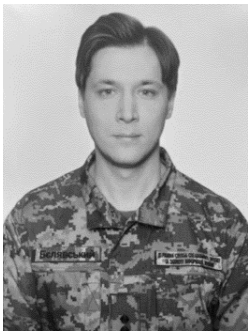
DOI: 10.18372/2225-5036.30.18606

NIST CSF 2.0: НОВИЙ ФРЕЙМВОРК З КІБЕРБЕЗПЕКИ ВІД НАЦІОНАЛЬНОГО ІНСТИТУТУ СТАНДАРТІВ І ТЕХНОЛОГІЙ США

Артем Жилін, Владислав Бєлявський, Олександр Бакалинський

Національний технічний університет «Київський політехнічний інститут імені Ігоря Сікорського»

ЖИЛІН Артем Вікторович, к.т.н., доцент
Рік та місце народження: 1982, м. Олександрія, Кіровоградської обл., Україна.
Освіта: ЖВІРЕ ім. С.П. Корольова, 2005.
Посада: професор кафедри кібербезпеки і застосування інформаційних систем і технологій ІСЗЗІ КПІ ім. Ігоря Сікорського.
Наукові інтереси: кібербезпека, методологічні підходи та засоби забезпечення кібербезпеки.
Публікації: більше 40 наукових публікацій, серед яких наукові статті, монографії, підручники та навчально-методичні посібники.
E-mail: zhylinartem@gmail.com.
Orcid ID: 0000-0002-4959-612X.



БЄЛЯВСЬКИЙ Владислав Олександрович, PhD
Рік та місце народження: 1989, м. Одеса, Україна.
Освіта: КНУ ім. Тараса Шевченка, 2012.
Посада: старший офіцер Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України.
Наукові інтереси: інформаційна безпека, реагування на інциденти інформаційної безпеки, штучний інтелект.
Публікації: більше 10 наукових публікацій, серед яких наукові статті, монографії та авторські методики.
E-mail: faroden663@gmail.com.
Orcid ID: 0000-0002-2626-0279.

БАКАЛИНСЬКИЙ Олександр Олегович, к.т.н., старший дослідник
Рік та місце народження: 1970 р., м. Київ, Україна.
Освіта: Київський військовий інститут управління та зв'язку, Національна академія Служби безпеки України.
Посада: заступник директора Департаменту кіберзахисту Адміністрації Державної служби спеціального зв'язку та захисту інформації України.
Наукові інтереси: системи управління інформаційною безпекою, управління ризиками, кібербезпека критичної інфраструктури, вища освіта.
Публікації: більше 70 наукових публікацій у галузі інформаційної, кібербезпеки, серед яких наукові статті, монографії, підручники та навчально-методичні посібники, патенти на корисні моделі.
E-mail: baov@meta.ua.
Orcid ID: 0000-0001-9712-2036.

Анотація. *Стаття присвячена детальному розгляду Cybersecurity Framework версії 2.0, який був представлений Національним Інститутом стандартів і технологій (NIST, National Institute of Standards and Technology) на початку 2024 року. CSF 2.0 створений для ефективного управління та зменшення ризиків в області кібербезпеки для різноманітних організацій, незалежно від їх розміру та сфери діяльності. Стаття розкриває ключові компоненти фреймворку, такі як Ядро (CSF Core), Організаційні профілі (CSF Organizational Profiles), Рівні безпеки (CSF Tiers), і надає інформацію щодо їхнього використання для покращення кібербезпекових практик організацій. Підкреслюється гнучкість фреймворку, яка дозволяє організаціям адаптувати свої підходи до управління кібербезпекою відповідно до їхніх унікальних ризиків та потреб. CSF 2.0 розглядається як важливий інструмент, призначений сприяти покращенню кібербезпеки на всіх рівнях організацій, незалежно від їхнього рівня технічної зрілості. Стаття також надає загальне уявлення про можливості використання ресурсів CSF для покращення кібербезпекових практик та наголошує на важливості постійного вдосконалення стратегій управління кібербезпекою для ефективного протистояння зростаючим кіберзагрозам.*

