DOI: https://doi.org/10.36910/6775-2524-0560-2025-59-02
УДК 519.7-004.056
Личик Владислав Васильович, асистент
https://orcid.org/0009-0006-3314-6550
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ, Україна.

АДАПТИВНИЙ ПІДХІД ДО РЕАГУВАННЯ НА ПОРУШЕННЯ КІБЕРСТІЙКОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Личик В. В. Адаптивний підхід до реагування на порушення кіберстійкості об'єктів критичної інфраструктури. Кібератаки на об'єкти критичної інфраструктури в ході сучасної повномасштабної війни стали невід'ємним аспектом тиску на системи розподілення та однією з ключових частин безпосередніх військових дій. Зокрема, останні актуальні атаки у кіберпросторі спрямовані не тільки нанести шкоду окремим локальним підсистемам, а й направлені на дестабілізацію внутрішніх процесів в країні через вплив на енергетичні компанії та підрозділи, водопостачальні мережі, фінансові установи та інші життєво важливі об'єкти. Саме тому, все ще актуальною залишається проблематика кількісної оцінки кіберстійкості, тобто здатності системи/підприємства витримати певний негативний вплив та у майбутньому відновитися до прийнятного функціонального стану. Разом з тим, важливо також розуміти чітку структуру та ієрархію критичності таких кіберінцидентів, оскільки як показали останні події – вони можуть мати абсолютно різний характер, в залежності від сфери чи сектору держави. Таким чином, в ході дослідження було проведено аналіз найбільших існуючих фреймворків та систем для оцінки кіберстійкості, саме з точки зору можливості кількісної, а не якісної оцінки. У статті йдеться про недостатність традиційних якісних методів оцінювання та обґрунтовуються потреба у впровадженні кількісних метрик, які дозволяють оцінювати рівень кіберстійкості, моделювати та оцінювати потенційні втрати. У статті проаналізовано сучасні підходи до кількісної оцінки кіберстійкості, їхню застосовність в умовах українського енергетичного сектору та запропоновано розподіл кіберінцидентів за критичністю, порядок реагування та потенційні напрямки уражень.
Ключові слова: кіберстійкість; відновлення; функціональний стан об'єкта; кількісна оцінка рівня кіберстійкості; критичність кіберінциденту.

Lychyk V. Adaptive Approach to Responding to Cyber Resilience Breaches of Critical Infrastructure Facilities. Cyberattacks on critical infrastructure during modern full-scale war have become an integral aspect of pressure on distribution systems and one of the key components of direct military action. In particular, recent attacks in cyberspace are aimed not only at damaging individual local subsystems, but also at destabilising internal processes in the country by affecting energy companies and divisions, water supply networks, financial institutions and other vital facilities. That is why the issue of quantitative assessment of cyber resilience, specifically the ability of a system/enterprise to withstand a certain negative impact and recover to an acceptable functional state in the future, remains relevant. At the same time, it is also important to understand the precise structure and hierarchy of the criticality of such cyber incidents, since, as recent events have shown, they can be of a completely different nature, depending on the field or sector of the state. Thus, the paper analysed the largest existing frameworks and systems for assessing cyber resilience, specifically from the point of view of quantitative rather than qualitative assessment. The paper described the inadequacy of traditional qualitative assessment methods and justified the need to introduce quantitative metrics that allow assessing the level of cyber resilience, modelling and evaluating potential losses. The paper analysed modern approaches to quantitative assessment of cyber resilience, their applicability in the Ukrainian energy sector and proposed a classification of cyber incidents by criticality, response procedure and potential areas of damage.
Keywords: cyber resilience; recovery; functional state of an object; quantitative assessment of cyber resilience; criticality of a cyber incident.

Постановка наукової проблеми. Сучасні умови гібридної війни продемонстрували, що кібератаки на критичну інфраструктуру у різних сферах життєдіяльності можуть мати не менш руйнівний характер, ніж фізичні військові дії. З огляду на зростання кількості та складності кібератак, особливо в умовах воєнного стану та гібридної агресії, питання забезпечення безперервного функціонування енергетичних систем набуває пріоритетного значення. Зокрема, гостро постає питання щодо існуючих підходів для забезпечення кіберстійкості [1], або ж навіть відсутності чіткого алгоритму реагування для подальшого відновлення. Таким чином, з'явилась необхідність зміщення фокусу прямої інтеграції безпекових заходів щодо кібератак у сфері критичної інфраструктури на акцент на відновленні системи/об'єкта до прийнятного робочого стану, тобто забезпечення кіберстійкості. Про актуальність цієї тенденції та проблематики також говорять тенденції до створення нових державних органів, на найвищому рівні.

Йдеться про національну систему реагування на інциденти та атаки у кібернетичному просторі [2]. Такий підхід дозволяє організаціям та державним інституціям оцінити потенційні загрози, визначити слабкі місця системи та скоригувати подальші локальні та глобальні стратегії захисту/протидії [3]. Даний аспект необхідний для досягнення оптимального/прийнятного рівня

захисту. Це в свою чергу дає змогу забезпечувати безперервність роботи об'єктів критичної інфраструктури, незважаючи на інтенсивну ворожу діяльність у секторі кібератак. Врахування кількісних оцінок кіберстійкості допомагає інтегрувати кіберзахист як такий у загальну стратегію національної безпеки. Зокрема, визначати потенціал можливого відновлення після завданої шкоди та розподіл необхідних ресурсів та необхідних сервісів, чи органів управління.

