УДК 519.7-004.056
DOI https://doi.org/10.32689/maup.it.2023.2.3

Леонід ГАЛЬЧИНСЬКИЙ
кандидат технічних наук, доцент кафедри інформаційної безпеки, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», проспект Берестейський, 37, Київ, Україна, індекс 03056 (hleonid@gmail.com)

ORCID: 0000-0002-3805-1474

Владислав ЛИЧИК
аспірант та асистент кафедри інформаційної безпеки, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», проспект Берестейський, 37, Київ, Україна, індекс 03056 (lychyk.vlad@gmail.com)

ORCID: 0009-0006-3314-6550

Leonid GALCHINSKYI
Candidate of technical sciences, associate professor of the Department of Information Security, National Technical University of Ukraine "Igor Sikorskyi Kyiv Polytechnic Institute", 37 Beresteysky prospect, Kyiv, Ukraine, index 03056 (hleonid@gmail.com)

Vladyslav LYCHYK
PhD student and assistant at the Department of Information Security, National Technical University of Ukraine "Igor Sikorskyi Kyiv Polytechnic Institute", 37 Beresteysky prospect, Kyiv, Ukraine, index 03056 (lychyk.vlad@gmail.com)

Бібліографічний опис статті: Гальчинський Л., Личик В. Метрики оцінки кібервідмовостійкості (аналітичне оглядове дослідження). *Інформаційні технології та суспільство*. 2023. Вип. 2(8). 27–33. DOI: https://doi.org/10.32689/maup.it.2023.2.3

Bibliographic description of the article: Halchynskyi L., Lychyk V. (2023). Metryky otsinky kibervidmovostiikosti (analitychne ohliadove doslidzhennia) [Cyber resilience assessment metrics (analytical and review research)]. *Informatsiini tekhnolohii ta suspilstvo – Information technology and society*, 2(8), 27–33. DOI: https://doi.org/10.32689/maup.it.2023.2.3

МЕТРИКИ ОЦІНКИ КІБЕРВІДМОВОСТІЙКОСТІ (АНАЛІТИЧНЕ ОГЛЯДОВЕ ДОСЛІДЖЕННЯ)

Останні події в Україні та світі поставили гостре питання здатності об'єктів та організацій витримувати належний рівень функціонування, незважаючи на зовнішні кібервпливи та обмеженість ресурсів. Саме тому в сучасних реаліях забезпечення кібервідмовостійкості відіграє надзвичайно важливу роль для цілих секторів промисловості, ІТ-систем та, як показала сучасна гібридна війна – для життєдіяльності цілих держав. Зокрема, кібератаки в енергетичному секторі чи на іншу критичну інфраструктуру можуть впливати не лише на сам сектор, але й на економіку в цілому та всю структуру держави, як на соціальну, так і на організаційну. ***Мета статті*** *полягає у формуванні понятійного апарату кібервідмовостійкості та аналізу метрик для оцінки кібервідмовостійкості. Предметом аналізу та огляду матеріалу для написання статті використовувались провідні* ***методології*** *для оцінки кібервідмостійкості, а саме: методологія групи Лінкова, методологія управління стійкістю CERT (CERT-RMM) та інженерна структура кібервідмовостійкості MITRE.* ***Наукова новизна*** *даної статті полягає у введенні до наукового поля в Україні понятійного апарату та комплексного аналізу метрик кібервідмовостійкості. Виконано співставлення та порівняння провідних метрик для оцінки кібервідмовостійкості.* ***Висновки.*** *У статті інтерпретовано понятійний апарат терміну кібервідмостійкості, досліджено різницю між кібербезпекою та кібервідмовостійкістю. У ході дослідження виявлено, що основні системи та метрики для оцінки кібервідмовостійкості мають досить схожу загальну будову (цілі та домени), однак не є похідними одна від одної. Була проаналізована інженерна структура кібервідмовостійкості та інтерпретована на український варіант загальна матриця стійкості. Пропонується проводити дослідження в напрямі порівняння систем оцінювання кібервідмовостійкості та розробки фреймворків для реальних ІТ-об'єктів в Україні.*

Ключові слова: *кібервідмовостійкість, NIST, MITRE, матриця стійкості, CERT-RMM.*

