17. Prest, T. (2020). Efficient implementation issues in Falcon. https://falcon-sign.info.
18. SPHINCS+ Team. (n.d.). SPHINCS+ Specification. https://sphincs.org/data/sphincs+-specification.pdf.

Надійшла до редакції (Received): 22.01.2026
Прийнята до друку (Accepted): 17.03.2026
Опубліковано онлайн (Available online): 30.03.2026

УДК 004.056:005.6
DOI: 10.31673/2409-7292.2026.010656

Іванченко Є.В., Ковальчук О.А.

АНАЛІЗ МЕТОДИК ТА СТАНДАРТІВ УПРАВЛІННЯ КІБЕРСТІЙКІСТЮ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Проведено комплексний аналіз сучасних міжнародних стандартів та прикладних методологій оцінювання кіберстійкості інформаційних ресурсів (ІР). Визначено, що теоретичним підґрунтям для побудови систем кіберстійкості виступають стандарти ISO/IEC 27001 (системи управління інформаційною безпекою), ISO/IEC 27031 (готовність ІКТ до забезпечення безперервності бізнесу) та спеціальні публікації NIST (Framework for Improving Critical Infrastructure Cybersecurity, SP 800-160), які формують системний підхід, інтегруючи превентивне управління безпекою, відновлення після інцидентів та принципи системної інженерії. Проведено порівняльний аналіз п’яти провідних фреймворків оцінювання: Cyber Resilience Review (CRR), Cyber Assessment Framework (CAF), Cyber Resilience Assessment Framework (C-RAF), Cyber Resilience Index (CRI) та IT Governance Framework. Для порівняння застосовано п’ять критеріїв: наявність числового (індексного) вираження стійкості, фокус оцінки (якісна зрілість чи кількісні показники), динаміка оцінювання (статичний аудит чи тестування), джерела даних та врахування їх адекватності. Виявлено розбіжності між існуючими підходами. Встановлено, що якісні моделі (CRR, CAF) зосереджені на оцінці зрілості процесів («паперова стійкість»), тоді як кількісні моделі (CRI) базуються на метриках часу (MTTD, MTTR), проте часто ігнорують організаційний контекст. Окремо відзначено досвід C-RAF щодо впровадження динамічного тестування (iCAST), який, однак, має вузькогалузеву специфіку. Ключовим результатом дослідження є виявлення критичної наукової прогалини – відсутності в існуючих моделях механізмів перевірки адекватності, повноти та достовірності вхідних даних. Обґрунтовано необхідність розробки механізму, що поєднав би кількісні архітектурні метрики з оцінкою зрілості процесів та коефіцієнтом адекватності вхідних даних.

Ключові слова: кібербезпека, кіберстійкість, кібератака, оцінювання кіберстійкості, NIST CSF, ISO 27001, C-RAF, адекватність даних, модель, метод, методологія, стандарт, інформаційна безпека, механізм оцінювання кіберстійкості.

Вступ

В умовах зростання інтенсивності та складності кібератак, традиційні підходи до інформаційної безпеки, орієнтовані виключно на запобігання інцидентам, стають недостатніми. Актуальним стає перехід до парадигми кіберстійкості (Cyber Resilience) – здатності інформаційного ресурсу (ІР) не лише протистояти загрозам, але й адаптуватися до них та швидко відновлювати функціонування після збоїв.

Теоретичною базою для цього є міжнародні стандарти, такі як ISO/IEC 27001 та NIST CSF, які визначають системний підхід до управління ризиками та безперервністю. Проте, на практиці виникає проблема об'єктивної оцінки реального рівня стійкості. Існуючі методології варіюються від опитувальників зрілості до складних технічних метрик, що ускладнює вибір універсального інструменту.

Мета та постановка задачі

Метою є аналіз існуючих методологій та стандартів управління кіберстійкістю, виявлення їхніх переваг та недоліків. Для досягнення поставленої мети необхідно провести порівняльний аналіз існуючих методологій оцінки кіберстійкості за такими критеріями, як джерела даних, фокус оцінки та наявність механізмів динамічного тестування.