Проте, водночас, якщо з аналізом якісних показників кіберстійкості наявних систем та фреймворків, а також з моделюванням прототипів систем цих об'єктів, ситуація загалом зрозуміла. То в контексті саме кількісного підходу та визначення конкретних метрик/параметрів думки експертів розходяться [4]. Наразі, все ще не існує більш-менш чіткого єдиного механізму, який можна було б застосувати до об'єктів критичної інфраструктури з різних сфер. Спочатку треба розібратися з життєвим циклом забезпечення кіберстійкості. Він може бути узагальнений в наступному порядку:

- планування та підготовка;
- виявлення та аналіз;
- сповіщення та стримування;
- ліквідація наслідків;
- адаптація та відновлення;
- подальша діяльність інфраструктурного об'єкту.

Аналіз останніх досліджень і публікацій. У минулому нашому дослідженні [1] ми сформували саме понятійний апарат, набувавшого актуальності в той час терміну «кібервідмовосткійть» та розглядали його забезпечення в контексті якісних показників та розподілу на домени, як окремі підструктурні одиниці. Зокрема, раніше було з'ясовано, що найбільш комплексним для оцінки розгалуженої системи об'єкту є Шотландський фреймворк для державного сектору [5]. Головними критичними функціями кіберстійкості є:

- *Ідентифікація* – завчасний пошук індикаторів впливу, векторів атак, які можна використати, щоб проникнути у IT-екосистему.
- *Захист* – зменшення вразливих місць відповідно до вашої терпимості до ризику.
- *Виявлення* – виявлення індикаторів компрометації за допомогою аудиту в реальному часі, виявлення аномалій та попередження.
- *Відповідь* – швидкий збір та аналіз інформації про інцидент, задля прийняття обґрунтованих рішень щодо найкращого способу дій.
- *Відновлення* – швидке, точне та ефективне відновлення системи і даних.
- *Керування* – наскрізна функція, яка інформує та підтримує інших; наприклад, результати управління визначають пріоритетність засобів контролю безпеки.

Нижче проведена детальна апробація Шотландського фреймворку [6] для прототипу енергетичного об'єкту критичної інфраструктури України. А саме для системи розподілення.

Organisation	Critical infrastructure facility.
Sector	Energy sector. Distribution systems.
Statement of Applicability	Framework for assessing cyber resilience

Report Date	Baseline	Target	Advanced
7 червень 2019 р.	56,67%	9,81%	5,09%
12 червень 2019 р.	91,67%	34,46%	17,74%
21 червень 2019 р.	100,00%	81,50%	42,91%
26 червень 2019 р.	93,33%	89,73%	66,29%
3 липень 2019 р.	96,67%	90,41%	74,84%
11 липень 2019 р.	70,00%	74,66%	89,73%

Рис. 1. Оцінка кіберстійкості інфраструктурного об'єкту за визначений часовий період

CE	PSAP	PSN - ITHC	PCI-DSS	10 Steps	GDPR	HMG SPF	ISO 27001	NIS - CAF
93,33%	86,67%	44,00%	41,67%	45,65%	38,89%	44,68%	35,19%	34,43%
100,00%	93,33%	76,92%	72,00%	71,74%	69,44%	72,92%	61,82%	64,52%
100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	96,36%	96,77%
86,67%	93,33%	88,46%	92,00%	93,48%	94,44%	93,75%	94,55%	91,94%
100,00%	96,67%	88,46%	96,00%	89,13%	91,67%	89,58%	90,91%	90,32%
60,00%	70,00%	76,92%	84,00%	71,74%	88,89%	81,25%	85,45%	85,48%