CYBER RESILIENCE ASSESSMENT METRICS (ANALYTICAL AND REVIEW RESEARCH)

Recent events in Ukraine and the world have raised the acute issue of the ability of facilities and organizations to maintain an adequate level of functioning despite external cyber influences and limited resources. That is why, in today's realities, ensuring cyber resilience plays an extremely important role for entire sectors of industry, IT systems, and, as the modern hybrid war has shown, for the vital activity of entire states. In particular, cyberattacks in the energy sector or on other critical infrastructure can affect not only the sector itself, but also the economy as a whole and the entire structure of the state,

*both social and organizational. The **purpose** of the article is to formulate the conceptual apparatus of cyber resilience and analyze metrics for assessing cyber resilience. The subject of the analysis and review of the material for writing the article were the leading **methodologies** for assessing cyber resilience, namely: the Linkov Group methodology, the CERT Resilience Management Methodology (CERT-RMM) and the MITRE Cyber Resilience Engineering Framework. The scientific novelty of this article is the introduction of the conceptual apparatus and a comprehensive analysis of cyber resilience metrics to the scientific field in Ukraine. The article compares and contrasts the leading metrics for assessing cyber resilience. **Conclusions.** The article interprets the conceptual apparatus of the term cyber resilience, examines the difference between cybersecurity and cyber resilience. In the course of the study, it was found that the main systems and metrics for assessing cyber resilience have a fairly similar general structure (goals and domains), but are not derived from each other. The engineering structure of cyber resilience was analyzed and the general resilience matrix was interpreted for the Ukrainian version. It is proposed to conduct research in the direction of comparing cyber resilience assessment systems and developing frameworks for real IT objects in Ukraine.*

Key words: *cyber resilience, NIST, MITRE, resilience matrix, CERT-RMM.*

Постановка проблеми. Кібервідмовостійкість як поняття має порівняну коротку історію вживання і ще не набула однозначного визнання для української спільноти науковців, спеціалістів з ІТ та кібер-захисту. Цей термін не входить до жодного стандарту України, який би так, чи інакше мав би відношення до використання комп'ютерних та інформаційно-комунікаційних систем. Щоправда, згідно частини другої статті 6 Закону України "Про основні засади забезпечення кібербезпеки України" постановою Кабінету Міністрів України [1] були затверджені *Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури,* в яких записано про доступність та відмовостійкість компонентів та інформаційних ресурсів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури. Термін «відмовостійкість» в цьому офіційному документі вжитий цілком коректно, бо відповідає багатьом стандартам України, зокрема і *ДСТУ 2506-94 Засоби обчислювальної техніки. Відмовостійкість і живучість. Загальні технічні вимоги*. Однак, поняття кібербезпеки стосується не тільки об'єктів критичної інфраструктури, а практично всіх сфер людської діяльності, бо їх функціонування наразі неможливе без використання комп'ютерних та інформаційно-комунікаційних систем. Добре відомо, що в наш час кіберзагрози існують також у всіх сферах, де використовуються комп'ютерні ресурси. Не потребує доведення, що здатність протистояти загрозам залежить не тільки від рівня інформаційної безпеки системи, а має більш широкий контекст. Кібербезпека зосереджена на запобіганні кібератакам та іншим інцидентам безпеки та на мінімізації шкоди, яку вони можуть завдати. Вона включає заходи для запобігання проникненню зловмисників у мережу, такі як брандмауери та антивірусні інструменти, і засоби контролю доступу, а також нетехнічні підходи, як-от навчання користувачів з питань безпеки. Вона також містить стратегії для виявлення поточних загроз і своєчасного реагування на них, щоб обмежити їхній вплив.

Разом з тим в останні роки до багатьох фахівців прийшло розуміння, що хоча кібербезпека залишається ключовою проблемою, вона є лише частиною більшої мети: підтримувати життєдіяльність систем і організацій у належному стані. Виникає питання про відмовостійкість систем в цілому при наявності кіберзагроз. Ця тенденція має загальний характер і стосується також об'єктів ІТ-інфраструктури в Україні. Відповідно, настав час зосередитися на кібервідмовостійкості, зокрема як це поняття зробити корисним, а це в першу чергу залежить від того як можна оцінювати рівень кібервідмовостійкості.

