КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (30), 2025
Спеціальний випуск ISSN 2663 – 4023
Special issue
DOI 10.28925/2663-4023.2025.30.980
УДК 004.056

Захарова Ярина Анатоліївна
Національний університет «Львівська Політехніка», Львів, Україна
ORCID: 0009-0006-0129-7944
yaryna.zakharova.mkbas.2024@lpnu.ua

Партика Андрій Ігорович
кандидат технічних наук, доцент
доцент кафедри "Захисту інформації"
Національний університет «Львівська Політехніка», Львів, Україна
ORCID: 0000-0003-3037-8373
andrii.i.partyka@lpnu.ua

ЕВОЛЮЦІЯ УПРАВЛІННЯ КІБЕРРИЗИКАМИ КРІЗЬ ПРИЗМУ NIST CYBERSECURITY FRAMEWORK

Анотація. У статті здійснено комплексний аналіз еволюції NIST Cybersecurity Framework від початкової редакції 1.0 до сучасної версії 2.0. Висвітлено передумови створення фреймворку, його місце у міжнародній практиці та ключову роль у підвищенні кіберстійкості організацій різного масштабу від невеликих компаній до глобальних корпорацій і державних установ. Детально розглянуто особливості попередніх редакцій, зокрема CSF 1.0, яка заклала основу у вигляді п’яти базових функцій (Identify, Protect, Detect, Respond, Recover), та CSF 1.1, що уточнила підходи до управління ризиками у ланцюгах постачання і зробила рамку більш прикладною. Показано, що перехід до CSF 2.0 у 2024 році став якісним етапом розвитку, оскільки нова версія орієнтована не лише на технічні аспекти, а й на стратегічне корпоративне управління. Серед ключових нововведень виділено функцію Govern, що формально закріплює відповідальність керівництва, а також розширення можливостей щодо інтеграції з міжнародними стандартами, удосконалення метрик ефективності та посилення уваги до управління ризиками ланцюгів постачання. Окремо проаналізовано особливості процесу переходу організацій до CSF 2.0. Він включає здійснення аналізу розривів між існуючим станом безпеки та новими вимогами, формування політик, побудову стратегії впровадження, застосування автоматизації та інструментів Zero Trust, а також навчання персоналу. Наголошено, що успіх адаптації залежить від підтримки вищого керівництва, формування культури безпеки й постійного вдосконалення процедур.

Ключові слова: NIST CSF 2.0, кібербезпека, управління ризиками, інформаційна безпека, політика кібербезпеки.

ВСТУП

У сучасних умовах глобальної цифровізації питання управління кіберризиками набуває стратегічного значення для організацій усіх рівнів – від державних установ до приватних компаній. Зростання залежності бізнес-процесів і державного управління від інформаційних систем робить питання кіберстійкості ключовим елементом національної та економічної безпеки. Традиційні підходи до кіберзахисту, що ґрунтуються виключно на технічних рішеннях, поступово втрачають ефективність, оскільки сучасні загрози стають більш комплексними.

Серед міжнародних практик особливе місце посідає NIST Cybersecurity Framework (CSF), розроблений Національним інститутом стандартів і технологій США (NIST – National Institute of Standards and Technology). Від часу першої публікації у 2014 році цей

фреймворк став універсальним інструментом побудови системи кіберзахисту, що охоплює не лише технічні, а й управлінські та організаційні аспекти. Його гнучкість, масштабованість і практична орієнтація сприяли широкому впровадженню у різних галузях і країнах світу, зокрема у критично важливих секторах економіки.

Оновлена у 2024 році версія – NIST CSF 2.0 – відзначилася суттєвими змінами, спрямованими на інтеграцію кібербезпеки в систему корпоративного управління. У новій редакції з'явилася функція Govern, яка формалізує відповідальність керівництва та забезпечує узгодження стратегічних цілей організації з її політиками безпеки. Ці зміни демонструють перехід від технічного рівня управління ризиками до стратегічного. Водночас, попри значний міжнародний досвід, в українських умовах питання адаптації CSF 2.0 та практичного переходу до оновленої моделі залишаються недостатньо вивченими.

Актуальність теми.

У наслідок зростанням масштабів і складності сучасних кібератак, що загрожують не лише бізнесу, а й державним інституціям, критичній інфраструктурі та національній безпеці. Використання хмарних технологій, впровадження штучного інтелекту й цифрова трансформація економіки створюють нові вектори ризику, які вимагають системного підходу до їх ідентифікації, оцінки та управління.

Для урядових організацій України впровадження міжнародно визнаних підходів, таких як NIST CSF 2.0, має стратегічне значення. Це дозволить не лише підвищити рівень кіберзахисту, а й створити єдину методологічну основу для координації дій між державними структурами, підвищення прозорості управлінських процесів та забезпечення стійкості критичних інформаційних систем в умовах триваючої війни.

Аналіз останніх досліджень і публікацій.

Проблематика стандартизації управління кіберризиками послідовно розкривається у публікаціях Національного інституту стандартів і технологій США, який розробив базову рамку Cybersecurity Framework [1-3].

Подальші дослідження підтвердили ефективність NIST CSF як універсального інструменту. Наукова література фіксує значний інтерес до практичного застосування фреймворку NIST у різних секторах економіки, зокрема у сфері критичної інфраструктури, державного управління та малого бізнесу. Зокрема, на прикладі державного сектору Малайзії показали, що підхід може бути успішно адаптований у країнах, що розвиваються, без втрати ефективності [4]. В іншому досліджені довели придатність CSF до оцінювання кіберстійкості в органах місцевого самоврядування [5]. Підкреслюються гнучкість фреймворку й можливість його адаптації до корпоративного управління [6-7]. Доведено позитивний вплив CSF на кіберстійкість критичної інфраструктури [8].

Оновлена версія CSF 2.0 відображає перехід від технічного до стратегічного рівня управління. Як зазначає Гатінен поява функції Govern розподілила відповідальність за кіберризики між технічними фахівцями та керівництвом [9]. CSF 2.0 також забезпечує глибшу інтеграцію з міжнародними стандартами, зокрема ISO/IEC 27001, що сприяє гармонізації практик у межах ЄС і США [10]. Практичні аспекти впровадження нової версії висвітлено у працях розкривають оновленні структури категорій, розширення прикладів реалізації та впровадження метрик ефективності [9,11-12].