© Єлісєєва Г.С. Постквантова криптографія: сучасний стан та перспективи. Сучасний захист інформації, 1(65), 38–46. https://doi.org/10.31673/2409-7292.2026.010544

Виклад основного матеріалу

Теоретичним підгрунтям для побудови та оцінки кіберстійкості є міжнародні стандарти та методології, що визначають системний і структурований підхід. Вони охоплюють управління безпекою, безперервність бізнесу та системну інженерію.

Стандарт ISO/IEC 27001 [1] закладає основу для кіберстійкості, за рахунок впровадження системи управління інформаційною безпекою (СУІБ). Його роль у контексті стійкості є превентивною та організаційною:

- управління ризиками: ISO 27001 вимагає систематичного управління ризиками (Risk Management), що включає їх ідентифікацію, аналіз та обробку. Це забезпечує початкову ціль кіберстійкості – Протистояння (Withstand);
- заходи контролю: Додаток А стандарту містить перелік заходів контролю, які охоплюють ідентифікацію, захист активів, контроль доступу та криптографічні заходи, спрямовані на запобігання інцидентам;
- організаційний цикл: стандарт працює за циклом PDCA (Plan-Do-Check-Act), який забезпечує постійне вдосконалення СУІБ, що є кроком до адаптації системи до нових загроз.

Наявність ефективно впровадженої СУІБ зменшує ймовірність виникнення інциденту, а також визначає ресурси для відновлення у разі його виникнення.

Стандарт ISO/IEC 27031 [2] безпосередньо пов'язує інформаційні та комунікаційні технології (ІКТ) з вимогами безперервності бізнесу (BCM). Стандарт надає керівництво щодо підготовки ІКТ-інфраструктури, яка формує IP, до забезпечення безперервності критичних процесів після збоїв, катастроф або кібератак. ISO 27031 вимагає, щоб плани аварійного відновлення та плани безперервності були інтегровані з заходами інформаційної безпеки, гарантуючи, що відновлення не призведе до компрометації. Стандарт допомагає визначити необхідний рівень готовності ІКТ для досягнення цільових RTO (Recovery Time Objective), що є важливою частиною кількісної оцінки кіберстійкості.

Отже, стандарт поєднує превентивну безпеку та активні дії для BCM, надаючи практичні рекомендації щодо відновлення IP.

Рис.1. Функції NIST CSF v.2.0

NIST CSF [3] є важливим фреймворком для оцінки кіберстійкості, оскільки він описує життєвий цикл, що дозволяє систематизовано підходити до питання кіберстійкості. Це дозволяє організації забезпечити п'ять основних функцій (рис. 1):

1. Ідентифікація (Identify): визначення активів, ризиків та критичних функцій ІР. Це є основою для подальшого визначення RTO та RPO (Recovery Point Objective);

2. Захист (Protect): реалізація контрольних заходів для обмеження або стримування впливу події;

3. Виявлення (Detect): своєчасна ідентифікація кіберподій, що впливає на метрику MTTD (Mean Time To Detect);

4. Реагування (Respond): розробка та виконання дій для нейтралізації виявленого інциденту. Спроможність до реагування прямо впливає на час, протягом якого ІР перебуває в небезпеці;

5. Відновлення (Recover): розробка та реалізація планів для відновлення будь-яких функцій та послуг, що були порушені. Ці функції безпосередньо пов'язані з відновлюваністю (Recoverability) та метрикою MTTR (Mean Time To Recover), які є серцевиною кіберстійкості.

NIST CSF забезпечує цілісний погляд на стійкість, інтегруючи як превентивні, так і реактивні заходи. Останні дві функції CSF є методологічною основою для оцінки здатності ІР до адаптації та швидкого повернення до нормального стану.