Рис. 2. Тенденція оцінки відповідності існуючим стандартам за аналогічний період

Рис. 3. Виконання вимог доменів Шотландського фреймворку для державного сектору

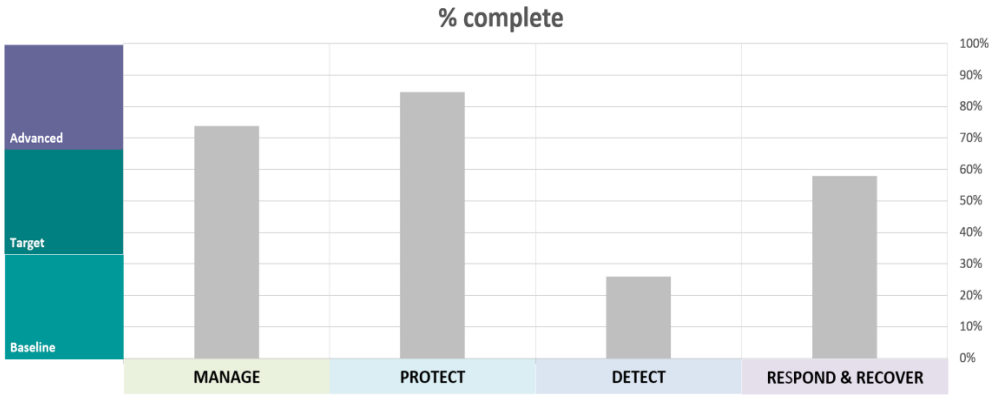

Рис. 4. Процес інтеграції вимог кіберстійкості на різних рівнях

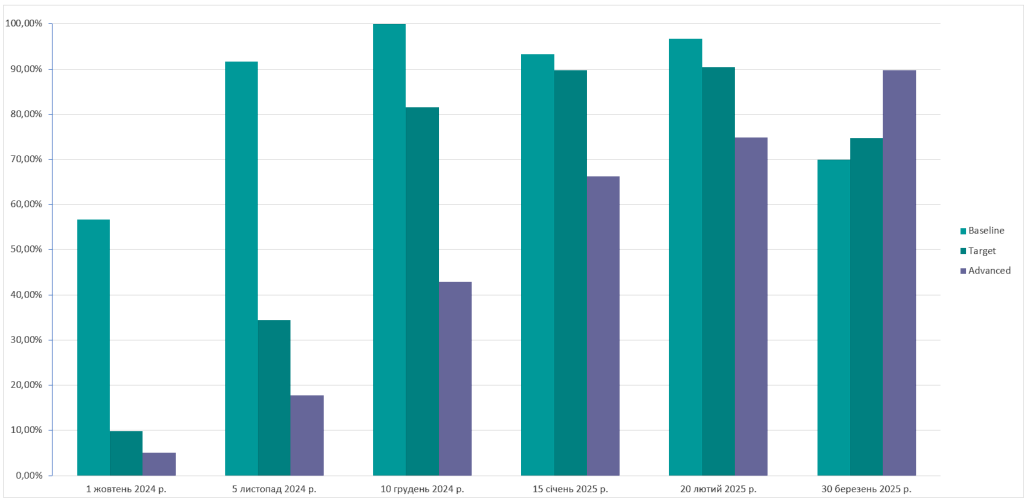

Рис. 5. Градація індикатора кіберстійкості за визначений часовий період

Водночас, незважаючи на розподіл та градацію якісних параметрів кіберстійкості, все ще залишилась невирішою проблема кількісної оцінки кіберстійкості [1]. З моменту введення в широке застосування терміну «кіберстійкість», або ж «кібервідмовостійкість» систем, акцент в її оцінки змінився з якісного характеру [7-8] на кількісну оцінку.

Тому, варто провести аналіз останніх фреймворків для оцінки кіберстійкості - саме в контексті кількісного підходу. Можна стверджувати, що з плином часу стала спостерігатися планомірна інтеграція кіберзахисту з кіберстійкістю. Певні підходи вже не розділяють ці два напрямки окремо, а розглядають як частини одного цілого. До того ж, вже з плином часу з'явилась необхідність саме пошуку підходів до кількісного аналізу.

Оскільки, шкода внаслідок кіберінцидетів вже напряму має вплив на цілі сектори держави та навіть навколишнє середовище, не кажучи вже про конкретні інфраструктурні об'єкти. Що ставить під загрозу не тільки фінансове питання, а й життєдіяльність цілих регіонів.

Тобто, в умовах коли мова йде не про сам захист від кібератаки, а відновлення об'єкта до прийнятного функціонального стану та надалі до штатного режиму роботи. І в такому контексті вже варто провести аналіз наявних та найбільш релевантних фреймворків, метрик чи систем для кількісної оцінки кіберстійкості.

Таблиця 1. Порівняльна характеристика фреймворків для забезпечення кіберстійкості

Фреймворк	**Основні характеристики**	**Підходи та принципи**	**Мета та цілі**	**Ключові переваги в порівнянні з іншими**	**Сфера застосування**	**Кількісні показники для розрахунку**
Scottish Public Sector Cyber Resilience Framework	Відновлення, безперервне вдосконалення, кризове управління.	Плани реагування, адаптація.	**Мета:** Забезпечення кіберстійкості в державному секторі. **Цілі:** Зниження наслідків кіберінцидентів, відновлення.	Фокус на відновленні та безпеці державних структур.	Державний сектор, критична інфраструктура.	Час відновлення після інцидентів, зменшення кількості інцидентів.
NIST Cyber Resilience Review (CRR)	Аналіз загроз, виявлення вразливостей, планування та відновлення.	Кризове управління, оцінка ризиків, сценарне тестування.	**Мета:** Покращення здатності до відновлення та стійкості. **Цілі:** Виявлення слабких місць, покращення планів відновлення**.**	Орієнтований на критичну інфраструктуру та виявлення потенційних загроз.	Критична інфраструктура, організації з високими ризиками.	Час до відновлення після інциденту, кількість виявлених загроз.
ISO/IEC 27032	Захист критичної інфраструктури, тестування систем на проникнення.	Управління інцидентами.	**Мета:** Підвищення рівня кіберстійкості через виконання вимог міжнародних стандартів. **Цілі:** Створення узгоджених підходів до кіберстійкості**.**	Інтеграція з іншими стандартами безпеки та кіберстійкості.	Міжнародні організації, критична інфраструктура.	Кількість інцидентів, час відновлення.
Cyber Resilience Assessment Model (CRAM)	Сценарне моделювання, ризик-менеджмент.	Оцінка стану функціональності та відновлення, стратегія дій після	**Мета:** Оцінка здатності до відновлення та покращення стійкості бізнесу. **Цілі:** Визначення недоліків у	Гнучкість в оцінці різних типів організацій та сценаріїв.	Бізнес-організації, малий та середній бізнес.	Відсоток відновлених бізнес-процесів, час повернення ключових процесів до