В українському науковому полі відзначають потенціал CSF 2.0 для гармонізації національних практик кіберзахисту з міжнародними підходами, хоча і обмежується переважно ознайомчим матеріалом [13]. Таким чином, літературний аналіз демонструє,

що NIST CSF 2.0 розглядається як логічна еволюція попередніх версій, спрямована на інтеграцію технічних, управлінських і стратегічних аспектів управління кіберризиками.

Постановка проблеми.

Попри значний поступ у стандартизації підходів до кібербезпеки, більшість організацій досі стикаються з труднощами інтеграції управління кіберризиками у загальну систему корпоративного менеджменту. Попередні редакції NIST Cybersecurity Framework (CSF 1.0 та 1.1) заклали міцну методологічну основу, однак залишали акцент переважно на технічних аспектах захисту. Це призводило до того, що питання кібербезпеки залишалися на рівні IT-підрозділів і не охоплювали управлінські процеси. Відсутність чітких показників ефективності та стратегічного бачення знижувала здатність організацій оцінювати й контролювати власні ризики.

Зростання масштабів кібератак, поширення хмарних технологій, штучного інтелекту та ускладнення ланцюгів постачання потребують переходу до цілісного, вимірюваного й проактивного управління ризиками. Виходом на ці виклики стала поява NIST CSF 2.0, що запровадила функцію Govern та підкреслила роль керівництва у формуванні політик і стратегій безпеки. Однак постає завдання дослідити, яким чином нова структура та принципи CSF 2.0 змінюють підхід до управління кіберризиками й сприяють побудові ефективної системи корпоративного кіберзахисту.

Метою дослідження є виявлення ключових зміни у фреймворку CSF 2.0 та визначення їх значення для формування сучасних підходів до управління кіберризиками.

Завдання дослідження:

1. Проаналізувати еволюцію структури, функцій і принципів NIST Cybersecurity Framework від версії 1.0 до 2.0;
2. Визначити особливості переходу організацій до CSF 2.0, включаючи формування політик, стратегії впровадження та роль керівництва;
3. Виявити ключові структурні зміни, зокрема впровадження функції Govern, та оцінити їх вплив на управління кіберризиками;
4. Визначити кроки української влади для переходу до CSF 2.0 у межах національної системи кібербезпеки.
5. Проаналізувати сучасні інструменти, призначені для впровадження, моніторингу та оцінки відповідності NIST Cybersecurity Framework.

ІСТОРІЯ ТА ЕВОЛЮЦІЯ NIST CYBERSECURITY FRAMEWORK

NIST Cybersecurity Framework розроблений Національним інститутом стандартів і технологій США Цей документ став орієнтиром для організацій у вибудові системного підходу до кіберзахисту, забезпечуючи уніфіковану основу для управління ризиками та підвищення стійкості інформаційних систем [1].

NIST є провідною державною науково-дослідною установою США, яка спеціалізується на розробці стандартів, методологій і рекомендацій у сфері технологій і безпеки. Cybersecurity Framework, у свою чергу, являє собою набір добровільних практик, що допомагають організаціям оцінювати власний рівень кіберзахищеності, формувати заходи реагування на інциденти та розробляти довгострокові стратегії управління ризиками. Структурно фреймворк складається з трьох ключових елементів: Core (Ядро), що містить набір функцій і категорій для управління кіберризиками; Implementation Tiers (Рівні впровадження), які відображають рівень зрілості системи безпеки; та Profiles (Профілі), що дозволяють адаптувати вимоги фреймворку до контексту конкретної організації.

Перший варіант, CSF 1.0, був опублікований у лютому 2014 року на виконання Указу Президента США № 13636 “Improving Critical Infrastructure Cybersecurity”[1]. Його головною метою було підвищення захищеності критичної інфраструктури держави, зокрема в галузях енергетики, транспорту, телекомунікацій і фінансів. Основними досягненнями цієї версії стало визначення п’яти базових функцій (Identify, Protect, Detect, Respond, Recover), орієнтація на добровільність та універсальність застосування, а також впровадження концепції «профілю», що дозволяла налаштовувати вимоги CSF під особливості конкретної організації. Версія 1.0 заклала фундамент для формування єдиного методологічного підходу до кіберзахисту як у державному, так і в приватному секторі.

У квітні 2018 року була опублікована оновлена версія 1.1, яка врахувала досвід практичного використання попередньої редакції протягом чотирьох років. Серед основних вдосконалень варто виокремити деталізацію питань управління ризиками в ланцюзі постачальників, уточнення ролі механізмів автентифікації та ідентифікації користувачів, розширення рекомендацій щодо інтеграції управління ризиками в бізнес-процеси, а також доопрацювання глосарію та методологічних пояснень. Версія 1.1 зробила фреймворк більш практичним інструментом, особливо для компаній, що функціонують у глобальних ланцюгах постачання.

Найбільш масштабним оновленням став випуск версії 2.0 у лютому 2024 року. Цей документ суттєво розширив сферу застосування CSF: якщо початково він був спрямований насамперед на критичну інфраструктуру, то тепер його рекомендації поширюються на будь-які організації – від малого бізнесу до міжнародних корпорацій. Серед ключових нововведень варто відзначити запровадження шостої функції Govern (Управляти), що охоплює принципи стратегічного управління, ролі керівництва, політики й процеси прийняття рішень у сфері кібербезпеки. Посилено увагу до вищого менеджменту та рад директорів, які мають усвідомлювати власну відповідальність за кіберризики. Оновлені методології управління ризиками у ланцюгах постачальників враховують зростаючу глобалізацію та появу загроз нового покоління. Крім того, було розширено набір ресурсів і прикладів, що полегшують адаптацію фреймворку до потреб різних організацій.

Важливо підкреслити, що популярність CSF вийшла далеко за межі США. Уже після першої редакції 2014 року його активно почали адаптувати у Європі, Азії та країнах, що розвиваються, адже рамка не накладає жорстких регуляторних вимог, а пропонує універсальні орієнтири [4]. Це дозволило організаціям різного масштабу створити власні профілі безпеки, адаптовані до галузевих ризиків та локального законодавства.