Спеціальна публікація NIST SP 800-160 [4] надає інженерний підхід до побудови стійких систем, розглядаючи безпеку та стійкість як невід'ємні властивості архітектури ІР. Стандарт пропонує інтегрувати вимоги до стійкості на етапах проєктування (Security by Design). Це гарантує, що стійкість ІР не є випадковою, а є цільовою властивістю. NIST SP 800-160 є методологічною базою для оцінки архітектурної стійкості ІР.

Документ детально описує принципи, які мають бути реалізовані в архітектурі:

- здатність системи продовжувати виконувати свою місію, незважаючи на значні пошкодження;
- включення надмірності та механізмів «м'якої деградації» (Graceful Degradation);
- архітектурна підтримка швидкого повернення до цільового стану;

Для переведення теоретичних стандартів у практичну площину оцінки рівня стійкості інформаційного ресурсу (ІР) застосовуються спеціалізовані для науково обґрунтованої кількісної оцінки використовуються метрики, пов'язані з часом та зрілістю процесів:

- метрики часу: оцінка ІР базується на вимірюванні MTTD та MTTR. Чим менші ці показники, тим вища відновлюваність системи [4]. Коефіцієнт готовності ІР (A) може бути розрахований на основі MTTF (Mean Time To Failure) та MTTR за класичною формулою:

$$A = \frac{MTTF}{(MTTR+MTTF)}.$$

- моделювання загроз: застосування фреймворків, таких як MITRE ATT&CK [5], дозволяє систематизувати методи та техніки, які можуть бути використані для компрометації ІР. Це дає змогу оцінити здатність системи протистояти конкретним сценаріям атак;
- оцінка зрілості (Maturity Models): використання моделей, подібних до Cyber Resilience Review (CRR) [6], дозволяє оцінити ІР за ступенем відповідності встановленим найкращим практикам у п'яти функціях кіберстійкості: ідентифікація, захист, виявлення, реагування, відновлення. методики, які дозволяють отримати структуровану оцінку.

Cyber Resilience Review (CRR) [6] – це офіційна, нетехнічна оцінка, розроблена Агентством з кібербезпеки та безпеки інфраструктури США (CISA), яка ґрунтується на моделі зрілості (Maturity Model). Ця методологія підходить для оцінки ІР у критичній інфраструктурі. CRR оцінює організаційну зрілість та операційну спроможність щодо кіберстійкості. перевіряє не лише наявність технологій, а й те, наскільки ефективно впроваджені процеси управління ризиками, інцидентами та безперервністю. Оцінка охоплює 10 доменів, які включають управління ризиками, управління інцидентами, управління конфігурацією, забезпечення персоналом, а також аварійне відновлення (Disaster Recovery) та безперервність обслуговування (Service Continuity).

© Іванченко Є.В., Ковальчук О.А. Аналіз методик та стандартів управління кіберстійкістю інформаційних ресурсів. Сучасний захист інформації, 1(65), 46–53.
https://doi.org/10.31673/2409-7292.2026.010656

Організація оцінюється за п'ятьма рівнями зрілості (від *Неповного* до *Оптимізованого*). Це дозволяє визначити не просто наявність чи відсутність заходів, а рівень їхньої формалізації, документованості та тестування.

Результатом CRR є якісна оцінка слабких місць у процесах та пріоритетні рекомендації щодо інвестицій у підвищення стійкості.

Cyber Resilience Index (CRI) [7] – це клас наукових та комерційних моделей, спрямованих на створення композитного (інтегрального) показника кіберстійкості. Його основна мета – забезпечити кількісну, об'єктивну оцінку, яка може бути використана для порівняння або моніторингу прогресу.

На відміну від якісного CRR, CRI виражає стійкість IP єдиним числовим значенням (індексом), що підвищує об'єктивність оцінки. CRI використовує зважені кількісні метрики, які безпосередньо вимірюють ефективність елементів стійкості:

- часові метрики: RTO та MTTR – для оцінки відновлюваності;
- показники покриття: відсоток критичних даних, покритих резервуванням, або частка IP, охоплена сегментацією;
- показники відповідності: рівень дотримання вимог стандартів (наприклад, ISO, NIST).