Аналіз останніх досліджень і публікацій. Тематика оцінювання кібервідмовостійкості має більш ніж скромну літературу в українських наукових джерелах і водночас величезну в зарубіжних, причому як на Заході, так і на Сході. Так зокрема в [2] відзначається, що станом на 2020 рік автори з України опублікували тільки одну статтю, порівняно з 73 статтями авторів зі США та 48 статтями авторів з КНР. Слід зазначити, що у всій англомовній літературі існує консенсус щодо терміну *Cyber resilience*, там де ми вживаємо термін *кібервідмовостійкість*.

Мета роботи: сформувати загальний аналітичний огляд стану оцінювання кібервідмовостійкості організацій та систем в контексті зростання рівня кіберзагроз.

Виклад основного матеріалу. Перш ніж вдаватися до аналізу метрик та фреймворків оцінювання кібервідмовостійкості, які на них базуються, розглянемо саме поняття кібервідмовостійкості. На Рис. 1 показана загальна модель відмовостійкості системи, яка втрачає свою функціональність при виникненні деструктивної події, але має здатність за кінечний час відновити принаймні її до певного рівня. Ця модель у загальному вигляді є цілком придатна для систем, які потерпають від кіберзагроз. В науковій літературі існує досить багато визначень поняття кібервідмовостійкості (англ. – Cyber resilience). Автори не претендують на своє визначення цього складного поняття, проте поділяють точку зору тих експертів, які його розуміють як здатність обчислювальної системи об'єкта протистояти, реагувати та відновлюватися після кіберінцидентів, щоб забезпечити безперервність операцій об'єкта [3]. Причому кібервідмовостійкість не слід розглядати як синонім відновлення, а скоріше як синонім здатності

об'єкта знижувати наслідки інцидентів безпеки та досягати запланованих результатів, незважаючи на збій системи чи кібератаку.

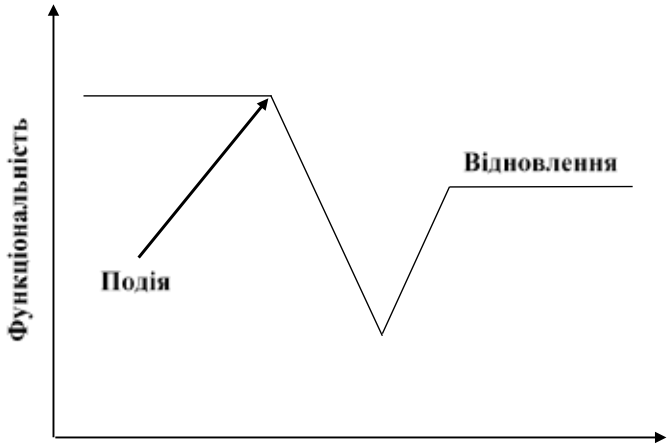


Рис. 1. Модель руйнування функціональності системи при відмовостійкості

Яка різниця між кібербезпекою та кібервідмовостійкістю? У той час як кібербезпека зосереджена на проактивних діях з метою надання допомоги та підтримки компанії в її боротьбі зі зростаючим поширенням кібератак, таких як програми-вимагачі та шкідливе програмне забезпечення, кібервідмовостійкість, зі свого боку, стосується потенціалу, який може мати компанія, щоб максимально обмежити втрати та збитки, відновивши роботу у звичному режимі після кібератаки. Разом з тим ці поняття тісно пов'язані між собою і джерела концепцій кібервідмовостійкісті витікають з понять кібербезпеки.

Інфраструктури кібервідмовостійкості беруть свій початок у структурах кібербезпеки, які розроблені, щоб допомогти організаціям керувати ризиками кібербезпеки. У сфері кібербезпеки домінують два загальні стандарти, які включають заходи, сумісні з підходом до кібервідмовостійкості: серія 27000 стандартів інформаційної безпеки Міжнародної організації зі стандартизації та Рамкова програма кібербезпеки Національного інституту стандартів і технологій.

