence (ECAI) (pp. 1-7). IEEE. https://doi.org/10.1109/ECAI54874.2022.9847498.

Надійшла 27.06.2025