УДК 342:351.746

В. О. Савкун

Л. О. Майданевич

ПРОЦЕСИ ІМПЛЕМЕНТАЦІЇ РАМКОВОЇ ПРОГРАМИ NIST CSF 2.0 У ПРАВОВЕ ПОЛЕ УКРАЇНИ

Вінницький національний технічний університет

Анотація

В доповіді розглянуто процеси імплементації рамкової програми NIST CSF 2.0 у правове поле України та її значення для розвитку національної системи кібербезпеки. Розглянуто основні компоненти фреймворку, нормативні зміни та впровадження ризик-орієнтованого підходу до управління кіберризиками. Визначено роль NIST CSF 2.0 у підвищенні кіберстійкості державних органів і суб'єктів критичної інфраструктури.

Ключові слова: інформаційна безпека, кібербезпека, NIST CSF 2.0, імплементація стандартів, правове регулювання, законодавство України.

Abstract

The report examines the implementation processes of the NIST CSF 2.0 framework programme in the legal field of Ukraine and its significance for the development of the national cybersecurity system. The main components of the framework, regulatory changes and the implementation of a risk-based approach to cyber risk management are considered. The role of NIST CSF 2.0 in improving the cyber resilience of government agencies and critical infrastructure entities is identified.

Keywords: *Information security, cybersecurity, NIST CSF 2.0, implementation of standards, legal regulation, legislation of Ukraine.*

Вступ

У сучасних геополітичних умовах, що характеризуються станом повномасштабної конвенційної та кібернетичної війни, захист критичної інфраструктури та державних інформаційних ресурсів стає фундаментальним елементом національної стійкості України. Світ загроз демонструє стрімку динаміку: щорічні збитки від кіберзлочинності в усьому світі вимірюються трильйонами доларів, а розвиток технологічного штучного інтелекту та автоматизації процесів дозволяє зловмисникам створювати дедалі складніші вектори атак [1]. Для ефективної протидії таким атакам, державні інституції та суб'єкти господарювання змушені відмовлятися від статичних моделей захисту на користь динамічних систем управління ризиками. Одним із найбільш авторитетних світових стандартів у цій сфері є програма NIST (National Institute of Standarts and Technology) CSF (Cybersecurity Framework), розроблена Національним інститутом стандартів та технологій США. Вихід у лютому 2024 року оновленої версії NIST CSF 2.0 запровадив нову еру в управлінні кібербезпекою, пропонуючи розширений фокус на стратегічному управлінні [2].

Імплементація NIST CSF 2.0 у правове поле України є не лише технічним завданням, а стратегічним кроком до покращення національного законодавства з міжнародними стандартами безпеки. Традиційні підходи, що базувалися на жорстких вимогах до побудови КСЗІ (Комплексних систем захисту інформації), часто виявлялися малоефективними для малих та середніх організацій через високу вартість та нестачу кваліфікованих кадрів. Також вони не забезпечували необхідної адаптивності до нових типів атак [2].

Проблема імплементації полягає у необхідності реалізації принципів фреймворку в межах специфічної національної моделі кіберзахисту, враховуючи при цьому обмеженість ресурсів та потребу в безперервності критичних процесів. Наказ Адміністрації Держспецзв'язку №54 від 30.01.2025 заклав фундамент для наближення українських стандартів до міжнародних. Також

прийняття наказу №75 від 30.01.2026 та оновлення постанов Кабінету Міністрів України №1470 та №1531 продемонстрували прагнення держави до впровадження ризик-орієнтованої моделі [3].

Завданням даного дослідження є комплексний аналіз процесів імплементації NIST CSF 2.0 в Україні, вивчення структури оновленого законодавства, оцінка механізмів управління ризиками та визначення практичних результатів впровадження нових нормативних вимог для суб'єктів критичної інфраструктури та державного сектору.