Узгодження з Британським інститутом стандартів призвело до створення стандарту ISO/IEC 27001 у 2005 році. Сімейство стандартів серії 27000 однозначно не визначає стійкість як одну зі своїх цілей, проте воно рекомендує багато заходів, які сприяють підвищенню кіберстійкості організації. Однак подальший розвиток положень стандарту ISO/IEC 27001 в кібервідмовостійкість не мав належного поширення, як із-за відсутності чіткого розмежування між кібербезпекою та кібервідмовостійкістю, так із-за складної та витратної процедури отримання сертифікату.

Натомість Рамкова система кібербезпеки (CSF) Національного інституту стандартів і технологій(NIST) дає визначення кібервідмовостійкісті і не зв'язує розробників формальними процедурами. CSF версії 1.1 містить п'ять основних функцій:

1. Ідентифікація – завчасний пошук індикаторів впливу, векторів атак, які можна використати, щоб проникнути у IT-екосистему.

2. **Захист** – зменшення вразливих місць відповідно до вашої терпимості до ризику.

3. **Виявлення** – виявлення індикаторів компрометації за допомогою аудиту в реальному часі, виявлення аномалій та попередження.

4. **Відповідь** – швидкий збір та аналіз інформації про інцидент, задля прийняття обґрунтованих рішень щодо найкращого способу дій.

5. **Відновлення** – швидке, точне та ефективне відновлення системи і даних.

Наступна версія NIST CSF 2.0 додала шосту функцію **Керування**. Це наскрізна функція, яка інформує та підтримує інших; наприклад, результати управління визначають пріоритетність засобів контролю безпеки.

Фактично введення функції **Керування** проклало для NIST міст до підтримки структур кібервідмовостійкості, які було реалізовано в документі 800-160 v2 «Розробка кіберстійких систем: підхід до розробки системної безпеки». У ньому детально описано дві важливі та пов'язані концепції структур кібервідмовостійкості: мети та цілі кібервідмовостійкості.

Чотири мети кібервідмовостійкості. Мета – це твердження високого рівня про очікувані результати. Чотири мети, описані в керівництві NIST:

- **Передбачення** – підтримка стану інформованої готовності до негараздів.
- **Витримка** – продовжувати свою важливу місію чи бізнес-функції, незважаючи на труднощі.
- **Відновлення** – здатність відновити свою місію під час та після негараздів, можливо, використовуючи поетапний процес.
- **Адаптація** – кінцева мета – змінити місію організації та їхню підтримку у відповідь на зміни в IT-середовищі та ландшафті загроз.

Цілі кібервідмовостійкості. Цілі – це більш конкретні заяви про очікувані результати. Вони виражені таким чином, щоб полегшити оцінку того, «наскільки добре», «як швидко» або «з яким ступенем впевненості чи довіри» можна досягти мети. Керівництво NIST окреслює вісім цілей кібервідмовостійкості:

1. **Запобігання або уникнення** – запобігання успішному виконанню атаки або реалізації несприятливих умов.
2. **Підготовка –** розуміння того, що негаразди відбудуться, і відповідно, дотримання набору реалістичних реакцій для подолання очікуваних негараздів.
3. **Продовження** – максимізація тривалості та життєздатності основних місій або бізнес-функцій під час труднощів.
4. **Обмеження** – обмеження шкоди від негараздів, завданих цінним активам, таким як ті, що зберігають або обробляють конфіденційну інформацію або підтримують важливі для місії можливості.
5. **Відновлення** – відновлення якомога більше функцій місії чи бізнесу після негараздів, гарантуючи, що відновлені ресурси є надійними.
6. **Розуміння** – підтримка корисного представлення місії та бізнес-залежностей і статусу ресурсів щодо можливих негараздів.
7. **Трансформація** – зміна місії або бізнес-функції та їх допоміжних процесів, щоб краще справлятися з труднощами.
8. **Перебудова** – зміна системи, місії та допоміжної архітектури, щоб ефективніше справлятися з труднощами.

Понятійний апарат NIST дає життєво важливе розуміння цілей і завдань для прийняття інфраструктури кібервідмовостійкості, але не є засобом фактичного впровадження цих цілей і завдань у конкретній організації. Відтак існує потреба в створенні методологій, які дозволяють використати структури кібервідмовостійкості для подальшої розробки конкретних методик оцінювання кібервідмовостійкості організації. Одну з таких методологій надає дослідницька організація MITRE.