		інциденті в.	комунікації бізнес-процесів**.**			функціона льного стану.
Resilience Manageme nt Model (RMM)	Оцінка інфраструкту ри, довгостроков а стабільність.	Визначен ня рівнів стійкості, аналіз інциденті в.	**Мета:** Побудова системи стійкості для організації на довгострокову перспективу. **Цілі:** Визначення рівнів стійкості, планування та відновлення**.**	Оцінка та планування стійкості для довгостроко вого розвитку.	Великі підприємств а, організації з глобальними операціями.	Рівень стійкості, час на відновлен ня після інциденту.
BCI Cyber Resilience Framewor k	Відновлення ключових процесів, кризові плани.	Інтеграція з бізнес-процесам и, підтримка критични х функцій.	**Мета:** Забезпечення безперервності функціонування бізнес-процесів навіть у разі кіберінцидентів. **Цілі:** Зниження ризику зупинки критичних бізнес-функцій**.**	Інтеграція кіберстійкос ті в бізнес-процеси для швидкого відновлення робочих процесів.	Великі та середні бізнеси, організації з критичними функціями.	Час простою, час відновлен ня критичних функцій.
Axelos RESILIA Framewor k	Навчання персоналу, стратегії реагування.	Підвищен ня обізнанос ті, плануван ня та прогнозув ання, соціальна інженерія.	**Мета:** Підвищення усвідомленості та обізнаності персоналу організації. **Цілі:** Формування культури кіберстійкості**.**	Фокус на поведінкови х аспектах безпеки.	Великі та середні підприємств а, освітні установи.	Кількість проведени х тренінгів, рівень обізнаност і співробітн иків.
Cybersecu rity Capability Maturity Model (C2M2)	Оцінка поточних можливостей, розвиток стратегій.	Покращен ня стабільно сті процесів, усунення слабких місць.	**Мета:** Оцінка стабільності процесів кіберстійкості та безпеки. **Цілі:** Підвищення ефективності заходів безпеки та відновлення.	Модульна система, що дозволяє покращувати окремі аспекти стійкості.	Організації будь-якого масштабу, критичні сектори.	Рівень функціона льності процесів, час на відновлен ня, рівень збереженн я функціона льності ключової місії.

Наведені методології оцінки кіберстійкості забезпечують структуровані підходи до визначення самих цілей безпеки, так і засобів контролю за відновленням прийнятного робочого стану системи/підприємства/об'єкта. Зокрема, у вищезгаданих фреймворках узгоджуються сформульовані раніше якісні критерії з актуальними ключовими кількісними показниками. При цьому, частина з цих систем все-таки все ще балансує на межі понять «кібербезпеки» та «кіберстійкості». Однак, все ще відкритим залишається питання підбору показників та метрик для оцінки.

Результати дослідження. Як бачимо проведений аналіз показав, що наразі розробники та аналітики фреймворків демонструють необхідність комплексного підходу до забезпечення захисту, а не розділення кібербезпеки та кіберстійкості - як двох окремих концепцій. Та також той факт, що незважаючи на часовий та методологічний прогрес, все ще не існує чітких критеріїв для

розрахунків. Це насамперед пов'язано з бажанням розробників до комерціалізації та відсутності чітких державних регуляторів *(в англомовній літературі - ролі «supervisor» з домінуючими правами та рівнями доступу до центрального управління)*. Що призводить до намагання створити «універсальний» механізм для стримування та застосування його на усі сектори та галузі.

Однак, як наглядно продемонстрували останні події (як українські [9], так і європейські) кіберінциденти в енергетиці, транспортому та військовому секторах мають абсолютно різні характери. В двох останніх ціллю стійкості стоїть забезпечення мінімальної шкоди від прямого процесу ураження. В той час як в енергетичному секторі в першу чергу страждають такі критичні функції як розподіл та транспортування електроенергії, оскільки ці аспекти ключової місії повинні бути неперервними, бо як відомо електроенергія не має як такого у звичайному розумінні накопичуваного ефекту. Тому, в першу чергу має бути розглянутий підхід до забезпечення кіберстійкості саме на терені української енергетики [10]. Пропонується розподіл на критичністю та порядок реагування на події в кіберпросторі. Виходячи із даної тенденції, можна виділити такі основні кількісні параметри для оцінки кіберстійкості об'єктів критичної інфраструктури різного характеру.

1. Середній час відновлення (MTTR)

- Розрахунок: Загальний час простою / Кількість інцидентів

- Ситуація: Атака програми-вимагача на систему управління підстанції розподілу електроенергії розпочалась о 10:00 ранку. При цьому повний контроль доступу до керування було відновлено о 18:00. Отже, сумарний час простою системи склав 8 годин. Оскільки, за цей часовий проміжок був зафіксований один кіберінцидент, тому MTTR буде становити: 8 годин / 1 інцидент = 8 годин.

2. Цільовий пункт відновлення (RPO)

- Розрахунок: Даний показник не є результатом обчислення, а передбачає за собою конкретне значення. Зокрема, RPO встановлюється згідно впливу загрози/атаки на саму систему.
- Ситуація: Дані з контролерів одного з метрологічного контурів інфраструктурного об'єкта передаються на робочу станцію та архівуються з інтервалом у 30 хвилин. Отже, у разі виникнення інциденту, що приведе до втрати даних або проблем з архівуванням нових даних, метою та ціллю (кіберстійкості) є відновлення до стану, який є останнім у відношенні актуального робочого стану зразка не пізніше ніж на 30 хвилин. Таким чином, для заподіянню цьому типу кіберінцидентів запроваджується реплікація даних, встановлення додаткових незалежних точок зберігання інформації та застосування резервного копіювання з інтервалом не менш ніж кожні 30 хвилин.

3. Цільовий час відновлення (RTO)

- Розрахунок: Даний показник також є визначеною ціллю, а не результатом обчислення. Він представляє максимально допустимий прийнятний час для відновлення критичних функцій об'єкта після інциденту.
- Ситуація: Підстанція розподілення електроенергії має RTO у 2 години для своєї основної системи управління. Водночас, підстанція підтримує резервну систему керування та має детальний план відновлення після інцидентів/аварій, щоб відповідати даному показнику RTO. Після змодельованої, або ж імітованої атаки персонал підстанції ініціює перехід на резервну систему управління та відстежує час, який необхідний для відновлення загальної системи до прийнятного стану – тобто, до коректного функціонування основних критичних функцій розподілу між споживачами. Таким чином, досягнення 2-годинної цілі в таких сценаріях демонструє прагнення персоналу підстанції мінімізувати перебої в доставленні електроенергії до кінцевого споживача та належному розподілі.