Інтегральний показник CRI розраховується за допомогою методу зваженої суми або мультиплікативних функцій, де кожна метрика отримує вагу відповідно до критичності компонента IP.

Cyber Assessment Framework (CAF) [8] – це методологія, розроблена Національним центром кібербезпеки Великобританії (NCSC). Призначена для оцінки кіберризиків для критичних національних функцій та організацій, що належать до критичної інфраструктури. CAF визначає, *що* має бути досягнуто (наприклад, здатність протистояти атакам базової складності), а не *як* це зробити. Структурно фреймворк декомпозується на 4 високорівневі цілі (Objectives), 14 принципів та 39 відповідних результатів (Contributing Outcomes):

1. *Ціль A: Управління ризиками безпеки (Managing Security Risk).* Ціль визначає фундамент стійкості і включає чотири принципи (A1–A4):

- A1 Управління (Governance): наявність чіткої структури прийняття рішень на рівні Ради директорів;
- A2 Управління ризиками: перехід від періодичного до безперервного процесу оцінки ризиків;
- A3 Управління активами:повна видимість активів, включно з "тіньовим IT";
- A4 Управління ланцюгом постачання: контроль ризиків, що виникають від третіх сторін;

2. *Ціль B: Захист від кібератак (Protecting Against Cyber Attack).* Група охоплює шість принципів (B1–B6) технічного захисту: від політик захисту сервісів (B1) та контролю доступу (B2) до забезпечення безпеки даних (B3) і підвищення обізнаності персоналу (B6). Особлива увага приділяється принципу B5 (Стійкі мережі та системи), який вимагає архітектурної сегментації та відмовостійкості;

3. *Ціль C: Виявлення подій безпеки (Detecting Cyber Security Events).* Визначає спроможність організації не лише пасивно вести логи, а й активно виявляти інциденти. Включає:

- C1 Моніторинг безпеки: збір та аналіз даних про події;
- C2 Проактивне виявлення: пошук загроз, що обійшли стандартні засоби захисту;

4. *Ціль D: Мінімізація впливу інцидентів (Minimising the Impact).* Фокусується на відновлюваності через принципи планування реагування (D1) та вивчення уроків (D2). Це співвідноситься з фазами Respond та Recover у NIST CSF.

Для оцінки результатів у CAF використовуються Індикатори найкращої практики (Indicators of Good Practice – IGPs). Замість оцінки "є"/"немає", організація визначає свій статус як:

- Achieved (Досягнуто): повністю відповідає індикаторам "good practice";
- Partially Achieved (Частково досягнуто): присутні певні недоліки, але основна функція виконується№
- Not Achieved (Не досягнуто): критичні прогалини у захисті.

CAF дозволяє адаптувати оцінку IP залежно від його критичності та здатності протистояти різним категоріям загроз (наприклад, атакам базової чи помірної складності), використовуючи концепцію профілів (Profiles). Наприклад, «Базовий профіль» (CAF Baseline Profile) для менш критичних систем та «Посилений профіль» (Enhanced Profile) для об'єктів критичної інфраструктури державного значення. Це дозволяє уникнути надлишкових вимог для невеликих організацій, водночас встановлюючи жорсткі критерії для операторів основних послуг. Не зважаючи на гнучкий підхід, у CAF залишається проблема *достовірності вхідних даних.* Оцінка "Achieved" часто базується на самооцінці (self-assessment) або результатах аудиту документації, без обов'язкового технічного підтвердження (як-от iCAST у C-RAF), що може призводити до розриву між заявленим та реальним станом кіберстійкості.