Ключові відмінності NIST 1.1 та NIST 2.0

Перехід від NIST Cybersecurity Framework версії 1.1 до версії 2.0 символізує значний еволюційний стрибок у сфері кібербезпеки, викликаний динамічною зміною кіберзагроз, розвитком технологій та потребою в організаційній стійкості. Версія 1.1 дала основні п’ять функцій (Identify, Protect, Detect, Respond, Recover), які сформували фундамент для побудови структурованого підходу до управління ризиками. Натомість CSF 2.0 вводить суттєво модернізовану базову структуру, водночас зберігаючи концептуальну непорушність оригінальних функцій, але адаптуючи їх до актуальних потреб і викликів сучасного кіберпростору.

Основною зміною у структурі є вдосконалення базових функцій Identify, Protect, Detect, Respond та Recover. У версії 1.1 ці функції окреслювали основні напрями діяльності в галузі кібербезпеки, але залишалися дещо узагальненими. Версія 2.0

деталізувала й уточнила їх зміст, зробивши структуру більш інтуїтивною та зручною для використання. Завдяки цьому рамка набуває більшої гнучкості та зрозумілості для різних категорій організацій, незалежно від їхнього розміру чи сфери діяльності.

Ключовим доповненням у CSF 2.0 є впровадження шостої основної функції – Govern. Цей функціонал формально виокремлює кібербезпеку як предмет корпоративного управління, що включає стратегію, політику, розподіл відповідальності та узгодження з бізнес-цілями. Governance дозволяє збільшити залучення топ-менеджменту, посилити прозорість прийняття рішень і інтегрувати кібербезпеку у загальну систему управління ризиками організації.

Особливий наголос робиться на узгодженні кібербезпекової стратегії з бізнес-цілями та на залученні керівництва до процесу прийняття рішень. Це підкреслює розуміння того, що ефективний захист від загроз можливий лише за умови, коли кібербезпека перестає бути виключно завданням IT-відділу й охоплює всі рівні організаційної ієрархії.

Особливістю CSF 2.0 є надання більш практичного, прикладного підґрунтя. Введено розділ «Implementation Examples», який допомагає організаціям конкретизувати субкатегорії через реальні приклади, зменшуючи розрив між концепцією та практикою. Паралельно CSF 2.0 укріплює напрями безпеки у ланцюгах постачання (Supply Chain Risk Management), із детальними рекомендаціями для оцінювання, класифікації постачальників, включення їх у політики та процедури управління кіберризиками. До того ж, у функції Identify з'явилася нова категорія Improvement, яка надає більше можливостей для постійного удосконалення практик кіберзахисту.

Ще однією ключовою відмінністю стало посилення інтеграції з іншими міжнародними стандартами. Версія 1.1 лише частково враховувала взаємозв'язок із суміжними підходами, тоді як CSF 2.0 значно розширила можливості узгодження з такими сферами, як управління приватністю чи ризиками в ланцюгах постачання. Завдяки цьому рамка стала інструментом, що забезпечує комплексне бачення ризик-менеджменту та підвищує узгодженість дій на міжорганізаційному рівні.

Помітні зміни торкнулися і системи вимірювання ефективності. Якщо у попередній версії метрики мали здебільшого високорівневий характер, то у CSF 2.0 з'явився акцент на кількісних і якісних показниках. Це дозволяє організаціям здійснювати більш точну оцінку результатів та визначати зони, які потребують удосконалення. Це забезпечує можливість не лише впроваджувати заходи кіберзахисту, а й відстежувати їх реальну дієвість.

У версії 2.0 надано детальнішу увагу проблематиці безпеки ланцюгів постачання. У CSF 1.1 цей аспект визнавався, проте обмежувався загальними зауваги. Натомість у новій редакції пропонуються комплексні стратегії управління ризиками, пов'язаними з постачальниками, що стало відповіддю на низку масштабних атак у цій сфері. Наприклад, 5 вересня 2025 року компанія GitGuardian виявила GhostAction – масштабну атаку на ланцюг постачання, яка торкнулася 327 користувачів GitHub у 817 репозиторіях; зловмисники впровадили шкідливі workflows і викрали 3 325 секретів, включно з токенами PyPI, npm та DockerHub [14]. Такий підхід дозволяє організаціям не лише краще захищати власні інформаційні системи, а й враховувати взаємозалежності та потенційні вразливості у ширшій мережі співпраці.

Перехід від версії NIST Cybersecurity Framework 1.1 до версії 2.0 став якісним кроком уперед у розвитку концепції управління кіберризиками. CSF 2.0 переглянута структура категорій і субкатегорій: тепер він містить 6 функцій, 22 категорії та 106 субкатегорій, тоді як у CSF 1.1 було 5 функцій, 23 категорії й 108 субкатегорій.

Значна кількість підкатегорій CSF 1.1 була переміщена у нову функцію **Govern**, що відображає акцент на стратегічному вимірі кібербезпеки. Наприклад:

- контроль **ID.GV** («політики, процедури та процеси з управління кіберризиками») у CSF 2.0 трансформувався в **GV** із уточненням, що йдеться саме про систему управління ризиками на рівні організації;
- контроль **ID.BE** («місія, цілі та зацікавлені сторони організації») переміщено у категорію **GV.OC**, де підкреслено залежність кібербезпеки від бізнес-контексту;
- контроль **ID.RM-1** («процеси управління ризиками») отримав нове формулювання у **GV.RM-01**, що деталізує завдання з формування об'єктивів управління ризиками.

Ці зміни показують, що кібербезпека перестає розглядатися лише як технічне завдання IT-підрозділу, натомість інтегрується у стратегічне управління організацією.

Частина підкатегорій CSF 1.1 була інкорпорована в інші контролі або об'єднана для уникнення дублювання. Зокрема:

- контроль **ID.BE-2** («місце організації у критичній інфраструктурі») та **ID.BE-3** («пріоритети місії та цілей») об'єднані у нову підкатегорію **GV.OC-01**, яка більш комплексно описує розуміння місії організації в контексті кіберризиків;
- контроль **ID.GV-2** («роль і відповідальність у кібербезпеці») інтегрований у **GV.OC-02**, де йдеться про ширше розуміння внутрішніх і зовнішніх зацікавлених сторін;
- контроль **ID.SC-2** («постачальники та партнери інформаційних систем») також став частиною **GV.OC-02**, що підкреслює важливість управління стейкхолдерами у єдиній площині.

Таким чином, замість кількох розрізнених вимог користувач отримує цілісніші, логічно впорядковані категорії.