4. Безперервність системних процесів (SPC)

- Розрахунок: (Кількість функціональних/відновлених критичних процесів / Загальна кількість критичних процесів) * 100%.
- Ситуація: Оператор енергосистеми визначив п'ять ключових процесів, критично важливих для підтримки стабільності мережі. Під час змодельованої атаки оператор оцінив, що після відновлення протягом 4 годин чотири з п'яти критичних процесів були повністю функціональними. Це призвело такого показника SPC: 4 / 5 * 100% = 80% .

5. Відсоток збереження функціональності ключової місії

- Розрахунок: Оцінюється шляхом визначення доступності та продуктивності критичних систем і служб. Зокрема, з використанням порівняльних функцій на основі індикатора критичності (про це далі у статті) для важливого компонента системи.
- Ситуація: Енергетичне підприємств визначило три основні функції місії та присвоїло їм вагові коефіцієнти: Розподільча система (40%), Інформаційна система моніторингу показників (30%) та Транспортування електроенергії (30%). Після кібератаки на об'єкт критичної інфраструктури було оцінено функціональність кожної із підсистем: Розподільча система працювала на 50%, Інформаційна система моніторингу показників не працювала (0%), а Транспортування електроенергії працювало з незначними перебоями, тобто – умовно на 90%. Загальний відсоток збереження функціональності ключової місії об'єкта інфраструктури склав (0.50 * 40%) + (0.00 * 30%) + (0.90 * 30%) = 47% .

Узагальнюючи, ці основні кількісні критерії демонструють, як кількісно на даному етапі розвитку оцінюються ключові аспекти кіберстійкості у різних фреймворках в контексті об'єктів критичної інфраструктури. Зокрема, у нашому випадку – у контексті енергетичної сфери. Тому, показники, критерії, конкретні цілі та методи забезпечення прийнятного стану функціонування будуть відрізнятися залежно від галузі, організації та конкретних ризиків.

Тепер, як було вже згадано вище, потрібно розібратися з класифікацією потенційних інцидентів, зокрема з їх рівнем критичності, типами та категоріями. Для побудови наступних аналітичних таблиць були використані дані з власних джерел, зокрема типових політик українських об'єктів критичної інфраструктури.

Таблиця 2. Класифікація інцидентів

Категорія інциденту	**Тип інциденту**	**Опис інциденту**
Шкідливий вміст контенту	Спам	Надсилання зловмисних повідомлень, або ж великої кількості таких повідомлень.
Шкідливий програмний код	Розповсюдження шкідливого програмного забезпечення (далі – ШПЗ)	Виявлення у системі застосунків/програм/утиліт з шкідливим програмним кодом.
	Підміна команд у центрі управління	Мережа ботів (ботнет) в якості збору інформації.
	Шкідливе підключення	Підключення від мережі з наявним ШПЗ, або ж ботнету.
Збір інформації	Моніторинг	Збір інформації про стан та характеристики системи/мережі (їх компонентів).
	Сніфінг та фішинг	Несанкціоноване перехоплення, моніторинг, читання та аналіз мережевого трафіку. Застосування методів соціальної інженерії задля збору інформації.
Несанкціоноване проникнення	Експлуатація вразливості	Використання наявних вразливостей у системі, або ж мережі.

	Автентифікація у системі управління	Використання служб та ресурсів системи для отримання доступу та подальшої авторизації у систему.
Втручання	Компрометація облікових профілів користувачів з різними ролями	Безпосереднє вторгнення у систему, або ж її компоненти, шляхом отримання облікових даних.
Порушення доступності	DDoS атака (на відмову в обслуговуванні)	Перенасичення пропускної можливості ресурсу системи.
	Саботаж/шкідливі дії/збій роботи системи	Пряме пошкодження інформації, переривання функціональних процесів компонентів та підрозділів системи.
Порушення цілісності інформації	Несанкціонований доступ	Витік інформації із інформаційних ресурсів системи.
	Несанкціонована модифікація	Зміна інформаційних ресурсів системи.
Шахрайські дії	Шахрайський ресурс	Впровадження та розгортання в системі програмних засобів з ціллю підміни використання ресурсів, відмінних від передбачуваних.
Наявна вразливість	Вразливість	Відкриті для експлуатації вразливості у системі, чи її компонентах (структурних підрозділах, одиницях, тощо).
	Неправильне налаштування/конфігурація	Некоректно задані умови та налаштування системи (її компонентів), якими може скористатися зловмисник, або ж ШПЗ.
Невідоме та інше	Нової невідомої раніше формації/типу інцидент. Або ж невизначена подія втручання	Відсутність або недостатність об'єму даних для аналізу/обробки інциденту, які необхідні для подальшої реакції.