Cyber Resilience Assessment Framework (C-RAF) [9] – це спеціалізований фреймворк, розроблений Валютним управлінням Гонконгу (HKMA) для оцінки стійкості фінансових установ (Authorized Institutions, AIs). Він вирізняється комплексною структурою та інтеграцією трьох ключових етапів:

1. Оцінка властивого ризику (Inherent Risk Assessment). Визначення притаманного рівня ризику IP на основі його архітектури, технологій, каналів доставки послуг та обсягу операцій. Це встановлює очікуваний (цільовий) рівень зрілості стійкості;
2. Оцінка зрілості (Maturity Assessment): оцінка фактичного рівня впровадження заходів кібербезпеки та стійкості;
3. Імітаційне тестування на основі розвідданих про загрози (Intelligence-led Cyber Attack Simulation Testing, iCAST): Це обов'язкове тестування, яке моделює атаки, використовуючи актуальну інформацію про загрози (Threat Intelligence), спрямовані саме на цей сектор. Це забезпечує перевірку спроможності IP до реагування та відновлення.

C-RAF демонструє найкращу практику інтеграції організаційної зрілості (Maturity) з тестуванням (Simulation), що є критичним для повноцінної оцінки. Це розширює класичний підхід NIST CSF. На відміну від п’яти функцій NIST, C-RAF базується на семи доменах, які ієрархічно розподілені за трьома рівнями впливу:

1. *Управлінський рівень (Governance):* управління є ядром моделі. Оцінює, наскільки керівництво організації залучене до процесів кіберстійкості, наявність стратегії, політик та розподіл відповідальності. Це підкреслює, що кіберстійкість є не лише технічною, а й управлінською проблемою;
2. *Внутрішнє середовище (Internal Environment):* охоплює чотири операційні домени, що відповідають за технічний захист активів організації:
   - ідентифікація (Identification): визначення критичних активів та ризиків;
   - захист (Protection): впровадження контролів для запобігання інцидентам;
   - виявлення (Detection): моніторинг аномалій та подій безпеки;
   - реагування та Відновлення (Response & Recovery): ці функції об’єднані в один домен, що акцентує на нерозривності процесу нейтралізації загрози та повернення до штатного режиму роботи.
3. **Зовнішнє середовище (External Environment):** C -RAF, яка додає два домени, часто відсутні в інших моделях:
   - ситуаційна обізнаність (Situational Awareness): оцінює здатність організації отримувати та використовувати дані про загрози (Threat Intelligence) з зовнішніх джерел;
   - Управління ризиками третіх сторін (Third-Party Risk Management): визначає спроможність контролювати ризики, що виникають через взаємодію з підрядниками, постачальниками хмарних послуг та партнерами по ланцюгу постачання.

Таблиця 1

Домени методології C-RAF

	Домен	**Компонент**
Управління (Governance)	Управління	Оверсайт за кіберстійкістю
		Стратегії та політики
		Менеджмент кіберризиків
		Аудит
		Кадрове забезпечення та навчання
Внутрішнє середовище	Ідентифікація	Ідентифікація IT активів
		Ідентифікація та оцінка кіберризиків
	Захист	Контролі захисту інфраструктури
		Контроль доступу
		Безпека даних
		Безпека коду
		Патч-менеджмент
		План усунення недоліків/план відновлення
	Виявлення	Виявлення вразливостей
		Виявлення аномальної активності
		Виявлення кіберінцидентів
		Моніторинг та аналіз загроз
	Реагування та відновлення	Планування реагування
		Управління інцидентами
		Ескалація та звітування
Зовнішнє середовище	Ситуаційна обізнаність	Розвідка про загрози
		Обмін розвідкою про загрози
	Управління ризиками третіх сторін	Зовнішні зв’язки
		Управління третіми сторонами
		Постійний моніторинг ризиків, пов’язаних з третіми сторонами

Така трирівнева структура («Центр – Внутрішнє середовище – Зовнішнє середовище») дозволяє проводити більш якісну оцінку, враховуючи не лише внутрішні технічні спроможності, але й залежність від зовнішньої екосистеми та якість управлінських рішень.

IT Governance Cyber Resilience Framework [10], розроблений консалтинговими компаніями, являє собою практичну інтеграційну модель, яка систематизує вимоги різних стандартів (ISO, NIST) у чотири ключові елементи контролю та чотири стадії стійкості: управління та забезпечення (Govern and Assure), управління та захист (Manage and Protect), ідентифікація та виявлення (Identify and Detect), реагування та відновлення (Respond and Recover). Модель орієнтована на профіль ризику організації та допомагає визначити високоцінні активи, на яких потрібно зосередити зусилля зі стійкості.