Результати дослідження

Для розуміння реформи в Україні необхідно розглянути архітектуру самого NIST CSF 2.0. Ця програма є добровільним керівництвом, яке надає спільну мову та систематизований підхід до управління кіберризиками. Вона розроблена таким чином, щоб бути нейтральною до технологій, секторів та країн, що робить її універсальним інструментом для будь-якої організації. Архітектура CSF 2.0 складається з трьох компонентів: Ядра, Організаційних профілів, та Рівнів [2]. Ядро є фундаментом фреймворку і уособлює собою ієрархію функцій, категорій та підкатегорій, що описують бажані результати кібербезпеки. У версії 2.0 було введено шосту функцію Govern (Управління), яка тепер стоїть в основі всієї цієї системи. Також окрім функції Govern є ще такі функції, як ідентифікація. Ціль ідентифікації полягає в фокусуванні на розумінні активів, вразливостей, загроз та контексту ризиків для організації. Функція захисту спрямована на впровадження засобів контролю для запобігання або обмеження негативного впливу інцидентів. Виявлення передбачає розробку та впровадження активностей для своєчасного виявлення подій кібербезпеки. Реагування описує дії, які необхідно вчинити у разі виявлення інциденту для мінімізації його наслідків. Та відновлення визначає плани та заходи для повернення систем та сервісів у робочий стан після атаки [2]. Організаційні профілі дозволяють організаціям порівнювати свій поточний стан кібербезпеки із бажаним. Такий підхід створює механізм для виявлення прогалин та пріоретизації інвестицій у заходи захисту. Рівні описують ступінь зрілості процесів управління ризиками від часткового до адаптивного, що дозволяє оцінювати не лише наявність технічних збоїв, а й якість управлінських процесів.

Процеси імплементації NIST CSF 2.0 в Україні характеризуються швидкою адаптацією законодавства. Першим значним кроком стало видання Наказу Адміністрації Держспецзв'язку №54 від 30.01.2025, яким були затверджені базові заходи з кіберзахисту та відповідні методичні рекомендації [3]. Цей наказ став офіційним стартом використання фреймворку у національній практиці. Проте динаміка загроз та необхідність більш чіткої регуляції призвели до того, що 30.01.2026, був виданий наказ №75, який скасував наказ №54 та запровадив більш досконалий каталог заходів з кіберзахисту [4].

Наказ №75 від 30.01.2026 запровадив «Каталог заходів з кіберзахисту», який став єдиним переліком організаційних та технічних дій, структурованих за шістьма функціями NIST CSF 2.0. Це дозволяє уникнути розбіжностей у тлумаченні вимог різними регуляторами. Каталог включає заходи спрямовані на стратегічне управління відповідною функцією та оперативне реагування на інциденти, після яких йде відновлення. Важливою рисою Каталогу є його диференційованість. Базові заходи спрямовані на категорії критичності об'єктів об'єктів критичної інфраструктури, типу систем, в яких обробляються державні інформаційні ресурси та вимог захисту інформації з обмеженим доступом. Це забезпечує масштабованість: малі організації можуть виконувати спрощений набір базових заходів, тоді як великі оператори ОКІІ зобов'язані доповнювати свій профіль більш складними заходами з Каталогу відповідно до результатів управління ризиками. Наказ також затвердив форму «Плану кіберзахисту», яка є обов'язковим документом для фіксації прогресу організації на шляху до цільового стану [3].

NIST CSF 2.0 є оптимальним інструментом для України через свою адаптивність та універсальність. Саме в умовах хронічного дефіциту кадрів та фінансування, цей фреймворк дозволяє організаціям створювати ефективні політики без необхідності миттєвого впровадження дороговартісних рішень. Значущість фреймворка полягає у можливості застосування для виявлення вразливостей та побудови стійких систем, здатних витримувати атаки та протидіяти зловживанням технологіям штучного інтелекту [1].