У CSF 2.0 з'явилися абсолютно нові підкатегорії, які не мають прямих аналогів у CSF 1.1. Наприклад:

- **GV.RM-07** – «Стратегічні можливості (позитивні ризики) враховані в управлінні кіберризиками». Це нововведення вводить концепцію позитивного ризику (opportunity), яка у попередніх версіях не розглядалася.
- **GV.RR-01** – «Організаційне керівництво несе відповідальність і підзвітне за управління кіберризиками». Це чітко закріплює відповідальність керівництва, чого у версії 1.1 бракувало.
- **GV.OV-01/02** – підкатегорії, що описують результати та сталість стратегії управління ризиками, які взагалі не мали попередників.

Поява таких нових контролів пов'язана з глобалізацією застосування Framework і потребою інтегрувати кібербезпеку у стратегічне управління, а не лише в операційний рівень.

У CSF 2.0 є підкатегорії, які не мають прямих посилань на CSF 1.1. Це пояснюється двома причинами: розширення сфери застосування та зміна структури та термінології. Framework більше не обмежується критичною інфраструктурою, тому з'явилися вимоги, релевантні малому бізнесу, неурядовим організаціям тощо.

Таблиця 1

Порівняння NIST CSF 1.1 та NIST CSF 2.0

Характеристика	NIST CSF 1.1 (2018)	NIST CSF 2.0 (2024)
Основні функції	5 функцій: Identify, Protect, Detect, Respond, Recover	6 функцій: Govern, Identify, Protect, Detect, Respond, Recover
Структура категорій і субкатегорій	23 категорій, 108 субкатерогій	22 категорій, 106 субкатерогій
Фокус управління	Обмежені рекомендації з управління	Сильний фокус на управлінні кібербезпекою та відповідальності керівництва
Сфера застосування	Переважно для секторів критичної інфраструктури	Розширено для всіх організацій, включаючи малі підприємства та уряд
Безпека ланцюга постачання	Загальні рекомендації щодо ризиків, пов'язаних із третіми сторонами	Підвищена увага до управління ризиками ланцюга поставок та безпеки постачальників
Сучасні загрози	Обмежена увага до безпеки хмарних технологій, загроз, пов'язаних з штучним інтелектом, та моделі «нульової довіри»	Оновлено з урахуванням безпеки хмарних технологій, атак на основі штучного інтелекту, програм-вимагачів та моделі «нульової довіри»
Керівництво з впровадження	Загальні рекомендації щодо впровадження	Більш детальне керівництво для кращого впровадження
Відповідність нормативним вимогам	Відповідність деяким нормативним вимогам, таким як ISO 27001 та NIST 800-53	Краща відповідність мінливим глобальним нормативним вимогам та поточним рамкам відповідності

Порівняємо для додаткового розуміння NIST CSF 2.0 і стандарт ISO/IEC 27001. Обидва базуються на оцінці ризиків, підтримують постійне вдосконалення та можуть адаптуватися до різних організацій. Головна відмінність у тому, що ISO 27001 – це міжнародний стандарт, який можна сертифікувати, і він фокусується на створенні системи управління інформаційною безпекою [10]. Натомість NIST CSF 2.0 – це гнучка рамка, яка більше орієнтована на практичне управління кіберризиками та відновлення після інцидентів. NIST часто використовують як стартову точку, а ISO – для побудови більш формальної та сертифікованої системи безпеки.

Незважаючи на скорочення кількості підкатегорій із 108 до 106, CSF 2.0 забезпечує якісне посилення: у ньому впорядковано й об’єднано дублювальні раніше вимоги, інтегровано нові підходи до корпоративного управління, відповідальності керівництва та управління ланцюгами постачання. Зміни не лише підвищили логічну цілісність моделі, але й надали організаціям більш гнучкий, прикладний та стратегічно значущий інструмент для протидії сучасним кіберзагрозам.

Особливості переходу до NIST 2.0

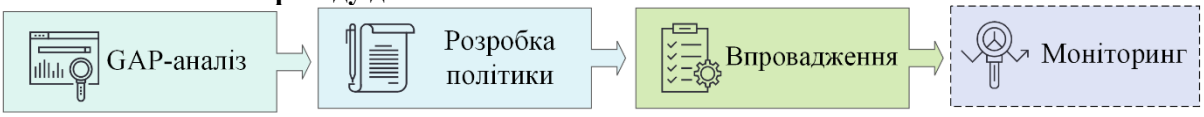

Рис 1. Блок-схема процесу переходу до NIST 2.0

Процес переходу NIST 2.0 не зводиться лише до технічної інтеграції нових вимог – він вимагає комплексного підходу. Першим кроком є усвідомлення змістовних нововведень, адже саме вони визначають логіку адаптації чинних механізмів безпеки. Як ми вже визначили, серед найвагоміших змін у CSF 2.0 є введення нової функції Govern,

що підкреслює підзвітність вищого керівництва та потребу у формуванні корпоративної культури, орієнтованої на усвідомлення ризиків. Водночас посилено увагу до вимірюваних результатів діяльності у сфері кібербезпеки, управління ризиками ланцюгів постачальників, а також інтеграції практик безпечної розробки програмного забезпечення. Нововведення також торкнулися сфери розвідки загроз, інтеграції з SIEM-системами, захисту даних та процесів відновлення після інцидентів.

Усвідомивши характер цих змін, організація повинна розпочати підготовчий етап, який передбачає аналіз розривів між існуючим станом відповідності CSF 1.1 та новими вимогами CSF 2.0. На цьому етапі здійснюється оцінка наявних заходів безпеки, визначаються прогалини та формуються пріоритети їхнього усунення. Важливою умовою є забезпечення належної підтримки з боку керівництва, адже впровадження змін неможливе без чіткого розподілу ресурсів, навчання персоналу та формування єдиного бачення мети переходу. Ретельно підготовлений план дозволяє мінімізувати ризик операційних збоїв і забезпечити поступову адаптацію.

Перед безпосереднім переходом до NIST CSF 2.0 одним із ключових завдань для організацій є формалізація політик, що визначають принципи та правила функціонування системи кібербезпеки. Політики виступають базисом управлінської відповідальності та засобом комунікації між керівництвом, технічними фахівцями й персоналом загалом. Саме наявність чітко сформульованих і затверджених політик забезпечує узгодженість практик кіберзахисту з бізнес-цілями та правовими вимогами.