Інженерна структура кібервідмовостійкості MITRE. Ідея інженерної структури кібервідмовостійкості MITRE базується на структурах кібервідмовостійкості NIST, забезпечуючи не лише мети та цілі кібервідмовостійкості, але ще й методи кібервідмовостійкості.

Показники кібервідмовостійкості потрібні як основа для прийняття рішень щодо забезпечення життєздатності системи. Показник кібервідмовостійкості є похідним або пов'язаним з деяким елементом інженерної структури кібервідмовостійкості (CREF) – мета, ціль, принцип розробки, техніка або підхід до реалізації техніки. Методологію оцінки кібервідмовостійкості можна використовувати, щоб оцінити, наскільки добре дана система може відповідати своїм оперативним цілям або місії і порівняти альтернативні рішення. Якщо система недостатньо кібервідмовостійка, то для вирішення цієї проблеми спочатку необхідно оцінити рівень кібервідмовостійкості. Очевидно, що це потребує використання показників кібервідмовостійкості – вимірювання, значення, обчислені на основі вимірювань. На Рис. 2 показано вибір і встановлення пріоритетів елементів CREF для даної системи, яка керується за принципами кібервідмовостійкості. Системи підрахунку балів, ранжирування та оцінки надають напівкількісні значення, щоб уможливити порівняння з теоретичним ідеалом або різними альтернативами.

Методологія визначення кібервідмовостійкості (SSM-CR) – це налаштована методологія оцінки, призначена для того, щоб надати менеджерам програм простий відносний показник того, наскільки дана система є кібервідмовостійкою, а також й наскільки різні альтернативи змінюють цей показник.

Визначення системи показників кібервідмовостійкості передбачає вибір показників. SSM-CR, як частина CREF MITRE, корисна тим, що специфікацію метрики можна отримати за допомогою розробленого шаблону [5]. На даний час відомі системи оцінювання кібервідмовостійкості реальних систем, розроблених за методологією CREF MITRE [5]. Є позитивний досвід апробації цих фреймворків на під-

приємствах критичної інфраструктури [6], який проте показав, що необхідні додаткові дослідження. Однак, інженерна методологія MITRE не є монополією в просторі ідей кібервідмовостійкості.

