УДК 004.056.5

ПОРІВНЯЛЬНА ОЦІНКА СИСТЕМ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ В СПОЛУЧЕНИХ ШТАТАХ АМЕРИКИ

Олександр Пелюх[1], Марина Єсіна[1,2], Дмитро Голубничий[2]

[1]Харківський національний університет імені В.Н. Каразіна, майдан Свободи, 4, Харків, 61022, Україна
oleksandrpelyukh@gmail.com, m.v.yesina@karazin.ua
[2]АТ «ІІТ», вулиця Коломенська, 15, Харків, 61166, Україна
goldim1971@gmail.com

Надійшла: жовтень 2023. Прийнята: листопад 2023.

Анотація: *В умовах сучасного світу кіберзагрози стають серйозною проблемою для компаній у всіх професійних галузях. Для всіх організацій незалежно від сфери діяльності, кіберзагрози в сучасному світі є, безперечно, вагомим викликом. Безсумнівно, сучасні організації повинні ставити перед собою завдання ефективної протидії кіберзагрозам незалежно від їхньої професійної галузі. Задля ефективного протистояння цим загрозам, організації повинні мати ефективні системи з реагування на інциденти, зокрема у кіберпросторі. У США існує безліч фреймворків з реагування на інциденти, кожен з яких має свої переваги та недоліки. Ця стаття пропонує порівняльний аналіз чотирьох провідних фреймворків з реагування на кіберінциденти в США: NIST Cybersecurity Framework (CSF), CISA Cyber Incident Response Guide, ISO/IEC 27001 та NIST Special Publication 800-61. Мета дослідження полягає в тому, щоб надати організаціям огляд чотирьох провідних фреймворків реагування на інциденти в США, аби вони могли обрати найбільш відповідний фреймворк для власних конкретних потреб. Задля проведення дослідження було використано якісний підхід, що складався з ретельного вивчення офіційних документів, перегляду релевантної сучасної літератури та консультування із фахівцями з кібербезпеки. Ця стаття є додатковим інформаційним ресурсом для організацій і компаній, які шукають дієвий та оптимальний метод реагування на інциденти, включаючи кіберпростір. Вона надає огляд чотирьох провідних фреймворків в США, що дозволяє організаціям порівняти їх переваги й недоліки, та у результаті обрати найбільш відповідний фреймворк для своїх чітких цілей.*

Ключові слова: *реагування на кіберінциденти, NIST CSF, CISA, ISO/IEC 27001, NIST SP 800-61, управління ризиками, системи безпеки.*

1. Вступ

У сучасному світі кіберзагрози є серйозною проблемою для всіх організацій, незалежно від їхньої галузі. Згідно з оцінкою *Cybersecurity Ventures*, у 2023 році глобальні щорічні витрати на кіберзлочинність сягнуть 8 трильйонів доларів США. Крім того, очікується зростання вартості збитків від кіберзлочинів, обсяг яких до 2025 року сягне 10,5 трильйонів доларів США [1]. Ця тенденція продовжуватиме зростати в міру того, як кіберзлочинці будуть розробляти все більш складні методи атак.

Щоб ефективно протистояти цим загрозам, організації повинні мати ефективні системи реагування на інциденти, зокрема у кіберпросторі. Система реагування на інциденти – це комплекс заходів, спрямованих на виявлення, реагування та усунення кіберінцидентів. Вона включає в себе наступні компоненти [2]:

- детектування – виявлення ознак кіберінциденту;
- локалізація – реагування на кіберінцидент у спосіб, що мінімізує його вплив;
- ліквідація – усунення наслідків кіберінциденту;
- відновлення – прийняття заходів для виключення повторної ймовірності виникнення кіберінциденту.

У США існує безліч фреймворків реагування на інциденти, кожен з яких має свої переваги та недоліки. Ця стаття пропонує порівняльний аналіз чотирьох провідних фреймворків реагування на інциденти в США [3-6]:

- NIST Cybersecurity Framework (CSF);

- CISA Cyber Incident Response Guide;
- ISO/IEC 27001;
- NIST Special Publication 800-61.