Основні політики, які рекомендує формувати та підтримувати NIST CSF 2.0, охоплюють такі напрями:

1. **Політика управління кіберризиками** (Cybersecurity Risk Management Policy) – визначає підходи до ідентифікації, аналізу, оцінки й зниження ризиків, узгоджуючи їх із загальною стратегією управління ризиками організації.

2. **Політика управління активами** (Asset Management Policy) – описує порядок інвентаризації, класифікації та контролю IT-ресурсів, включаючи обладнання, програмне забезпечення, дані та сервіси.

3. **Політика управління доступом** (Access Control Policy) – регламентує принципи надання, обмеження й моніторингу доступу до систем та інформації, у тому числі на основі ролей та мінімально необхідних прав.

4. **Політика управління інцидентами** (Incident Response Policy) – визначає процедури виявлення, повідомлення, ескалації та реагування на кіберінциденти, забезпечуючи чіткі механізми відповідальності.

5. **Політика управління постачальниками та ланцюгом постачання** (Supply Chain Risk Management Policy) – встановлює вимоги до оцінювання кіберризиків постачальників, укладання контрактів і моніторингу відповідності партнерів встановленим стандартам.

6. **Політика безперервності бізнесу та відновлення після інцидентів** (Business Continuity and Recovery Policy) – формалізує підхід до підтримки критичних процесів та швидкого відновлення після порушень чи атак.

7. **Політика управління персоналом та навчання** (Awareness and Training Policy) – регламентує вимоги до підвищення обізнаності співробітників, програм навчання та перевірки знань у сфері кібербезпеки.

8. **Політика удосконалення практик кіберзахисту** (Improvement Policy) – підтримує принцип постійного розвитку системи безпеки, враховуючи результати аудиту, аналізу інцидентів і нові регуляторні вимоги.

Таким чином, ще до переходу до CSF 2.0 організація має сформувати комплекс політик, які стануть «каркасом» для операційних процесів, технічних заходів та стратегічних рішень.

Не менш значущим етапом є формування стратегії впровадження, яка має містити деталізований календар робіт, чіткий розподіл відповідальностей та інтеграцію змін у чинні бізнес-процеси. Саме на цьому етапі з'являється можливість для модернізації: впровадження архітектури Zero Trust, використання механізмів автоматизаціїзаходів безпеки, а також перехід до хмароорієнтованих інфраструктур. Успіх такої стратегії залежить від регулярного перегляду результатів, своєчасного коригування дій та ефективної комунікації між усіма рівнями організаційної ієрархії.

Важливу роль у досягненні відповідності CSF 2.0 відіграє автоматизація операцій кіберзахисту. Вона забезпечує значну оптимізацію рутинних процесів – таких як сканування вразливостей, аналіз журналів та виявлення загроз, – підвищуючи сталість і надійність захисних механізмів. Автоматизовані інструменти надають можливість здійснювати моніторинг у режимі реального часу та оперативно реагувати на інциденти, що повністю узгоджується з акцентом CSF 2.0 на проактивному управлінні загрозами. Крім того, автоматизація сприяє безперервному вдосконаленню систем захисту шляхом забезпечення актуальних даних для прийняття рішень, що зміцнює кіберстійкість організації у динамічному середовищі загроз.

Варто також підкреслити, що кібербезпека є динамічною сферою, і тому постійна обізнаність та гнучкість залишаються необхідною умовою. Регулярний моніторинг публікацій NIST, участь у професійних форумах, інтеграція розвідки загроз, постійне оновлення політик і підготовка персоналу дозволяють організаціям своєчасно реагувати на нові виклики. Лише ті інституції, які здатні швидко адаптуватися та переглядати власні підходи, зберігають високу кіберстійкість у мінливому середовищі.

В Україні перехід до NIST CSF 2.0 почався доволі швидко. Вже 30 січня 2025 року голова Держспецзв'язку Олександр Потій підписав наказ про впровадження оновленого Cybersecurity Framework 2.0 [15]. Цей документ закріпив перелік базових заходів із кіберзахисту та надав практичні рекомендації для їх реалізації. Уже раніше Держспецзв'язку почала впровадження окремих елементів CSF 2.0. Наприкінці минулого року було оновлено Організаційно-технічну модель кіберзахисту (ОТМ), що передбачає обов'язкове виконання базових кіберзахисних заходів усіма суб'єктами сфери кібербезпеки – незалежно від їхнього масштабу, галузі діяльності чи рівня зрілості. Це стосується як державних установ і об'єктів критичної інфраструктури, так і приватного сектора, включно з промисловими підприємствами. Вказані заходи охоплюють шість ключових функцій кіберзахисту: управління, ідентифікація, захист, виявлення, реагування та відновлення.

У 2024 році завдяки підтримці USAID було впроваджено проєкт «Кібербезпека критично важливої інфраструктури України». За принципами CSF 2.0 відбулась кібердіагностика ОДА та інших структурних органів управління. У результаті проведених кібердіагностичних заходів учасники отримали всебічну оцінку стану своєї цифрової безпеки. Виконання наданих рекомендацій дозволить їм суттєво покращити рівень кіберзрілості та підвищити готовність до можливих кіберінцидентів.

Перехід до NIST CSF 2.0 є не стільки технічним оновленням, скільки стратегічним кроком, що дозволяє організаціям переосмислити управління ризиками та підняти зрілість кіберзахисту на якісно новий рівень. Успіх залежить від усвідомлення змін, ретельної підготовки, побудови чіткої стратегії, інтеграції автоматизації та використання сучасних інструментів, а також готовності до постійного навчання і гнучкої адаптації. У

підсумку CSF 2.0 стає фундаментом для довгострокової цифрової стійкості та зміцнення довіри до кіберсистем організацій.

Інструменти для впровадження NIST Cybersecurity Framework

Практична реалізація NIST Cybersecurity Framework (NIST CSF) у сучасних організаціях вимагає не лише методологічної зрілості, а й використання спеціалізованих інструментів, які забезпечують оцінку, впровадження та моніторинг заходів безпеки. У цьому контексті з'явився цілий спектр рішень – від безкоштовних державних платформ до потужних корпоративних систем управління ризиками. Їхня роль полягає у тому, щоб зробити NIST CSF не лише нормативною рамкою, а дієвим інструментом постійного управління кіберризиками.