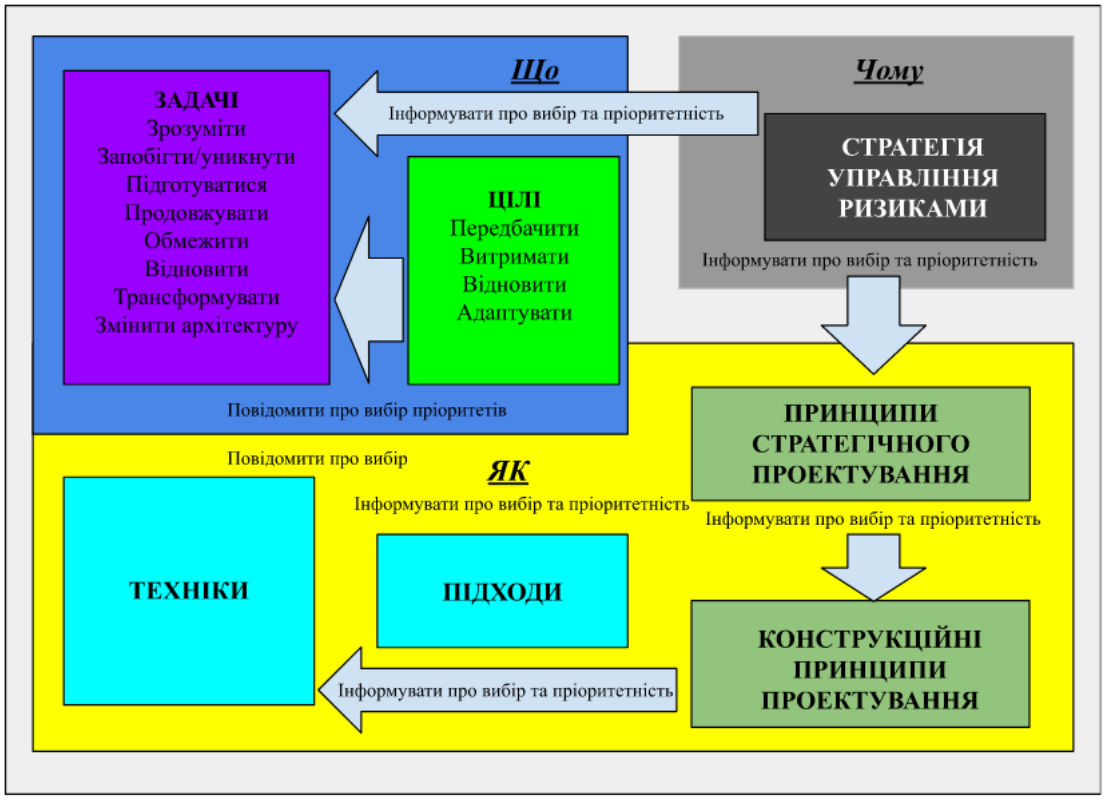


Рис. 2. Інженерна структура кібервідмовостійкості MITRE[4]

Методологія групи Лінкова. Групою дослідників у США, які не були афілійовані тільки з однією установою, проте мали спільні погляди, була представлена суттєво інша методологія визначення кібервідмовостійкості [7]. Як фундаментальні засади цієї методології були взяті з розробки Національної академії наук США (NAS) [8]. Вони полягають в тому, що для систем, які надають критично важливі послуги, стійкість характеризується чотирма здібностями: планувати/готуватися, абсорбувати, відновлюватися та адаптуватися до відомих і невідомих загроз.

З іншого боку для визначення фундаментальних засобів, що дозволять застосувати ці здібності група Лінкова опиралась на дослідження Альбертса [9], яке в загальному вигляді визначило чотири домени в умовах доктрини мережево-центричної війни (network-centric warfare-NCW).

Доктрина NCW визначає чотири домени, які створюють спільний інформаційний ресурс у ситуації, коли необхідне прийняття рішень для підтримки виживання системи:

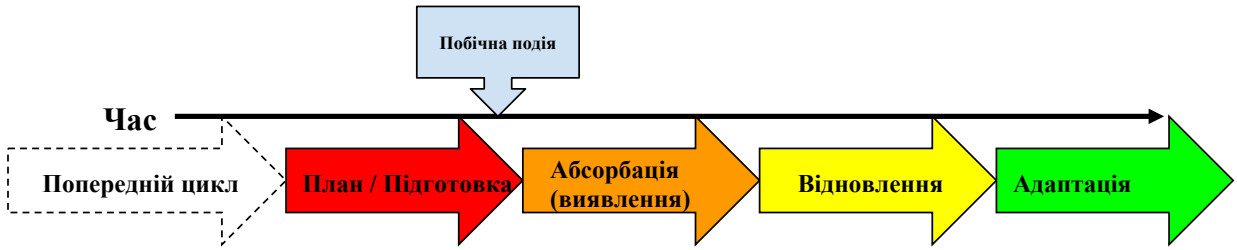
- Фізичний: фізичні ресурси, можливості та дизайн цих ресурсів.
- Інформаційний: інформація та розвиток інформації про фізичну область.
- Когнітивний: використання інформації доменів для прийняття рішень.
- Соціальний: організаційна структура та комунікація для прийняття когнітивних рішень.

В статті[10] співставили визначення чотирьох системних функцій NAS і чотирьох доменів NCW, щоб створити загальну матрицю показників стійкості. Ця матриця, яка у загальному вигляді відображає структуру відмовостійкості будь-яких систем показана в Таблиці 1.

У подальших дослідженнях група Лінкова значно розширила та специфікувала системні функції та домени цієї загальної матриці для застосування структур кібервідмовостійкості, зокрема і для метрик кібервідмовостійкості [10]. Важливо зазначити, що слова «метрика» та «міра» визначаються по-різному. Міра – це кількісний або якісний засіб запису атрибута конкретної системи або компонента системи. Метрика – це засіб для порівняння якості двох або більше систем або системних компонентів шляхом застосування міри. Наприклад, продуктивність системи під час кібервпливу буде метрикою, де швидкість передачі даних через неї буде мірою, пов'язаною з цією метрикою.