Мета дослідження полягає в тому, щоб надати організаціям огляд чотирьох провідних фреймворків реагування на інциденти в США, щоб вони могли обрати найбільш відповідне джерело для своїх конкретних потреб.

2. Огляд основних аспектів фреймворків

Задля проведення всебічної оцінки, необхідно ознайомитися з кожним із фреймворків більш детально й визначити їх основні аспекти.

- NIST Cybersecurity Framework (CSF)

NIST – Національний інститут стандартів і технологій при Міністерстві торгівлі США. Така концепція кібербезпеки NIST допомагає компаніям будь-якого розміру краще розуміти, управляти та зменшувати ризики кібербезпеки, а також захищати свої мережі та дані. Вона надає компанії перелік найкращих практик, які допоможуть визначити, на чому зосередити свій час і гроші для захисту кібербезпеки.

NIST CSF може бути застосована у роботі підприємства в наступних п'яти напрямках: ідентифікація, захист, виявлення, реагування та відновлення. Вона базується на загальновідомих стандартах і практиках та представляє найкращі сучасні підходи у сфері кібербезпеки [3,7]. Однак кожна організація і галузь повинні будуть визначити свої особливі теми і питання, на які слід звернути увагу. Проте більшість тем є спільними для всіх секторів.

Концепція визначає рівні, які описують міру, до якої впроваджуються вимоги (табл. 1). Ці категорії іноді називають рівнями зрілості, але, згідно з NIST, вони є скоріше інструментом для внутрішньої комунікації між управлінням ризиками кібербезпеки та управлінням операційними ризиками, і не повинні розглядатися як рівні зрілості. Проте, вищі рівні представляють вищий ступінь досконалості та зрілості в управлінні ризиками кібербезпеки та реагування на них [7].

Таблиця 1 – Рівні «зрілості» у *NIST Cybersecurity Framework*
Table 1 – «Maturity» levels in *NIST Cybersecurity Framework*

Рівень	Назва	Пояснення
1	Частковий	Неформальні практики; обмежена обізнаність; відсутність координації у сфері кібербезпеки
2	З урахуванням ризиків	Затверджені процеси та визначені пріоритети, але не впроваджені в масштабах всієї організації; існує високий рівень обізнаності, надані адекватні ресурси; неформальний обмін інформацією та координація дій.
3	Постійно оновлюваний	Офіційна політика визначає процеси управління ризиками з регулярним переглядом та оновленням; загально організаційний підхід до управління ризиками кібербезпеки з впровадженими процесами; регулярна формалізована координація.
4	Адаптивний	Практики активно адаптуються на основі отриманих уроків та прогнозних показників; кібербезпека впроваджена і є частиною культури всієї організації; активне управління ризиками та обмін інформацією.

Загалом, процес впровадження рамкової концепції від NIST можна звести до вигляду у форматі спрощеного циклу дій (рис. 1).