Модель є прикладом того, як індустрія комбінує елементи NIST CSF та ISO 27001 для створення практичного циклу оцінки та вдосконалення IP.

Для аналізу існуючих методологій оцінки виділимо наступні п'ять критеріїв:

1. Числове (індексне) вираження стійкості: здатність методології агрегувати результати в єдиний числовий інтегральний показник кіберстійкості (ІПКС);

2. Фокус оцінки: зосередженість моделі — на якісній оцінці зрілості процесів чи на кількісній оцінці архітектурної надійності (технічна реалізація);

3. Динаміка оцінки: чи включає методологія динамічне тестування (тестування, наприклад, iCAST) як обов'язковий компонент, чи вона є статичною (аудит документації).

4. Основне джерело даних – опитувальники (self-assessment) чи технічні метрики (MTTR, RPO, результати тестів).

5. Врахування адекватності даних: чи має модель механізм для перевірки якості, повноти та достовірності вхідних даних, що використовуються для самої оцінки.

Таблиця 2

Аналіз існуючих методологій оцінки кіберстійкості

Критерій	CRR (CISA)	CAF (UK NCSC)	C-RAF (HKMA)	CRI (Академічні моделі)	IT Governance Framework
1. Числове (індексне) вираження стійкості	Низька. (Якісний профіль зрілості).	Низька. (Якісна оцінка досягнення цілей).	Помірна. (Модель розрахунку не публічна).	Висока. (Мета – розрахунок числового індексу).	Низька. (Якісний консалтинговий фреймворк).
2. Фокус оцінки	Якісна (Зрілість процесів).	Якісна (Результати процесів).	Гібридна(Зрілість + Технічна перевірка).	Кількісна (Метрики: MTTR, RTO тощо).	Якісна (Зрілість процесів).
3. Динаміка оцінки	Статична	Статична	Динамічна	Статична	Статична
4. Основне джерело даних	Опитуванн, документація.	Документація та надані докази.	Опитування + тестування	Технічні метрики	Опитування, документація.
5. Врахування адекватності даних	Ні	Ні	Частково. (iCAST валідує *реакцію*, але не вхідні дані).	Ні	Ні

Проведений порівняльний аналіз методологій оцінки кіберстійкості (CRR, CAF, C-RAF, CRI та IT Governance Framework), що наведено у табл. 2, висвітлює три основні проблеми: відмінність між кількісними та якісними підходами, відсутність динамічної валідації та ігнорування проблеми адекватності вхідних даних.

По-перше, існує чітка методологічна відмінність між кількісними та якісними моделями. Такі підходи, як CRR та IT Governance Framework, є переважно якісними. Вони зосереджені на оцінці зрілості процесів, але їхні результати базуються на суб'єктивних опитуваннях та аналізі документації, що дає уявлення про «паперову стійкість», а не про реальну технічну живучість. З іншого боку, академічні моделі, такі як CRI, є кількісними та прагнуть до об'єктивності через використання метрик (наприклад, MTTR, RTO). Однак вони є статичними і часто ігнорують критично важливий організаційний та процесуальний контекст, в якому ці метрики існують.

По-друге, більшість методологій є статичними та не включають динамічну перевірку. CRR та CAF олрієнтовані на аудит документації. Винятком є C-RAF, який вимагає обов'язкового динамічного тестування iCAST, що є передовою практикою. Проте, C-RAF є вузькогалузевим (призначеним для фінансового сектору Гонконгу), а його математична модель розрахунку не є публічною, що унеможливлює її універсальне наукове застосування.