Таблиця 3. Узагальнена класифікація кіберінцидентів за рівнем критичності

Рівень критичності кіберінциденту	**Загроза**	**Загальний стан**
Некритичний (білий)	Можливий потенційний негативний вплив на сталий стан локальних компонентів.	Кіберінцидент не загрожує штатному режиму роботи систем інфраструктурного об'єкта.
Низький (зелений)	Загрози конфіденційності, цілісності і доступності інформації та даних, що обробляються всередині систем, немає.	Кіберінцидент безпосередньо загрожує безперервній та надійній роботі локальних підсистем низького рівня на об'єкті/підприємстві.
Середній (жовтий)	Є загроза створення передумов для порушення захищеності потоків інформації, що може призвести до тимчасового припинення роботи функцій цілих систем об'єкта критичної інфраструктури.	Кіберінцидент безпосередньо загрожує штатному режиму інформаційно-комунікаційних та технологічних систем на об'єкті.
Високий (помаранчевий)	Є потенційна загроза для критичних функцій об'єкта критичної інфраструктури. Зокрема, що може мати негативний вплив навіть на рівень національної безпеки, стану навколишнього середовища та економічного сектору.	Кіберінцидент напряму впливає на надійність, стійкість та саму здатність критичного об'єкта до відновлення. Повернення рівня функціональності критичної інфраструктури до прийнятного робочого стану може потребувати задіяння декількох суб'єктів національної системи безпеки (кібербезпеки).
Критичний (червоний)	Прямий негативний вплив не тільки на цілісність потоків інформації та даних, роботу систем, а й загалом на можливість об'єкта до функціонування як таку. Наслідки кібератаки можуть призвести до безпосередньої шкоди для сфери національної безпеки, природи та навіть тимчасового припинення працездатності цілих критичних сфер державного рівня.	Кіберінцидент прямо загрожує робочому стану об'єкта критичної інфраструктури та несе за собою повне припинення виконання основних функцій та послуг. Відбиття атаки та подальше відновлення від інциденту потребує безпосереднього залучення ключових суб'єктів національної безпеки та системи кіберзахисту державного рівня.

Надзвичайний (чорний)	Повне припинення функціонування об'єкта критичної інфраструктури. Несе під собою транснаціональний характер загрози. Призводить до прямого фізичного руйнування інфраструктури, витоку чутливої таємної інформації та непоправної репутаційної/фінансової/ресурсної шкоди.	Кіберінцидент повністю перешкоджає або унеможливлює хоча б якийсь мінімальний стан функціонування критичного сектору. Потребує залучення усіх внутрішніх та зовнішніх ресурсів на державних рівнях.

На момент останнього аналітичного дослідження, найбільш комплексною системою для оцінки (точніше, для аналізу) кіберстійкості було визначено Шотландський фреймворк. Проте, часова тенденція змістила акцент з розподілу на домени та категорії – на оцінку рівня адаптивності та відновлення після кіберінциденту. Зокрема, акцентованість саме на енергетичному секторі притаманна не лише для України.

Рис. 6. Сфера застосування фреймворку C2M2 [11]

Водночас, все ще не існує чіткого концептуального підходу до реагування кіберінциденти у різних сферах критичної інфраструктури. Оскільки, вищезгадані фреймворки та актуальні релевантні метрики для оцінювання [12-13] акцентують свою увагу саме на розподілі функцій на категорії та ролях у ланцюгу виконання конкретних вимог до забезпечення кіберстійкості, однак при цьому не пропонують алгоритм реакції та протидії.

Провівши аналіз на основі на власних джерел, було запропоновано наступний порядок управління при кіберінциденті з «супервайзером» у головній ролі. Враховуючи специфіку енергетичного сектору України та необхідності насамперед забезпечення процесу відновлення до прийнятного функціонального режиму роботи інфраструктурного об'єкта отримуємо наступний алгоритм дій.