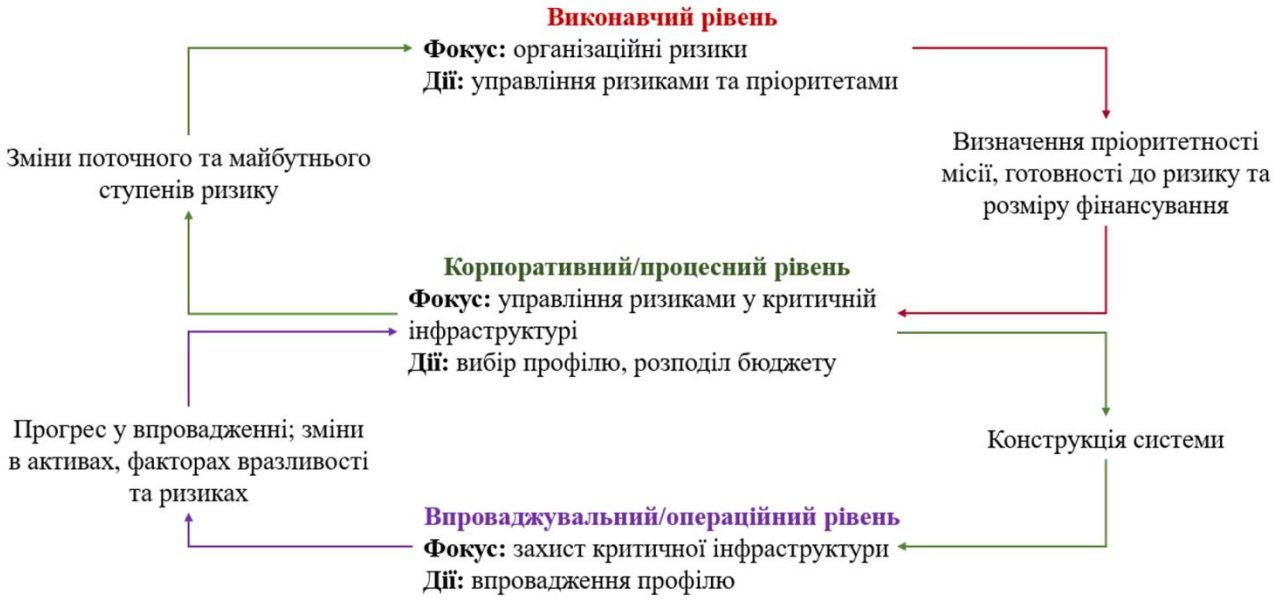

Рис. 1 – Схема впровадження «*NIST Cybersecurity Framework*»
Fig. 1 – «*NIST Cybersecurity Framework*» implementation scheme

- CISA Cyber Incident Response Guide

У 2021 році Агентство з кібербезпеки та безпеки інфраструктури (*CISA*) опублікувало документ з двома окремими інструкціями, спеціально призначеними для інцидентів та вразливостей. Інструкція щодо інцидентів дуже схожа на систему реагування NIST, але розбиває процес на менші частини. Інструкції щодо вразливостей також дуже схожі, але переосмислені, щоб зосередитися на проблемах, які ще не призвели до інцидентів.

Документ містить комбінацію інструментів і програмного забезпечення (ПЗ) з відкритим кодом, послуг, що пропонуються державними та приватними організаціями з кібербезпеки, а також ресурсів, які безкоштовно надає саме *CISA* [5].

Агентство спочатку рекомендує компаніям вжити базових заходів для підвищення рівня власної безпеки, включаючи впровадження циклів виправлень для усунення відомих вразливостей ПЗ, впровадження двофакторної або багатофакторної автентифікації (*2FA/MFA*), оновлення застарілого та/чи непідтримуваного ПЗ, а також оновлення стандартних або «старих» паролів. Після виконання вищезазначених кроків *CISA* рекомендує організаціям ознайомитися з додатковими категоріями.

Серед ресурсів є посилання на служби оцінки фішингу, віддалені тести на проникнення, розподілений захист від атак типу «відмова в обслуговуванні» (*DDoS*), *Project Shield*, сховища даних про загрози, антивірусні інструменти, ПЗ для аудиту випадків та служби резервного копіювання. Слід зазначити, що передбачені різні рівні кваліфікації для кожного сервісу або інструменту, які розділені на базові та більш професійні. Список CISA буде постійно оновлюватися,тому в майбутньому агентство має намір створити процес для організацій, які зможуть подавати безкоштовні інструменти та послуги на їх розгляд.

- ISO/IEC 27001

ISO/IEC 27001 – це міжнародний стандарт інформаційної безпеки (ІБ). Він встановлює специфікацію для ефективної СУІБ (*системи управління інформаційною безпекою*). Підхід ISO 27001, заснований на найкращих практиках, допомагає організаціям управляти своєю інформаційною безпекою, звертаючи увагу на людей, процеси та технології [6].

Сертифікація за стандартом ISO 27001 визнана в усьому світі і свідчить про відповідність СУІБ найкращим практикам у сфері інформаційної безпеки. Рішення про сертифікацію

приймається акредитованим органом сертифікації після успішного аудиту СУІБ організації. Стандарт ISO 27001, який є частиною серії ISO 27000, встановлює основу для створення, впровадження, функціонування, моніторингу, аналізу, підтримки та постійного вдосконалення СУІБ в організаціях.