Ключові слова: *CSF 2.0, кібербезпека, NIST, організаційні профілі, фреймворк, кіберзагрози, інформаційна безпека.*

Постановка проблеми

У світі, де кіберзлочинність постійно зростає, ефективне управління кібербезпекою стає надзвичайно важливим завданням для будь-якої організації. Саме тому Національний Інститут стандартів і технологій (NIST) розробив Cybersecurity Framework (CSF) версії 2.0 – новий інструмент, який призначений допомогти організаціям різних розмірів та форм власності (від промисловості та уряду до неприбуткових організацій) зменшити свої ризики кібербезпеки. Незважаючи на рівень зрілості та технічну складність кібербезпекових програм, NIST CSF 2.0 пропонує гнучкий підхід, придатний для різних сценаріїв.

Мета та постановка завдання

Метою статті є докладне висвітлення основних аспектів та компонентів Cybersecurity Framework 2.0, а також можливостей використання цього фреймворку в сфері кібербезпеки.

Аналіз останніх досліджень і публікацій

NIST CSF 2.0, випущений Національним Інститутом стандартів і технологій США, представляє собою новий етап у розвитку інструментів кібербезпеки для організацій різного розміру та секторів. Фреймворк призначений для управління та зменшення ризиків в галузі кібербезпеки [1-3].

NIST CSF 2.0 визначає бажані результати, які можуть бути зрозумілі різною аудиторією, включаючи виконавців, менеджерів та фахівців, незалежно від їхньої експертизи в галузі кібербезпеки. Оскільки ці результати є сектор-, країна- та технологічно-нейтральними, вони надають організаціям гнучкість, необхідну для врахування їхніх унікальних ризиків, технологій та призначення.

Виклад основного матеріалу

NIST CSF 2.0 складається з наступних компонентів:

1. Ядро (CSF Core). Ядро CSF є таксономією високорівневих вимог до кібербезпеки, що допомагає організаціям управляти своїми ризиками. Включає Функції, Категорії та Підкатегорії, описуючи бажані результати кібербезпеки, зрозумілі різним аудиторіям;

2. Організаційні профілі (CSF Organizational Profiles). Організаційні профілі описують поточний та/або цільовий стан кібербезпеки організації, враховуючи її місію, очікування зацікавлених сторін, загрози та вимоги;

3. Рівні безпеки (CSF Tiers). Рівні безпеки – це рівні зрілості практик управління кіберризиками в організації. Ці рівні дозволяють визначити, наскільки виважено та прогресивно організація впроваджує стратегії кібербезпеки, а також як вона оцінює та управляє ризиками.

Центральною складовою NIST CSF 2.0 є ядро (CSF Core). Це основа фреймворку, що визначає високорівневі цілі та вимоги до кібербезпеки для організацій. CSF Core описує бажані результати в галузі кібербезпеки, що можуть бути зрозумілі широкій аудиторії, включаючи керівників, менеджерів та фахівців, незалежно від їхнього рівня експертизи в області кібербезпеки. CSF Core складається з таксономії, що охоплює кілька рівнів: функції (Functions), категорії (Categories) та підкатегорії (Subcategories). Функції є найвищим рівнем в цій ієрархії та представляють загальні аспекти управління кібербезпекою. Кожна функція поділяється на категорії, які в свою чергу розкривають специфічні аспекти кібербезпеки, а ці категорії поділяються на підкатегорії, що надають ще більш деталізовані вимоги та рекомендації.

Кожна функція визначає високорівневі вимоги та цілі, що служать певною основою. У Категоріях та Підкатегоріях вимоги ще більше деталізуються і надається детальний опис вимог та очікуваних результатів.