Таблиця 1

Матриця стійкості [10]



Фізичний	Стан і можливості обладнання та персоналу; структура мережі.	Розпізнавання подій та продуктивність системи для підтримки функціональності.	Системні зміни для відновлення попередньої функціональності.	Зміни для підвищення стійкості системи.
Інформаційний	Підготовка, представлення, аналіз та зберігання даних.	Оцінка функціональності в режимі реального часу, передбачення каскадних втрат і закриття події.	Використання даних для відстеження прогресу відновлення та прогнозування сценаріїв відновлення.	Створення та вдосконалення протоколів зберігання та використання даних.
Когнітивний	Проектування системи та рішення щодо експлуатації з передбаченням несприятливих подій.	Протоколи дії в надзвичайних ситуаціях та проактивне управління діями.	Комунікація та прийняття рішень щодо відновлення.	Розробка нових конфігурацій системи, цілей та критеріїв прийняття рішень.
Соціальний	Соціальна мережа, громадський капітал, інституційні та культурні норми, навчання	Компетентний персонал, соціальні установи для реагування на події.	Командна робота та обмін знаннями для покращення процесу відновлення системи.	Додавання або зміни інституцій, політик, програм навчання та культури організацій.

Методологія управління стійкістю CERT (CERT-RMM). Деякі інституції, вийшовши за рамки загальних стандартів кібербезпеки, впроваджених в ISO/IEC і NIST, розробили більш спеціалізовані стандарти щодо різних етапів і областей кібервідмовостійкості. Найбільш детальною з них є методологія управління стійкістю CERT (CERT-RMM), розроблена в Університеті Карнегі-Меллона [11]. CERT Resiliency Engineering Framework містить перелік стандартів і кодексів практики, які зазвичай використовуються для цієї мети. В рамках цієї методології інструмент самооцінки, який більше зосереджений на кібер-ризиках доступний на сайті організації, щоб допомогти організаціям оцінити свій рівень кібервідмовостійкісті [12]. Оцінка кібервідмовостійкості ґрунтується на стрункій системі метрик:

- **Атрибут** – характеристика активу, сервісу або процесу стійкості.
- **Основна міра** – кількісно визначає атрибут.
- **Похідні міри** – математична функція двох або більше базових і/або похідних мір.
- **Показники** – критерії для прийняття рішення.
- **Інформаційна потреба** – комбінація показників для прийняття рішення.

Висновки. На основі аналізу наукових джерел було обґрунтовано різницю між кібербезпекою та кібервідмовостійкістю, деталізовано основні функції, цілі та мети кібервідмовостійкості. В наслідок цього інтерпретовано понятійний апарат кібервідмостійкості в контексті кращих сучасних систем для оцінки кібевідмовостійкості, зокрема це: методологія групи Лінкова, методологія управління стійкістю CERT (CERT-RMM) та інженерна структура кібервідмовостійкості MITRE. Для них визначено основні метрики та домени. Розглянуто важливість та актуальність використання даного поняття для українських об'єктів ІТ-інфраструктури. Що стосується **перспектив подальшого дослідження**, то після остаточного формування поняття "кібервідмовостійкості" та визначення основних систем оцінки слід перейти до порівняння їх ефективності. Що в свою чергу дасть можливість адаптувати, застосувати існуючі концепції та створити власну модель кібервідмовостійкості для українських реалій. Паралельно треба розробляти фреймворки для оцінки кібервідмовостійкості реальних об'єктів. Такий досвід дозволить в подальшому створити національний стандарт кібервідмовостійкості. При цьому, можливо,

доведеться уточнити сам термін “кібервідмовостійкость”, більш наближений до до цього поняття в зарубіжній науковій літературі.