Одним із найвідоміших інструментів є CSET (Cyber Security Evaluation Tool) – безкоштовне рішення, розроблене під егідою Департаменту внутрішньої безпеки США. Його основне завдання полягає у наданні організаціям можливості проводити самооцінку стану кібербезпеки відповідно до різних стандартів, зокрема NIST CSF, NIST SP 800-53, ISO/IEC 27001 та інших. CSET реалізує підхід структурованого опитувальника, що охоплює п'ять основних функцій NIST CSF: Identify, Protect, Detect, Respond та Recover. Результати аналізу автоматично порівнюються з еталонними профілями, що дозволяє визначати пріоритети удосконалення системи безпеки.

Перевагою CSET є його доступність і універсальність. Завдяки модульній структурі цей інструмент можна адаптувати як для малих організацій, так і для критичної інфраструктури. CSIRT також пропонує локалізовану версію CSET, що сприяє його поширенню у державному секторі [16].

Іншим важливим класом інструментів є системи GRC (Governance, Risk, and Compliance), які інтегрують принципи управління ризиками та відповідності нормативним вимогам. Одним із найпоширенішим корпоративним рішень цього класу є ServiceNow GRC. Ця платформа дозволяє організаціям централізовано керувати політиками, ризиками та аудитами, а також зіставляти внутрішні контролі з вимогами NIST CSF. Інтеграція з іншими модулями ServiceNow (зокрема IT Operations Management та Security Operations) забезпечує наскрізний моніторинг стану безпеки і дозволяє виявляти відхилення в режимі реального часу.

ServiceNow GRC також підтримує автоматизацію процесів комплаєнсу. Це означає, що виявлені невідповідності у політиках або технічних контролях можуть автоматично ініціювати завдання для відповідальних осіб [17].

До цієї ж категорії належить рішення Archer IRM. Archer забезпечує комплексний підхід до управління ризиками, охоплюючи ризики, політики, аудити та інциденти у єдиній інформаційній моделі. У контексті NIST CSF ця платформа дозволяє створювати власні профілі безпеки, що відповідають конкретним операційним цілям організації. Завдяки модульності Archer може інтегруватися з існуючими інформаційними системами, забезпечуючи прозорість у відстеженні змін рівня кіберзахисту.

Важливою перевагою Archer є аналітичні можливості – система надає гнучкі інструменти звітності та дашборди для вимірювання ефективності заходів кібербезпеки. Це дозволяє не лише підтримувати відповідність NIST CSF, а й продемонструвати керівництву вплив кіберризиків на бізнес-процеси. У цьому сенсі Archer є інструментом стратегічного управління, який поєднує технічну й організаційну складові кіберзахисту.

На технічному рівні важливу роль у забезпеченні функцій NIST CSF відіграють інструменти моніторингу та аналізу подій безпеки. Одним із найвідоміших рішень цього класу є Splunk, який використовується для збирання, обробки й аналітики даних журналів безпеки. Splunk підтримує реалізацію функцій Detect та Respond NIST CSF,

забезпечуючи своєчасне виявлення інцидентів і кореляцію подій між різними джерелами. Перевага Splunk полягає у високій масштабованості та можливості інтеграції з сотнями зовнішніх джерел – від систем ідентифікації до хмарних сервісів.

Ще одним важливим інструментом технічної перевірки відповідності є Tenable, який спеціалізується на виявленні вразливостей та аналізі кіберризиків. Tenable надає можливість безперервного моніторингу інформаційних систем, виявлення слабких місць у конфігураціях і співставлення їх із категоріями NIST CSF. Це дозволяє організаціям безпосередньо пов'язувати технічні ризики з бізнес-ризиками, підвищуючи ефективність пріоритизації заходів безпеки.

Tenable також реалізує концепцію "continuous view" – безперервного бачення стану кіберзахисту, що узгоджується з принципами NIST CSF щодо постійного удосконалення. Звіти, які формує система, можуть бути використані для підтвердження ефективності контрольних заходів у рамках аудиту відповідності. Таким чином, Tenable виступає як технологічна опора для реалізації функцій Protect та Detect.

Таблиця 2

Порівняльна характеристика інструментів для впровадження NIST Cybersecurity Framework

Інструмент	Тип рішення	Основні функції NIST CSF	Ключові можливості	Переваги	Обмеження
CSET	Безкоштовний інструмент самооцінки	Identify, Protect, Detect, Respond, Recover	Оцінка зрілості, опитувальники, графічна візуалізація результатів	Безкоштовність, простота, адаптація до різних стандартів	Відсутність автоматизації процесів, обмежена інтеграція
ServiceNow GRC	Корпоративна платформа GRC	Identify, Protect, Respond	Управління політиками, ризиками, аудитами, автоматизація процесів	Глибока інтеграція з IT-операціями, автоматизація комплаєнсу	Висока вартість впровадження, потреба у налаштуванні
Archer IRM	Платформа управління ризиками	Identify, Protect, Respond, Recover	Моделювання ризиків, політики, аудити, дашборди	Комплексний підхід, розвинена аналітика	Складність конфігурації, висока ціна
Splunk	Платформа аналітики та SIEM	Detect, Respond	Збір і кореляція журналів, машинне навчання, аналітика подій	Висока масштабованість, підтримка NIST CSF-панелей	Високе споживання ресурсів, складність налаштування
Tenable	Платформа моніторингу вразливостей	Protect, Detect	Сканування вразливостей, пріоритизація ризиків, звітування	Безперервний моніторинг, зв'язок технічних ризиків із бізнес-ризиками	Обмежена стратегічна аналітика, потреба у додаткових модулях

Впровадження NIST CSF слід розглядати не як одноразову дію, а як безперервний процес оцінювання, адаптації та вдосконалення механізмів кіберзахисту. Кожен із розглянутих тулзів відіграє власну роль: CSET – у первинній самооцінці, ServiceNow та Archer – у стратегічному управлінні ризиками, Splunk і Tenable – у технічному моніторингу та реагуванні.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Еволюція CSF засвідчує тенденцію до інтеграції кібербезпеки в загальну систему стратегічного управління організацією. Це виражається у появі нових функцій, таких як Govern, що ставить акцент на відповідальності керівництва, формуванні політик і врахуванні кіберризиків у контексті бізнес-цілей.