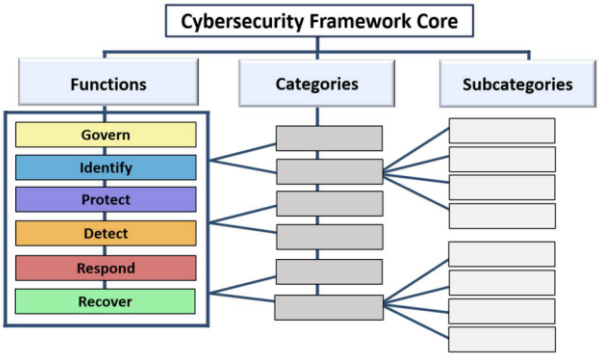


Рис.1. Структура CSF Core

Важливо відзначити, що CSF Core не визначає вимоги або методи досягнення визначених результатів. Замість цього, він надає основну структуру та загальні цілі, які організації можуть використовувати в рамках своїх конкретних потреб.

CSF Core виступає як основний компонент фреймворку, надаючи конкретні орієнтири для управління кібербезпекою, які можуть бути адаптовані та застосовані організаціями будь-якого розміру та сфери діяльності.

CSF Core включає шість функцій: Управління (Govern), Визначення (Identify), Захист (Protect), Виявлення (Detect), Реагування (Respond), та Відновлення (Recover). Кожна з цих функцій має свої унікальні завдання та цілі:

1. Управління (Govern) – визначає стратегію, очікування та політику організації щодо кібербезпеки. це основа для визначення пріоритетів у розробці стратегії та вибору заходів в інших функціях;
2. Визначення (Identify) – зосереджена на розумінні поточних ризиків кібербезпеки та активів організації, включаючи дані, апаратне забезпечення, програмне забезпечення та інші складові;
3. Захист (Protect) – забезпечує використання заходів для управління ризиками кібербезпеки, включаючи ідентифікацію, аутентифікацію, контроль доступу, навчання та тренування персоналу та збереження інфраструктури;
4. Виявлення (Detect) – спрямована на виявлення можливих кібератак та компрометацій, забезпечуючи аналіз аномалій та подій;
5. Реагування (Respond) – визначає дії, які слід вжити при виявленні кіберінциденту, зокрема управління інцидентами, їх аналіз та мінімізація;
6. Відновлення (Recover) – функція, яка відповідає за відновлення активів та операцій, які постраждали від кіберінциденту, забезпечуючи швидке відновлення звичайної діяльності.

Функції CSF Core зображені у вигляді кола, що ілюструє глибокий взаємозв'язок між ними (рис. 2).

Рис.2. Функції CSF Core

В центрі цього кола розташована функція Управління (Govern), яка представляє стратегію управління ризиками кібербезпеки та встановлення політики. Функція Управління визначає, як організація буде реалізовувати інші п'ять функцій: Визначення, Захист, Виявлення, Реагування, Відновлення.

Це коло ілюструє, що управління кіберризиками – це комплексний та взаємодіючий процес. Кожна функція має свою важливу роль у підготовці, захисті, виявленні, реагуванні та відновленні. Взаємодія між ними формує єдиний стратегічний підхід, де Управління (Govern), як центральний елемент, визначає шлях для імплементації інших п'ятьох функцій. Такий підхід допомагає забезпечити більш ефективне та цілісне управління кіберризиками в організації.

Організаційні профілі (CSF Organizational Profiles) – це другий компонент фреймворку. Ці профілі є механізмом для опису поточного (Current Profile) та/або бажаного (Target Profile) стану кібербезпеки організації (з використанням результатів, визначених у CSF Core) [4]:

1. Поточний Профіль (Current Profile). Цей профіль вказує на те, які результати в реалізації NIST CSF 2.0 організація вже досягла або намагається досягти, і яким чином це відбувається. Він характеризує поточний стан кібербезпеки організації і дозволяє зрозуміти, наскільки вона виконує цільові вимоги фреймворку;
2. Цільовий Профіль (Target Profile): Цей профіль визначає бажані результати, які організація вибрала та пріоритизувала для досягнення своїх стратегічних цілей з управління кібербезпекою. Цільовий Профіль враховує майбутні зміни в кібербезпеці, такі як нові вимоги, впровадження нових технологій та тренди в області інформаційної безпеки.

Організаційні Профілі допомагають організаціям зрозуміти свою поточну кібербезпекову ситуацію, визначити стратегічні цілі та пріоритети, і комунікувати їхні плани та досягнення зацікавленим сторонам.