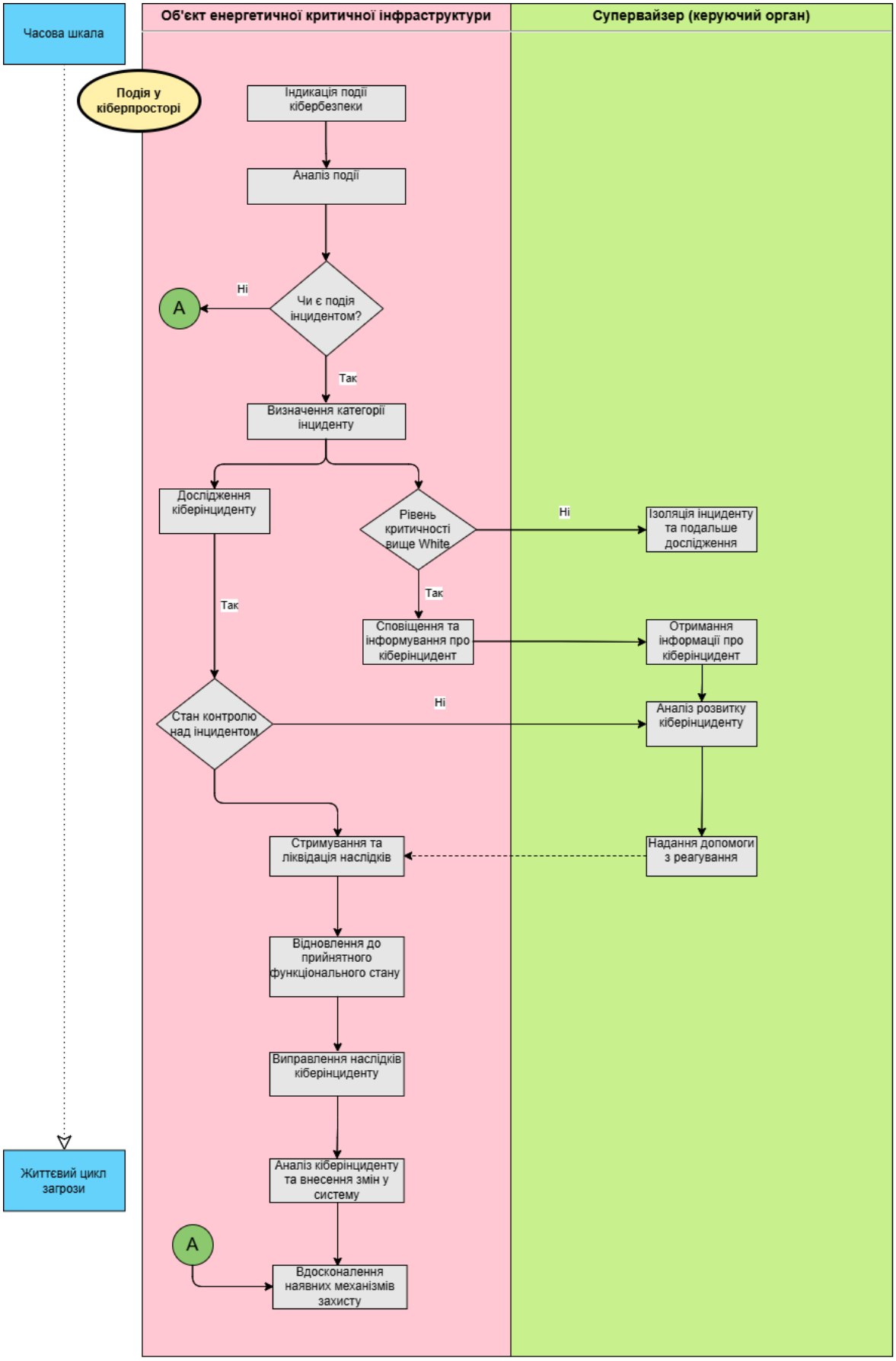

Рис. 7. Порядок реагування на потенційний інцидент

Висновки та перспективи подальшого дослідження. Проведений аналіз актуальних фреймворків та систем для оцінки кіберстійкості підтверджує тенденцію зміщення акценту з якісних показників на кількісні. В першу чергу, останні метрики зосереджені на прогнозуванні та адаптації до виникаючих умов, тобто до планування на випадок надзвичайних ситуацій чи інцидентів.

Водночас, можна стверджувати, що оцінка показників кіберстійкості безпосередньо та прямо залежить від характеру інцидентів та подій. Тому, при визначенні набору кількісних показників для конкретного об'єкта критичної інфраструктури необхідно враховувати специфіку, характер та критичність відповідних загроз, що несуть потенційний негативний вплив на критичну інфраструктуру. Тим не менше, універсальними критеріями для більшості об'єктів (та їх внутрішніх систем) є MTTR, RPO, RTO, SPC та відсоток збереженої функціональності ключової місії об'єкта/підприємства, які дають цінну кількісну інформацію для подальшого процесу відновлення. Даний матеріал дає підґрунтя для подальшого застосування та розрахунку показників кіберстійкості в комплексі з моделюванням, тобто вже на основі прототипів реальних інфраструктурних об'єктів та систем. Проведений аналіз формує фундамент для подальших досліджень в контексті моделювання процесу відновлення інфраструктури з точки зору відпрацювання систем управління задля пом'якшення атак відмови на енергетичні системи.

Стаття висвітлює стан сучасних фреймворків та метрик для оцінки кіберстійкості. Усі вони спеціалізуються на підході Data-driven, а саме на методах експертних оцінок. Тобто, розглядують кіберстійкість як якісний показник. Проте, як демонструють актуальні події у сфері кіберінцидентів даного підходу вже замало. Наразі гостро постає питання необхідності вирішення проблеми оцінювання кіберстійкості на основі моделей, які ґрунтуються на фундаментальних поняття резильєнтності як адаптивній властивості інфраструктурних об'єктів. Таким чином, наступним кроком до створення механізму кількісної оцінки індикатора кіберстійкості реальних об'єктів має стати перехід до підходу Model-driven, тобто до метамоделювання [14-15]. Це вимагає включення загальних понять категорій стійкості до певної структурованої моделі, на основі підходу MOF. А саме вираження концепцій кіберстійкості мовою UML, з подальшою можливістю переходу до рівня кількісної моделі конкретної області (у даному випадку – енергетичного сектору), з подальшим застосуванням інструментів ймовірнісної оцінки параметрів та розрахунку функціональних станів критичних функцій. Наприклад, таких як: Баєсові мережі, або кольорові мережі Петрі.

Список бібліографічного опису:

1. Гальчинський Л., Личик В. (2023). Метрики оцінки кібервідмовостійкості (аналітичне оглядове дослідження). Інформаційні технології та суспільство, 2 (8), 27–33. https://doi.org/10.32689/maup.it.2023.2.3
2. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/44275.
3. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF.
4. Kott, A., & Linkov, I. (2018). Cyber resilience of systems and networks. Springer. / Edited by Alexander Kott, Igor Linkov. 1st ed. Springer International Publishing. doi:10.1007/978-3-319-77492-3.
5. Харламова, К., & Гальчинський, Л. (2022). ОЦІНЮВАННЯ КІБЕРСТІЙКОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ. Collection of scientific papers «SCIENTIA», (November 11, 2022; Vilnius, Lithuania), 118-120.
6. Government of Scotland. (2024). *Cyber Resilience in the Public Sector: Framework for Improving Cyber Resilience*. URL: https://www.gov.scot/publications/scottish-public-sector-cyber-resilience-framework-v2-0/pages/2/
7. Linkov, I. & Palma-Oliveira, J. (eds) (2017) Resilience and Risk: Methods and Application in Environment, Cyber and Social Domains. Springer.
8. Resilience metrics for cyber systems / I. Linkov, D. A. Eisenberg, K. Plourde, T.P. Seager, J. Allen, A. Kott 2013. URL: https://link.springer.com/article/10.1007/s10669-013-9485-y.
9. State Service for Special Communications and Information Protection of Ukraine / Analytical Materials of the SSSCIP. WAR AND CYBER: THREE YEARS OF STRUGGLE AND LESSONS FOR GLOBAL SECURITY, SSSCIP & ICE TASK FORCE, 2025. URL: https://www.cip.gov.ua/ua/statics/analitichni-materiali-derzhspeczv-yazku.
10. Про затвердження Вимог до кіберзахисту інформаційних та керуючих систем атомних станцій для забезпечення ядерної та радіаційної безпеки. URL: https://zakon.rada.gov.ua/laws/show/z0395-22#Text.
11. U.S. Department of Energy (DOE). (2014). *Cybersecurity Capability Maturity Model (C2M2)*. URL: http://energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2.
12. Bodeau, D.J.; Graubart, R.D.; McQuaid, R.M.; Woodill, J. (2018). Cyber Resiliency Metrics, Measures of Effectiveness,and Scoring: Enabling Systems Engineers and Program Managers to Select the Most Useful Assessment Methods;Technical Report; Mitre Corp Bedford Ma Bedford United States: McLean, VA, USA.