Згідно із визначенням ISO 27001, основною метою СУІБ є захист трьох аспектів інформації [6, 8]:

- конфіденційність: тільки уповноважені особи мають право доступу до інформації;
- цілісність: тільки уповноважені особи можуть змінювати інформацію;
- доступність: інформація має бути доступною для уповноважених осіб у будь-який час, коли вона їм потрібна.

Це досягається шляхом з'ясування того, які потенційні інциденти можуть статися з інформацією (тобто, оцінки ризиків), а потім визначення того, що необхідно зробити, щоб запобігти таким інцидентам (*тобто, зменшення ризиків або їх обробки*). Таким чином, основна концепція ISO 27001 ґрунтується на процесі управління ризиками: з'ясуванні, де знаходяться ризики, а потім систематичної обробки їх шляхом впровадження засобів контролю безпеки.

- NIST Special Publication 800-61

NIST SP 800-61 – це документ, який містить керівні принципи та найкращі методи роботи з інцидентами. Він охоплює весь життєвий цикл реагування на інциденти, від підготовки та виявлення до дій після інциденту та узагальнення отриманих уроків. Він також містить рекомендації щодо політик, процедур, ролей та обов'язків, а також інструментів і методів аналізу для пом'якшення наслідків інцидентів. Стандарт ґрунтується на принципах гнучкості, масштабованості, координації та комунікації [4].

Варто зауважити, що NIST SP 800-61 надає ключові рекомендації для боротьби з кіберінцидентами (табл. 2), зокрема деталізовану схему координування дій під час інциденту ІБ.

Таблиця 2 – Ключові рекомендації *NIST Special Publication 800-61*

Table 2 – The main recommendations *NIST SP 800-61*

Рекомендація	**Пояснення**
Плануйте координацію інцидентів із зовнішніми сторонами до їх виникнення	Зовнішні сторони, такі як групи реагування на інциденти, правоохоронні органи та Інтернет провайдери, відіграють вирішальну роль у скоординованому плануванні для забезпечення ефективної комунікації та чітких обов'язків.
Проконсультуйтеся з юридичним відділом, перш ніж розпочинати будь-які зусилля з координації	Можуть існувати контракти або інші домовленості, які необхідно укласти до початку обговорення.
Здійснюйте обмін інформацією про інцидент протягом усього життєвого циклу реагування на інцидент	Обмін інформацією є життєво важливим для координації між організаціями. Не варто відкладати обмін деталями інциденту до його повного вирішення.
Намагайтеся автоматизувати якомога більшу частину процесу обміну інформацією	Ефективна міжорганізаційна координація є економічно вигідною. Слід прагнути до балансу між автоматизованим обміном інформацією та процесами управління потоками, орієнтованими на людину.
Збалансуйте переваги обміну інформацією з недоліками обміну конфіденційною інформацією	Тільки важлива інформація має бути надана потрібним сторонам. Деталі впливу на бізнес у командах, технічна інформація в цілому та зосередження на технічних деталях з організаціями-партнерами.
Діліться якомога більшою кількістю відповідної інформації про інцидент з іншими організаціями	Організації повинні вирішити, якою технічною інформацією ділитися. Зовнішні показники, такі як характеристики атак, зазвичай безпечні, але деталі використаних вразливостей можуть бути приховані з міркувань безпеки та відповідальності.

У цілому, чотири розглянуті фреймворки пропонують широкий спектр рекомендацій, які можуть допомогти організаціям розробити ефективну систему реагування на інциденти.

3. Порівняльний аналіз розглянутих документів

У цьому розділі ми проведемо детальний порівняльний аналіз чотирьох розглянутих фреймворків реагування на інциденти. Розглянемо наступні аспекти:

- Цільова аудиторія

NIST CSF та NIST Special Publication 800-61 призначені для широкого загалу організацій, незалежно від їхнього розміру, галузі або рівня кібербезпеки. CISA *Cyber Incident Response Guide* призначений для організацій, які підпадають під юрисдикцію CISA. ISO/IEC 27001 призначений для організацій, які хочуть отримати сертифікацію за цим стандартом.