Однак процес імплементації також стикається з низками викликів. По-перше, це потреба у зміні менталітету керівників організацій. Оскільки функція Управління тепер є центральною, на відміну від версії 1.0, кібербезпека перестає бути виключно зоною відповідальності ІТ-відділів. Ради директорів установи мають бути безпосередньо залучені до процесу управління ризиками. На середніх та малих підприємствах, які не мають своїх підрозділів кібербезпеки, критично важливим є розвиток кадрового потенціалу та наявність спрощених методичних рекомендацій, які Україна почала видавати у наказі №75 [1]

Висновки

Імплементація NIST CSF 2.0 у правове поле України протягом 2025-2026 років стала фундаментальним рішенням у стратегії національного кіберзахисту. Відмова від застарілих статичних моделей на користь ризик-орієнтованого підходу дозволяє державі та бізнесу більш гнучко реагувати на складні загрози сучасності, зокрема в умовах повномасштабної війни. Затвердження наказу Держспецзв'язку №75 завершив процес створення цілісної регуляторної бази, яка поєднує українські вимоги з найкращими світовими практиками [4]. Ключовим результатом є впровадження шести функцій кібербезпеки – Управління, Ідентифікація, Захист, Виявлення, Реагування та Відновлення. Запровадження концепції організаційних профілів та рівнів зрілості управління ризиками надає організаціям чітку карту розвитку. Це дозволяє здійснювати інвестиції в кібербезпеку осмислено, базуючись на реальних загрозах, а не на формальних переліках вимог. Створення єдиного каталогу заходів з кіберзахисту забезпечило суб'єктів практичним інструментарієм для самостійної оцінки та планування захисту. Незважаючи на значний прогрес, подальший успіх імплементації залежатиме від якості кадрового забезпечення та готовності керівництва організацій брати на себе відповідальність за управління кіберризиками. Розвиток кадрового потенціалу, впровадження спрощених інструментів для малих організацій та постійна адаптація методичних рекомендацій до нових технологічних викликів мають стати наступними кроками держави. Загалом, імплементація NIST CSF 2.0 значно підвищує кіберстійкість України та закладає надійний фундамент для захисту її цифрового суверенітету в довгостроковій перспективі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Іваночко Т. А., Семенюк С. А. Управління ризиками кібербезпеки з використанням NIST CSF 2.0. *Сучасний захист інформації.* 2025. № 3(63). С. 75–82. URL: https://journals.duikt.edu.ua/index.php/dataprotect/article/view/3306/3190 (дата звернення: 24.02.2026).
2. National Institute of Standards and Technology (NIST). The NIST Cybersecurity Framework (CSF) 2.0: NIST CSWP 29. Feb. 26, 2024. 32 с. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (дата звернення: 24.02.2026).
3. Україна впроваджує найкращі світові практики у сфері кібербезпеки та впроваджує норми NIST Cybersecurity Framework 2.0. 30.01.2025. URL: https://cybersec.net.ua/normatyvni-dokumenty/793-ukraina-vprovadzhuie-naikrashchi-svitovi-praktyky-u-sferi-kiberbezpeky-ta-vprovadzhuie-normy-nist-cybersecurity-framework-20.html (дата звернення: 24.02.2026).
4. Про затвердження Каталогу заходів з кіберзахисту, базових заходів з кіберзахисту, форми плану кіберзахисту та методичних рекомендацій щодо здійснення заходів з кіберзахисту : Наказ Адміністрації Держспецзв'язку № 75 від 30.01.2026. URL: https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-30-01-2026-75-pro-zatverdzhennya-katalogu-zakhodiv-z-kiberzakhistu-bazovikh-zakhodiv-z-kiberzakhistu-formi-planu-kiberzakhistu-ta-metodichnikh-rekomendacii-shodo-zdiisnennya-zakhodiv-z-kiberzakhistu (дата звернення: 24.02.2026).

Савкун Валентин Олександрович − студент групи 2БС-23б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, email: valiksavkun298@gmail.com.

Майданевич Леонід Олександрович – канд. філос. наук, доцент кафедри захисту інформації факультету інформаційних технологій та комп'ютерної інженерії Вінницького національного технічного університету, адвокат (Рада адвокатів Вінницької області), м. Вінниця, email: lmaidanevych@gmail.com

Savkun Valentyn O. − student of group 2BS - 23B, Faculty of Information Technologies of Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email : valiksavkun298@gmail.com.

Maidanevych Leonid – PhD in Philosophical Sciences, Associated Professor, Department of Information Security, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Lawyer, Vinnytsia Bar Council, Vinnytsia, e-mail: lmaidanevych@gmail.com.