Організації можуть використовувати ці профілі для внутрішньої комунікації, зовнішньої звітності та встановлення вимог до постачальників та партнерів щодо кібербезпеки. Третім компонентом NIST CSF 2.0 є Рівні безпеки (CSF Tiers). Рівні безпеки визначають рівень зрілості організації у сфері управління кіберризиками. Ці рівні допомагають оцінити, наскільки системно та ефективно впроваджені заходи безпеки в організації.

CSF Tiers включають чотири рівні, а саме: Частковий (Partial) (Tier 1), Інформований (Risk Informed) (Tier 2), Системний (Repeatable) (Tier 3) та Адаптивний (Adaptive) (Tier 4):

1. Частковий (Partial) (Tier 1) – на цьому рівні організація має обмежену системність та частковий підхід до управління кіберризиками та впровадження заходів безпеки;
2. Інформований (Risk Informed) (Tier 2) – на цьому рівні організація визнає важливість управління ризиками та встановлює процеси для регулярного оцінювання та вдосконалення своїх заходів безпеки;
3. Системний (Repeatable) (Tier 3) – на цьому рівні організація вже визначила та систематизувала свої процеси управління кіберризиками. Вона систематично застосовує свої підходи та методології до кібербезпеки;
4. Адаптивний (Adaptive) (Tier 4) – найвищий рівень відрізняється гнучким та адаптивним підходом до управління ризиками. Організації на цьому рівні постійно вдосконалюють свої підходи, враховуючи ландшафт загроз та технологічні інновації, що змінюються.

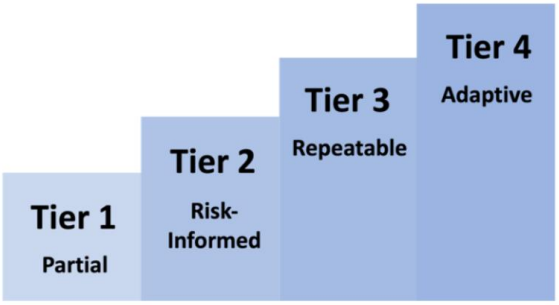


Рис.3 – Рівні безпеки NIST CSF 2.0

CSF Tiers надають організаціям рамки, щоб визначити рівень зрілості організації в управлінні кіберризиками. Чим вище рівень, тим більш високий рівень готовності та управління кіберризиками. Залежно від рівня, організації можуть приймати відповідні стратегії для поліпшення ефективності своїх заходів з кібербезпеки.

Необхідно підкреслити, що NIST CSF 2.0 надає не тільки сам фреймворк, але й додаткові ресурси, такі як Швидкі стартові посібники (Quick Start Guides), Інформаційні посилання (Informative References) та Приклади реалізації (Implementation Examples):

1. Швидкі стартові посібники (Quick Start Guides). Ці матеріали розширюють загальні концепції CSF та надають практичні рекомендації для ефективного використання фреймворку в реальних умовах;
2. Інформаційні посилання (Informative References). Посилання дозволяють організаціям визначити, які документи та ресурси можна використовувати для подальшого удосконалення своєї кібербезпекової стратегії [5];

3. Приклади реалізації (Implementation Examples). Ці приклади демонструють реальні сценарії використання CSF та надають інформацію про те, як інші організації вже успішно впроваджують фреймворк у свою практику.

Отже, ці додаткові ресурси допомагають організаціям краще розуміти, приймати та реалізувати фреймворк в їхніх кібербезпекових стратегіях та практиках.

Висновок. Основною перевагою NIST CSF 2.0 є універсальність і гнучкість. Цей інструмент створений для всіх видів організацій, незалежно від розміру, галузі та потреб, а також рівня зрілості кібербезпеки організації. Запровадження кібербезпекових заходів можливі як для організацій, що тільки починають розглядати свої кібербезпекові виклики, так і для тих, які вже мають велику та розвинену кібербезпекову команду.