- Сфера застосування

NIST CSF та NIST *Special Publication 800-61* мають широку сферу застосування, яка включає в себе всі аспекти реагування на інциденти. Порівняно з ним CISA *Cyber Incident Response Guide* має більш вузьку сферу застосування, яка фокусується на практичних аспектах реагування на інциденти. А сфера застосування ISO/IEC 27001 в більшої мірі сконцентрована на управлінні ризиками та запобіганні інцидентів безпеки.

- Рівень деталізації

NIST CSF та NIST Special Publication 800-61 є високорівневими фреймворками, які пропонують загальні рекомендації щодо реагування на інциденти. CISA *Cyber Incident Response Guide* є більш детальним фреймворком, який пропонує конкретні кроки та процедури для реагування на інциденти. ISO/IEC 27001 є найдетальнішим з розглянутих документів, що пропонує детальні вимоги та рекомендації, щодо управління ризиками та запобігання інцидентам ІБ.

- Переваги та недоліки

Кожен з розглянутих фреймворків має свої сильні та слабкі сторони. NIST CSF є хорошим вибором для організацій, які шукають гнучкий і адаптивний фреймворк, який охоплює весь цикл реагування на інциденти. ISO/IEC 27001 є хорошим вибором для компаній, які шукають всеосяжну і визнану міжнародну систему управління інформаційною безпекою. CISA *Cyber Incident Response Guide* є доволі прийнятним вибором для організацій, які шукають практичні і конкретні рекомендації щодо реагування на інциденти. NIST *Special Publication 800-61* є хорошим вибором для компаній і структур, які шукають докладні і всеосяжні рекомендації щодо виявлення та реагування на інциденти. Узагальнені переваги та недоліки розглянутих документів наведені у табл. 3.

Таблиця 3 – Переваги та недоліки розглянутих документів

Table 3 – Advantages and disadvantages of the documents under consideration

Документ	Переваги	Недоліки
NIST Cybersecurity Framework	Гнучкість, індивідуалізація	Недостатня деталізація процесів
CISA Cyber Incident Response Guide	Практичні рекомендації, вільний доступ	Менш комплексний, ніж інші розглянуті фреймворки
ISO/IEC 27001	Встановлений стандарт, спрямованість на управління ризиками	Не є спеціалізованим для реагування на інциденти
NIST Special Publication 800-61	Є конкретні рекомендації і методи з реагування на інциденти	Можлива складність розуміння та реалізації деяких з процесів

Таким чином, можна стверджувати, що кожен із розглянутих фреймворків може бути корисним для організацій, які шукають ефективні системи реагування на інциденти.

Однак компанії повинні вибрати фреймворк, який відповідає їхнім конкретним потребам і цілям.

4. Висновки

У роботі надано порівняльний огляд 4-х провідних фреймворків реагування на інциденти ІБ в США. Вибір фреймворку залежить від конкретних потреб і цілей організації.

NIST Cybersecurity Framework є хорошим вибором для організацій, які шукають гнучкий і адаптивний фреймворк, який охоплює весь цикл реагування на інциденти. Він пропонує загальні рекомендації, які можуть бути адаптовані до потреб будь-якої організації.

ISO/IEC 27001 слід обирати організаціям, які шукають всеосяжну і визнану міжнародну систему управління ІБ. Він пропонує детальні вимоги та рекомендації щодо управління ризиками та запобігання інцидентам.

CISA Cyber Incident Response Guide є доволі прийнятним для компаній, які шукають практичні і конкретні рекомендації, щодо реагування на інциденти. Пропонує конкретні кроки та процедури, які можуть бути використані для реагування на кіберінциденти.

NIST Special Publication 800-61 є хорошим вибором для організацій і структур, які шукають докладні і всеосяжні рекомендації щодо виявлення та реагування на інциденти. Містить детальні рекомендації та передові методи, які можуть бути використані для підвищення ефективності реагування на інциденти.

Організації, які шукають фреймворк реагування на інциденти, повинні враховувати такі фактори:

- цільова аудиторія: фреймворк повинен відповідати потребам і цілям організації;
- сфера застосування: фреймворк повинен охоплювати всі аспекти реагування на інциденти, які є важливими для організації;
- рівень деталізації: фреймворк має бути достатньо детальним, щоб бути корисним, але не надто, аби запобігти складнощам у розуміння та реалізації.