Фреймворк демонструє поступовий перехід від техніко-орієнтованого підходу до практичного, системного інструменту управління ризиками, який адаптується до змін середовища, технологій та глобальних викликів. Це підкріплюється як структурною перебудовою категорій, так і впровадженням прикладних рішень – зокрема, у сфері безпеки ланцюгів постачання та вимірювання ефективності.

Також, можна стверджувати, що впровадження NIST 2.0 вимагає не лише технічної адаптації, а й культурних змін усередині організації – від формування нових політик до розбудови свідомого ставлення до кіберризиків на всіх рівнях.

Таким чином, NIST CSF 2.0 є не просто оновленням існуючого стандарту, а якісно новим етапом у формуванні методологічної основи кіберзахисту. Він поєднує стратегічну орієнтацію, гнучкість, практичність і міжнародну сумісність, що робить його ефективним інструментом для зміцнення цифрової стійкості в умовах постійно зростаючих та ускладнених кіберзагроз.

Ефективна реалізація NIST Cybersecurity Framework на практиці засвідчує, що управління кіберризиками не може ґрунтуватися на використанні одного інструмента чи методології. Кожен з наявних тулзів виконує лише окрему функцію в загальній системі безпеки – від оцінки зрілості до моніторингу технічних ризиків. Лише їх комплексне застосування дає змогу сформувати цілісну картину стану захищеності, виявити взаємозалежності між бізнес-процесами та кіберзагрозами й забезпечити реальне управління ризиками, а не формальну відповідність вимогам.

Еволюція CSF засвідчує тенденцію до інтеграції кібербезпеки в загальну систему стратегічного управління організацією. Це виражається у появі нових функцій, таких як Govern, що ставить акцент на відповідальності керівництва, формуванні політик і врахуванні кіберризиків у контексті бізнес-цілей.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. National Institute of Standards and Technology. (2014). *Framework for improving critical infrastructure cybersecurity* (Version 1.0). Gaithersburg, MD: NIST. https://doi.org/10.6028/nist.cswp.02122014
2. National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). Gaithersburg, MD: NIST. https://doi.org/10.6028/nist.cswp.04162018
3. National Institute of Standards and Technology. (2023). *The NIST cybersecurity framework 2.0.* Gaithersburg, MD: NIST. https://doi.org/10.6028/nist.cswp.29
4. Teoh, C. S., Mahmood, A. K., & Dzazali, S. (2017). Is NIST CSF applicable for developing nations? A case study on government sector in Malaysia. *Proceedings of the Pacific Asia Conference on Information Systems (PACIS 2017).*
5. Ibrahim, A., Valli, C., McAteer, I., & Chaudhry, J. (2018). A security review of local government using NIST CSF: A case study. *The Journal of Supercomputing, 74*(10), 5171–5186. https://doi.org/10.1007/s11227-018-2479-2
6. Moskowitz, D., & Nichols, D. M. (2022). *A practitioner's guide to adapting the NIST cybersecurity framework.* London: TSO.
7. White, G. B., & Sjelin, N. (2022). The NIST cybersecurity framework. In I. Management Association (Ed.), *Research anthology on business aspects of cybersecurity* (pp. 39–55). IGI Global. https://doi.org/10.4018/978-1-6684-3698-1.ch003

8. Pemmasani, P. K. (2023). National cybersecurity frameworks for critical infrastructure: Lessons from governmental cyber resilience initiatives. *International Journal of Acta Informatica, 2*(1), 209–218.
9. Hätinen, M. (2024). *Evolution of cybersecurity risk management standardization: Comparison of the NIST cybersecurity framework version 1.1 and 2.0.*
10. Parmar, M., & Miles, A. (2024). Cyber security frameworks (CSFs): An assessment between the NIST CSF v2.0 and EU standards. *Proceedings of the IEEE Security Space Systems (3S) Conference,* Noordwijk, Netherlands, 1–7. https://doi.org/10.23919/3s60530.2024.10592293
11. Edwards, J. (2024). *A comprehensive guide to the NIST cybersecurity framework 2.0: Strategies, implementation, and best practice.* Hoboken, NJ: John Wiley & Sons.
12. SecurityCompass. (2025). *NIST CSF 1.1 vs. 2.0: Key differences explained.* https://www.securitycompass.com/blog/nist-csf-1-1-vs-2-differences/
13. Zhylin, A., Belyavskyi, V., & Bakalynskyi, O. (2024). NIST CSF 2.0: Novyi freimvork z kiberbezpeky vid Natsionalnoho instytutu standartiv i tekhnolohii SShA [NIST CSF 2.0: The new cybersecurity framework from the U.S. National Institute of Standards and Technology]. *Ukrainian Scientific Journal of Information Security, 30*(1), 73–76. https://doi.org/10.18372/2225-5036.30.18606
14. Ferry, G., & Valadon, G. (2025). *The Ghost Action Campaign: 3,325 secrets stolen through compromised GitHub workflows.* GitGuardian Blog. https://blog.gitguardian.com/ghostaction-campaign-3-325-secrets-stolen/
15. Derzhavna sluzhba spetsialnoho zviazku ta zakhystu informatsii Ukrainy. (2025). *Nakaz № 54 vid 30.01.2025 "Pro zatverdzhennia bazovykh zakhodiv z kiberzakhystu ta metodychnykh rekomendatsii shchodo zdiisnennia bazovykh zakhodiv z kiberzakhystu"* [Order No. 54 of January 30, 2025 "On approval of basic cybersecurity measures and methodological recommendations for their implementation"]. https://cip.gov.ua/ua/docs/nakaz-administraciyi-derzhspeczv-yazku-vid-30-01-2025-54-pro-zatverdzhennya-bazovikh-zakhodiv-z-kiberzakhistu-ta-metodichnikh-rekomendacii-shodo-zdiisnennya-bazovikh-zakhodiv-z-kiberzakhistu
16. CSIRT of the State Research Institute of Cybersecurity Technologies and Information Protection. (2025). *CSET cybersecurity assessment tool.* https://csirt.csi.cip.gov.ua/uk/pages/cset
17. DevTools. (2025). *ServiceNow GRC: Everything you need to know.* https://devtools.in/blog/servicenow-grc/

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (30), 2025
Спеціальний випуск ISSN 2663 – 4023
Special issue

Yaryna A. Zakharova
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: 0009-0006-0129-7944
yaryna.zakharova.mkbas.2024@lpnu.ua