Варто зазначити, що жодна з проаналізованих методологій не вирішує проблему адекватності вхідних даних. Якісні моделі (CRR, CAF, IT Governance) повністю залежать від достовірності, повноти та компетентності відповідей, наданих під час самооцінки чи опитувань. Вони не мають вбудованого механізму для валідації того, чи є задокументований процес дієвим. Аналогічно, кількісні моделі (CRI) повністю залежать від точності та актуальності наданих метрик. Якщо показник MTTR застарілий, або показник RPO не відповідає реальним бізнес-вимогам, отриманий ІПКС буде математично коректним, але практично неадекватним, створюючи уявлення про захищеність системи.

Таким чином, відсутня універсальна модель оцінки кіберстійкості IP, яка б не лише поєднала кількісні архітектурні метрики та якісну зрілість процесів, але й мала вбудований

© Іванченко Є.В., Ковальчук О.А. Аналіз методик та стандартів управління кіберстійкістю інформаційних ресурсів. Сучасний захист інформації, 1(65), 46–53.
https://doi.org/10.31673/2409-7292.2026.010656

механізм валідації для оцінки повноти, достовірності та актуальності самих вхідних даних, використовуючи цю оцінку як обов'язковий коефіцієнт при формуванні кінцевого показника кіберстійкості.

Висновки

У роботі проведено аналіз ключових стандартів та методологій оцінки кіберстійкості. В ході аналізу виявлено, що стандарти ISO та NIST створюють фундамент, інтегруючи превентивну безпеку та механізми відновлення. Порівняльний аналіз методик (CRR, CRI, CAF, C-RAF) виявив методологічну відмінність: якісні моделі оцінюють задокументовану зрілість процесів, ігноруючи технічну реальність, тоді як кількісні моделі часто є статичними і не враховують бізнес-контекст.

Можна зробити висновок, що жодна з проаналізованих методологій не вирішує проблему адекватності вхідних даних. Відсутність механізмів валідації призводить до того, що оцінка стійкості може базуватися на застарілих або недостовірних показниках (наприклад, некоректних RPO/MTTR), створюючи хибне уявлення про захищеність системи.

Перспективою подальших досліджень є розробка механізму оцінки кіберстійкості інформаційних ресурсів, що враховує адекватність вхідних даних.

Перелік посилань

1. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. [Електронний ресурс]. Режим доступу: https://www.iso.org/standard/27001

2. ISO/IEC 27031:2025. Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity. [Електронний ресурс]. Режим доступу: https://www.iso.org/standard/27031.

3. The NIST Cybersecurity Framework (CSF) 2.0. [Електронний ресурс]. Режим доступу: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

4. NIST Special Publication 800-160, Volume 2. [Електронний ресурс]. Режим доступу: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf.

5. MITRE ATT&CK Framework. [Електронний ресурс]. Режим доступу: https://attack.mitre.org/\.

6. Cyber Resilience Review. [Електронний ресурс]. Режим доступу: https://www.cisa.gov/resources-tools/services/cyber-resilience-review-crr.

7. Cyber Resilience Index. [Електронний ресурс]. Режим доступу: https://www3.weforum.org/docs/ WEF_Cyber_Resilience_Index_2022.pdf.

8. Cyber Assessment Framework. [Електронний ресурс]. Режим доступу: https://www.ncsc.gov.uk/collection/cyber-assessment-framework.

9. Cyber Resilience Assessment Framework. [Електронний ресурс]. Режим доступу: https://uploads-ssl.webflow.com/59d28ad983887e000196f803/5fecc1fe13498132b4fa835b_HKMA CFI, Cyber Resilience Assessment Framework, Dec 2016.pdf.

10. IT Governance Cyber Resilience Framework. [Електронний ресурс]. Режим доступу: https://www.itgovernance.co.uk/cyber-resilience-framework.

Надійшла до редакції (Received): 25.01.2026
Прийнята до друку (Accepted): 17.03.2026
Опубліковано онлайн (Available online): 30.03.2026

© Іванченко Є.В., Ковальчук О.А. Аналіз методик та стандартів управління кіберстійкістю інформаційних ресурсів. Сучасний захист інформації, 1(65), 46–53.
https://doi.org/10.31673/2409-7292.2026.010656