Організації також можуть розглянути можливість використання комбінації двох або більше фреймворків. Наприклад, організація може використовувати *NIST Cybersecurity Framework* для розробки загальної стратегії реагування на інциденти, а потім використовувати *CISA Cyber Incident Response Guide* для розробки більш конкретних процедур реагування на інциденти, зокрема у кіберпросторі.

Список літератури

[1] eSentire, Inc. (2023). “2022 Official Cybercrime Report.” Retrieved (https://www.esentire.com/resources/library/2022-official-cybercrime-report).

[2] American Public Power Association. (2021). “Public Power Cyber Incident Response Playbook” Retrieved (https://www.publicpower.org/resource/public-power-cyber-incident-response-playbook).

[3] Nist, Gaithersburg Md. (2023). The NIST Cybersecurity Framework 2.0. https://doi.org/10.6028/NIST.CSWP.29.ipd.

[4] NIST. (2021). “NIST SP 800-61 | NIST.” Retrieved (https://www.nist.gov/privacy-framework/nist-sp-800-61).

[5] Cybersecurity and Infrastructure Security Agency CISA. (2021). “CISA Releases Incident and Vulnerability Response Playbooks to Strengthen Cybersecurity for Federal Civilian Agencies | CISA.” Retrieved (https://www.cisa.gov/news-events/news/cisa-releases-incident-and-vulnerability-response-playbooks-strengthen).

[6] Information security, cybersecurity and privacy protection. Information security management systems. Requirements. ISO/IEC 27001. (2022). https://www.iso.org/standard/27001.

[7] NIST. (2023). “Cybersecurity Framework Components | NIST.” Retrieved (https://www.nist.gov/cyberframework/online-learning/cybersecurity-framework-components).

[8] Kosutic, Dejan. (2023). “What Is ISO 27001? A Detailed and Straightforward Guide.”. Retrieved (https://advisera.com/27001academy/what-is-iso-27001/).

Received: on October 2023. **Accepted:** on November 2023.

Authors:
Oleksandr Peliukh, student of the Department of Security of Information Systems and Technologies, V. N. Karazin Kharkiv National University, Ukraine.
E-mail: oleksandrpelyukh@gmail.com
ORCID: https://orcid.org/0000-0003-0507-0262
Maryna Yesina, Ph.D., Associate Professor, Department of Security of Information Systems and Technologies, V.N. Karazin Kharkiv National University, Ukraine.
E-mail: m.v.yesina@karazin.ua
ORCID: https://orcid.org/0000-0002-1252-7606
Dmytro Holubnychyi, Ph.D., Associate Professor, Head of the scientific department of JSC "IIT", Kharkiv, Ukraine.
E-mail: goldim1971@gmail.com
ORCID: https://orcid.org/0000-0002-1252-7606

Comparative Assessment of US Cyber Incident Response Systems.

Abstract. In today's world, cyber threats are becoming a serious issue for companies in all professional sectors. For all organisations, regardless of their field of activity, cyber threats in today's world are undoubtedly a significant challenge. Undoubtedly, modern organisations should set themselves the task of effectively countering cyber threats regardless of their professional industry. To effectively counter these threats, organisations must have effective incident response systems in place, including in cyberspace. There are many incident response frameworks in the US, each with its own advantages and disadvantages. This article offers a comparative analysis of the four leading US cyber incident response frameworks: NIST Cybersecurity Framework (*CSF*), *CISA Cyber Incident Response Guide*, *ISO/IEC 27001* and *NIST Special Publication 800-61*. The purpose of the study is to provide organisations with an overview of the four leading incident response frameworks in the US so that they can choose the most appropriate framework for their specific needs. The research was conducted using a qualitative approach that included a thorough review of official documents, a review of relevant current literature, and consultation with cybersecurity professionals. This article is an additional informational resource for organizations and companies looking for an effective and efficient method of responding to incidents, including cyber incidents. It provides an overview of the four leading frameworks in the US, allowing organisations to compare their advantages and disadvantages and ultimately choose the most appropriate framework for their specific objectives.

Keywords: *Cyber incident response, NIST CSF, CISA, ISO/IEC 27001, NIST SP 800-61, Risk management, Security frameworks.*