Список використаних джерел:

1. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF.
2. Hausken, K. (2020). Cyber resilience in firms, organizations and societies. Internet Things, 11, 100204.
3. Park, J., T.P. Seager, P.S.C. Rao, M. Convertino, and I. Linkov. 2013. Integrating risk and resilience approaches to catastrophe management in engineering systems. Risk Analysis 33(3): 356–367.
4. Bodeau, D.J., Graubart, R.D., McQuaid, R., & Woodill, J. (2019). Cyber Resiliency Metrics and Scoring in Practice-Use Case Methodology and Examples.
5. Scottish Public Sector Action Plan On Cyber Resilience. Cyber Resilience Framework: self-assessment tool user guide. URL: https://www.gov.scot/binaries/content/documents/govscot/publications/adviceand guidance/2019/10/cyber-resilience-framework/documents/cyber-resilience-framework.
6. Харламова, К., & Гальчинський, Л. (2022). ОЦІНЮВАННЯ КІБЕРСТІЙКОСТІ ОБ’ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ. Collection of scientific papers «SCIENTIA», (November 11, 2022; Vilnius, Lithuania), 118-120.
7. Linkov, I.; Eisenberg, D.A.; Bates, M.E.; Chang, D.; Convertino, M.; Allen, J.H.; Flynn, S.E.; Seager, T.P. Measurable Resilience forActionable Policy. Environ. Sci. Technol. 2013, 47, 10108–10110.
8. National Academy of Sciences (2012) Disaster resilience: a national imperative. Washington DC, United States. URL: http://www.nap.edu/catalog.php?record_id=13457.
9. Alberts D (2002) Information age transformation, getting to a 21st century military. DOD Command and Control Research Program. URL: http://www.dtic.mil/get-tr-doc/pdf?AD=ADA457904.
10. 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.
11. Caralli R, Allen J, White D, et al. CERT Resilience Management Model,Version 1.2. Pittsburgh: Carnegie Mellon University, 2016.
12. DHS. Cyber Resilience Review (CRR): Self-Assessment Package.Washington DC: Department of Homeland Security, 2016.

References:

1. Pro zatverdzhennia Zahalnykh vymoh do kiberzakhystu obiektiv krytychnoi infrastruktury [On the approval of General requirements for cyber protection of critical infrastructure objects. Retrieved from https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF] [In Ukrainian].
2. Hausken, K. (2020). Cyber resilience in firms, organizations and societies. Internet Things, 11, 100204.
3. Park, J., T.P. Seager, P.S.C. Rao, M. Convertino, and I. Linkov. 2013. Integrating risk and resilience approaches to catastrophe management in engineering systems. Risk Analysis 33(3): 356–367.
4. Bodeau, D.J., Graubart, R.D., McQuaid, R., & Woodill, J. (2019). Cyber Resiliency Metrics and Scoring in Practice-Use Case Methodology and Examples.
5. Scottish Public Sector Action Plan On Cyber Resilience. Cyber Resilience Framework: self-assessment tool user guide. Retrieved from https://www.gov.scot/binaries/content/documents/govscot/publications/adviceand-guidance/2019/10/cyber-resilience-framework/documents/cyber-resilience-framework.
6. Kharlamova, K., & Galchynskyi, L. (2022). Otsiniuvannia kiberstiikosti obiektiv krytychnoi infrastruktury Ukrainy. [Assessment of cyber resistance of critical infrastructure facilities of Ukraine. Collection of scientific papers «SCIENTIA», (November 11, 2022; Vilnius, Lithuania), 118-120 [In Ukrainian].
7. Linkov, I.; Eisenberg, D.A.; Bates, M.E.; Chang, D.; Convertino, M.; Allen, J.H.; Flynn, S.E.; Seager, T.P. Measurable Resilience for Actionable Policy. Environ. Sci. Technol. 2013, 47, 10108–10110.
8. National Academy of Sciences (2012) Disaster resilience: a national imperative. Washington DC, United States. Retrieved from http://www.nap.edu/catalog.php?record_id=13457.
9. Alberts D (2002) Information age transformation, getting to a 21st century military. DOD Command and Control Research Program. Retrieved from http://www.dtic.mil/get-tr-doc/pdf?AD=ADA457904.
10. Resilience metrics for cyber systems [Electronic resource] / I. Linkov, D. A. Eisenberg, K. Plourde, T.P. Seager, J. Allen, A. Kott – 2013. Retrieved from https://link.springer.com/article/10.1007/s10669-013-9485-y.
11. Caralli R, Allen J, White D, et al. CERT Resilience Management Model,Version 1.2. Pittsburgh: Carnegie Mellon University, 2016.
12. DHS. Cyber Resilience Review (CRR): Self-Assessment Package.Washington DC: Department of Homeland Security, 2016.