Фреймворк не є прескриптивним, що надає можливість адаптації до конкретних потреб та ризиків кожної організації. Також NIST CSF 2.0 сприяє інтеграції з іншими настановами та стандартами з кібербезпеки, що надає можливість користувачам розширювати та зміцнювати свої практики в сфері захисту.

NIST CSF 2.0 можна використати для розроблення методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури, таким чином актуалізувавши існуючі методичні рекомендації, що затвердженні наказом Адміністрації Держспецзв'язку від 6 червня 2021 року №601. Запропоновані зміни позитивно вплинуть на рівень кіберзахисту об'єктів критичної інфраструктури і їх стійкість перед кібератаками.

Таким чином, NIST CSF 2.0 є важливим кроком у напрямку управління кібербезпекою для різноманітних організацій, зокрема і об'єктів критичної інфраструктури.

Список літератури

[1]. NIST Releases Version 2.0 of Landmark Cybersecurity Framework [Електронний ресурс]. Режим доступу до ресурсу: https://www.nist.gov/news-events/news/ 2024 / 02 / nist-releases-version-20-landmark-cybersecurity-framework.

[2]. The NIST Cybersecurity Framework (CSF) [Електронний ресурс]. Режим доступу до ресурсу: https: // nvlpubs.nist.gov / nistpubs / CSWP / NIST. CSWP. 29.pdf.

[3]. CSF 2.0 Quick Start Guides [Електронний ресурс]. Режим доступу до ресурсу: https://www.nist.gov/quick-start-guides.

[4]. CSF 2.0 Organizational Profiles [Електронний ресурс]. Режим доступу до ресурсу: https://nist.gov/profiles-0.

[5]. CSF 2.0 Informative References [Електронний ресурс]. Режим доступу до ресурсу: https://www.nist.gov/informative-references.

УДК 004.056

Zhylin A., Beliavsky V. Bakalynsky O. NIST CSF 2.0: New Cybersecurity Framework from the National Institute of Standards and Technology of the United States

Abstract. *This article provides an in-depth analysis of the Cybersecurity Framework version 2.0, introduced by the National Institute of Standards and Technology (NIST) in early 2024. CSF 2.0 is designed to facilitate effective management and mitigation of cybersecurity risks for diverse organizations, regardless of their size and industry. The article explores key components of the framework, such as the Core (CSF Core), Organizational Profiles (CSF Organizational Profiles), Security Tiers (CSF Tiers), and provides insights into their utilization for enhancing organizational cybersecurity practices. Emphasis is placed on the flexibility of the framework, allowing organizations to adapt their approaches to cybersecurity management according to their unique risks and needs. CSF 2.0 is considered a crucial tool aimed at promoting cybersecurity improvement across all organizational levels, irrespective of their technical maturity. The article also offers a comprehensive overview of the potential uses of CSF resources for enhancing cybersecurity practices and underscores the importance of continuously refining cybersecurity management strategies to effectively counter growing cyber threats.*

Keywords: *CSF 2.0, cybersecurity, NIST, organizational profiles, framework, cyber threats, information security.*

Жилін Артем Вікторович, к.т.н., доцент, професор кафедри кібербезпеки і застосування інформаційних систем і технологій ІСЗЗІ КПІ ім. Ігоря Сікорського.

Artem Zhylin, candidate of technical sciences, associate professor, professor at the cybersecurity and application of information systems and technology academic department, Institute of special communication and information protection of National technical university of Ukraine «Igor Sikorsky Kyiv polytechnic institute».

Бєлявський Владислав Олександрович, PhD, старший офіцер Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України.

Vladyslav Beliavsky, Ph.D., Senior Officer, The State Cyber Protection Centre.

Бакалинський Олександр Олегович, к.т.н., старший дослідник, заступник директора Департаменту кіберзахисту Адміністрації Державної служби спеціального зв'язку та захисту інформації України.

Oleksandr Bakalynsky, Candidate of Technical Sciences, Senior researcher, Deputy Director of the Department of Cyber Defense of the Administration of the State Service for Special Communications and Information Protection of Ukraine

Отримано *14 лютого 2024 року*, затверджено редколегією *1 квітня 2024 року*