13. Bodeau, D.J., Graubart, R.D., McQuaid, R., & Woodill, J. (2018). Cyber Resiliency Metrics and Scoring in Practice-Use Case Methodology and Examples.
14. Bellini, E.; Marrone, S.; Marulli, F. Cyber Resilience Meta-Modelling: The Railway Communication Case Study. Electronics 2021, 10, 583. http:// doi.org/10.3390/electronics10050583
15. Salvi, Andrea & Spagnoletti, Paolo & Noori, Nadia S.. (2021). Cyber-resilience of Critical Cyber Infrastructures: Integrating digital twins in the electric power ecosystem. Computers & Security. 112. 102507. 10.1016/j.cose.2021.102507.

References

1. Galchynsky, L., & Lychyk, V. (2023). Cyber resilience assessment metrics (analytical and review research). Information Technology and Society, (2 (8), 27-33. doi:10.32689/maup.it.2023.2.3 (in Ukrainian).
2. Pro vnesennia zmin do deiakykh zakoniv Ukrainy shchodo zakhystu informatsii ta kiberzakhystu derzhavnykh informatsiinykh resursiv, obiektiv krytychnoi informatsiinoi infrastruktury. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/44275 (in Ukrainian).
3. Pro zatverdzhennia Zahalnykh vymoh do kiberzakhystu obiektiv krytychnoi infrastruktury. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF. (in Ukrainian).
4. Kharlamova, K., & Galchynsky, L. (2022). ASSESSING THE CYBER RESILIENCE OF CRITICAL INFRASTRUCTURE FACILITIES IN UKRAINE. Collection of scientific papers «SCIENTIA», (November 11, 2022; Vilnius, Lithuania), 118-120 (in Ukrainian).
5. Government of Scotland. (2024). Cyber Resilience in the Public Sector: Framework for Improving Cyber Resilience. URL: https://www.gov.scot/publications/scottish-public-sector-cyber-resilience-framework-v2-0/pages/2/.
6. Kott, A., & Linkov, I. (2018). Cyber resilience of systems and networks. Springer. / Edited by Alexander Kott, Igor Linkov. 1st ed. Springer International Publishing. doi:10.1007/978-3-319-77492-3.
7. Linkov, I. & Palma-Oliveira, J. (eds) (2017) Resilience and Risk: Methods and Application in Environment, Cyber and Social Domains. Springer.
8. Resilience metrics for cyber systems / I. Linkov, D. A. Eisenberg, K. Plourde, T.P. Seager, J. Allen, A. Kott 2013. URL: https://link.springer.com/article/10.1007/s10669-013-9485-y.
9. State Service for Special Communications and Information Protection of Ukraine / Analytical Materials of the SSSCIP. WAR AND CYBER: THREE YEARS OF STRUGGLE AND LESSONS FOR GLOBAL SECURITY, SSSCIP & ICE TASK FORCE, 2025. URL: https://www.cip.gov.ua/ua/statics/analitichni-materiali-derzhspeczv-yazku.
10. Pro zatverdzhennia Vymoh do kiberzakhystu informatsiinykh ta keruiuchykh system atomnykh stantsii dlia zabezpechennia yadernoi ta radiatsiinoi bezpeky. URL: https://zakon.rada.gov.ua/laws/show/z0395-22#Text (in Ukrainian).
11. U.S. Department of Energy (DOE). (2014). Cybersecurity Capability Maturity Model (C2M2). URL: http://energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2.
12. Bodeau, D.J.; Graubart, R.D.; McQuaid, R.M.; Woodill, J. (2018). Cyber Resiliency Metrics, Measures of Effectiveness,and Scoring: Enabling Systems Engineers and Program Managers to Select the Most Useful Assessment Methods;Technical Report; Mitre Corp Bedford Ma Bedford United States: McLean, VA, USA.
13. Bodeau, D.J., Graubart, R.D., McQuaid, R., & Woodill, J. (2018). Cyber Resiliency Metrics and Scoring in Practice-Use Case Methodology and Examples.
14. Bellini, E.; Marrone, S.; Marulli, F. Cyber Resilience Meta-Modelling: The Railway Communication Case Study. Electronics 2021, 10, 583. http:// doi.org/10.3390/electronics10050583
15. Salvi, Andrea & Spagnoletti, Paolo & Noori, Nadia S.. (2021). Cyber-resilience of Critical Cyber Infrastructures: Integrating digital twins in the electric power ecosystem. Computers & Security. 112. 102507. 10.1016/j.cose.2021.102507.