Andriy I. Partyka
Candidate of Technical Sciences, Associate Professor,
Associate Professor at the Departmentof Information Protection
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: 0000-0003-3037-8373
andrii.i.partyka@lpnu.ua

THE EVOLUTION OF CYBER RISK MANAGEMENT THROUGH THE PRISM OF THE NIST CYBERSECURITY FRAMEWORK

Abstract. The article provides a comprehensive analysis of the evolution of the NIST Cybersecurity Framework from its initial version 1.0 to the current version 2.0. It highlights the background to the creation of the framework, its place in international practice, and its key role in improving the cyber resilience of organizations of all sizes, from small companies to global corporations and government agencies. It examines in detail the features of previous editions, in particular CSF 1.0, which laid the foundation in the form of five basic functions (Identify, Protect, Detect, Respond, Recover), and CSF 1.1, which clarified approaches to risk management in supply chains and made the framework more applicable. It is shown that the transition to CSF 2.0 in 2024 was a qualitative stage of development, as the new version focuses not only on technical aspects but also on strategic corporate governance. Among the key innovations are the Govern function, which formally establishes management responsibility, as well as expanded opportunities for integration with international standards, improved performance metrics, and increased focus on supply chain risk management. The specifics of the transition process for organizations to CSF 2.0 are analyzed separately. It includes analyzing the gaps between the current state of security and the new requirements, forming policies, building an implementation strategy, applying automation and Zero Trust tools, as well as training personnel. It is emphasized that successful adaptation depends on support from senior management, the formation of a security culture, and continuous improvement of procedures. The article also considers the Ukrainian context, where the implementation of CSF 2.0 is supported at the state level by the State Service of Special Communications and Information Protection of Ukraine and with the participation of international partners. The practical value of the study lies in the possibility of using its conclusions and recommendations to develop long-term cyber risk management strategies in both the public and private sectors.

Keywords: NIST CSF 2.0, cybersecurity, risk management, information security, cybersecurity policy.

REFERENCES

1. National Institute of Standards and Technology. (2014). *Framework for improving critical infrastructure cybersecurity* (Version 1.0). Gaithersburg, MD: NIST. https://doi.org/10.6028/nist.cswp.02122014
2. National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). Gaithersburg, MD: NIST. https://doi.org/10.6028/nist.cswp.04162018
3. National Institute of Standards and Technology. (2023). *The NIST cybersecurity framework 2.0.* Gaithersburg, MD: NIST. https://doi.org/10.6028/nist.cswp.29
4. Teoh, C. S., Mahmood, A. K., & Dzazali, S. (2017). Is NIST CSF applicable for developing nations? A case study on government sector in Malaysia. *Proceedings of the Pacific Asia Conference on Information Systems (PACIS 2017).*
5. Ibrahim, A., Valli, C., McAteer, I., & Chaudhry, J. (2018). A security review of local government using NIST CSF: A case study. *The Journal of Supercomputing*, *74*(10), 5171–5186. https://doi.org/10.1007/s11227-018-2479-2

6. Moskowitz, D., & Nichols, D. M. (2022). *A practitioner's guide to adapting the NIST cybersecurity framework.* London: TSO.
7. White, G. B., & Sjelin, N. (2022). The NIST cybersecurity framework. In I. Management Association (Ed.), *Research anthology on business aspects of cybersecurity* (pp. 39–55). IGI Global. https://doi.org/10.4018/978-1-6684-3698-1.ch003
8. Pemmasani, P. K. (2023). National cybersecurity frameworks for critical infrastructure: Lessons from governmental cyber resilience initiatives. *International Journal of Acta Informatica, 2*(1), 209–218.
9. Hätinen, M. (2024). *Evolution of cybersecurity risk management standardization: Comparison of the NIST cybersecurity framework version 1.1 and 2.0.*
10. Parmar, M., & Miles, A. (2024). Cyber security frameworks (CSFs): An assessment between the NIST CSF v2.0 and EU standards. *Proceedings of the IEEE Security Space Systems (3S) Conference*, Noordwijk, Netherlands, 1–7. https://doi.org/10.23919/3s60530.2024.10592293
11. Edwards, J. (2024). *A comprehensive guide to the NIST cybersecurity framework 2.0: Strategies, implementation, and best practice.* Hoboken, NJ: John Wiley & Sons.
12. SecurityCompass. (2025). *NIST CSF 1.1 vs. 2.0: Key differences explained.* https://www.securitycompass.com/blog/nist-csf-1-1-vs-2-differences/
13. Zhylin, A., Belyavskyi, V., & Bakalynskyi, O. (2024). NIST CSF 2.0: Novyi freimvork z kiberbezpeky vid Natsionalnoho instytutu standartiv i tekhnolohii SShA [NIST CSF 2.0: The new cybersecurity framework from the U.S. National Institute of Standards and Technology]. *Ukrainian Scientific Journal of Information Security, 30*(1), 73–76. https://doi.org/10.18372/2225-5036.30.18606
14. Ferry, G., & Valadon, G. (2025). *The Ghost Action Campaign: 3,325 secrets stolen through compromised GitHub workflows.* GitGuardian Blog. https://blog.gitguardian.com/ghostaction-campaign-3-325-secrets-stolen/
15. Derzhavna sluzhba spetsialnoho zviazku ta zakhystu informatsii Ukrainy. (2025). *Nakaz № 54 vid 30.01.2025 "Pro zatverdzhennia bazovykh zakhodiv z kiberzakhystu ta metodychnykh rekomendatsii shchodo zdiisnennia bazovykh zakhodiv z kiberzakhystu"* [Order No. 54 of January 30, 2025 "On approval of basic cybersecurity measures and methodological recommendations for their implementation"]. https://cip.gov.ua/ua/docs/nakaz-administraciyi-derzhspeczv-yazku-vid-30-01-2025-54-pro-zatverdzhennya-bazovikh-zakhodiv-z-kiberzakhistu-ta-metodichnikh-rekomendacii-shodo-zdiisnennya-bazovikh-zakhodiv-z-kiberzakhistu
16. CSIRT of the State Research Institute of Cybersecurity Technologies and Information Protection. (2025). *CSET cybersecurity assessment tool.* https://csirt.csi.cip.gov.ua/uk/pages/cset
17. DevTools. (2025). *ServiceNow GRC: Everything you need to know.* https://devtools.in/blog/servicenow-grc/