УДК 342.951

ФЕДІЄНКО О.П., здобувач наукового ступеня.
ORCID: https://orcid.org/0009-0008-5383-3504.

МІЖНАРОДНІ СТАНДАРТИ ОЦІНКИ КІБЕРСТІЙКОСТІ

DOI…

Анотація. *Визначені типові характеристики кіберстійкості. Деталізовано поняття та зміст кіберстійкості. Окреслено взаємозв`язок між кібербезпекою та кіберстійкістю. Обгрунтовано основні кіберризики, які впливають на стан та процес забезпечення кіберстійкості. Розкрито алгоритми, які впливають на стан забезпечення кіберстійкості. Висвітлено світові методики здійснення оцінки кіберстійкості, зокрема розкрито огляд стану кіберстійкості (Cyber Resilience Review – CRR), індекс кіберсприйняття (The Cyber Resilience Framework – CRF), індекс кіберризику Cyber RiskIndex – CRI. На підставі аналізу кращих практик міжнародного досвіду визначено основну мету проведення оцінки кіберстійкості. Окреслено подальші кроки удосконалення практичного впровадження критеріїв оцінки стану кіберстійкості з метою посилення кібербезпеки та її складових.*

Ключові слова:*кібербезпека, кіберстійкість, кіберзагроза, методика, критерії, оцінка стану кіберстійкості, державна безпекова політика, хакери, кіберзлочинці, операційні системи, відновлення.*

Summary. *The typical characteristics for cyber resilience assessment are defined. The concept and content of cyber resilience are detailed. The link between cyber security and cyber resilience is outlined. The main cyber risks that affect the state and process of cyber resilience are substantiated. Algorithms that affect the state of ensuring cyber resilience are revealed. The global methods of cyber resilience assessment are highlighted, in particular the cyber resilience review (Cyber Resilience Review – CRR), the cyber perception index (The Cyber Resilience Framework – CRF), and the cyber risk index (Cyber Risk Index – CRI) are disclosed. Based on the analysis of the best practices of international experience, the main purpose of the cyber resilience assessment was determined. Further steps with the aim to improve the practical implementation of the criteria for assessing the state of cyber resilience in order to strengthen cyber security and its components are outlined.*

Keywords*: cyber security, cyber resilience, cyber threat, methodology, criteria, cyber resilience assessment, state security policy, hackers, cyber criminals, operating systems, recovery.*

Постановка проблеми. Кіберзагрози постійно та динамічно зростають, а їх ціллю можуть стати інформаційно-комунікаційні системи (далі – ІКТ-системи), технологічні ресурси будь-якої організації у будь-якій країні світу. У глобальних вимірах сучасні моделі управління кіберстійкістю є основою підходу до вдосконалення штатної роботи відповідних ресурсів та ІКТ-систем. Адже на цьому фоні понятійно-категоріальний термін “кіберстійкість” все ще залишається досить непопулярним в сучасному світі кібербезпеки. Активно його почали обговорювати тільки декілька років потому, хоча в світі безпеки цей термін існує вже досить тривалий час. Загалом поняття “кіберстійкість” включає в себе, крім безпеки, низку технічних завдань і процесів, які відносяться до передових інформаційних технологій – наприклад, копіювання, резервування та відновлення інформаційних систем та ресурсів після масштабних програмних збоїв або позаштатних ситуацій. При цьому важливим питанням залишається стійкість функціональності та безперервність роботи відповідних сервісів.

Передумовами для появи кіберстійкості як окремого напрямку стало сприйняття реальності про неминучість, ймовірність, вірогідність проведення кібератак та їхніх

негативних наслідків. Саме завдяки наявності кіберстійкості стає можливим заздалегідь підготуватися до кібератаки, спрацювати на упередження, забезпечити ефективну діяльність і протидію під час самої атаки, а також знизити потенційні та реальні негативні наслідки. На цьому фоні ризики кібератак ще більше посилюються високою залежністю критичної інфраструктури, фінансової системи, державних інформаційних ресурсів та ІКТ-систем від цифрових технологій, наявними труднощами захисту від загроз, що швидко та динамічно змінюються. Тому важливо, щоб уповноважені структури (банки, фінансові установи, об'єкти критичної інфраструктури) мали достатній рівень кіберстійкості задля забезпечення як свого власного захисту, так і захисту всієї екосистеми кібербезпеки.

Хакери та кіберзлочинці постійно шукають навіть крихітну вразливість у програмному забезпеченні за допомогою якої вони можуть зламати навіть потужний та надійний кіберзахист. Зловмисники використовують уразливості в застарілому програмному забезпеченні для розгортання програм-вимагачів і максимальному поширенню шкідливих програм. Найбільшу стурбованість викликають саме атаки з використанням технологій штучного інтелекту. Саме тому кіберстійкість охоплює широкий набір проактивних стратегій, практик і технологій кібербезпеки, спрямованих на локалізацію або мінімізацію впливу несприятливих кіберподій і забезпечення безперервності її функціонування, навіть в умовах масштабних програмних збоїв та нештатних ситуацій. Кіберстійкість може стосуватися як зовнішніх загроз, таких як хакери, кібершпигуни, програми-вимагачі, так і внутрішніх загроз, таких як ризик випадкового видалення або знищення інформації як наслідок "помилки людського фактору". Враховуючи викладене, доцільно розглянути на науково-практичному рівні питання здійснення оцінки стану кіберстійкості на підставі існуючих критеріїв, з урахуванням сучасних тенденцій та кращих практик міжнародного досвіду.

Результати аналізу наукових публікацій. Кіберстійкість як важливу складову національної безпеки певним чином висвітлювали: С. Онищенко, А. Глушко, О. Маслій [1]. Дослідження питань посилення кіберстійкості фінансової системи та банківського сектору перебували у фокусі уваги таких фахівців, як: Н. Трусової та І. Чкан [2], О. Криклія [3]. Методологію оцінки кіберстійкості об'єктів критичної інфраструктури вивчали: І. Мальцева, Ю. Черниш та В. Овсянніков [4], М. Комаров [5]. Оцінювання кіберстійкості через призму ризиків кібербезпеки: С. Гончаров [6], В. Мохор [7], Н. Барченко, В. Любчак та Т. Лаврик [8]. Але жоден із вказаних фахівців ретельно не досліджував світові тенденції встановлення критеріїв оцінки стану кіберстійкості держави та її інформаційних ресурсів, особливо в умовах глобальної кібервійни сучасності.

Метою статті є визначення світових тенденцій встановлення критеріїв оцінки стану кіберстійкості держави та її інформаційних ресурсів.

Виклад основного матеріалу. В умовах масштабування глобальної кібервійни функціонування більшості сучасних державних автоматизованих інформаційних систем, особливо В умовах масштабування глобальної кібервійни функціонування більшості сучасних державних автоматизованих інформаційних систем, особливо тих, що використовують мережеві технології, перебуває у фокусі різноманітних за інтенсивністю деструктивних та негативних впливів.. Зростаюча залежність систем від інформаційних технологій була фундаментальною для управління все більш складними системами та операціями. Складність взаємопов'язаних інформаційних систем призвела до ненавмисного створення деяких уразливостей, які наражають ці системи на кібератаки. Кібератаки вважаються однією з найсерйозніших загроз для державного сектору та бізнесу навколо світу. Організації, які напряму залежать від інформаційних технологій

(далі – ІТ), отримують користь не лише від запобігання кібератакам, але й від швидкого та узгодженого реагування на кібератаки, щоб мінімізувати їх руйнівний вплив на операції. Ця здатність називається кіберстійкістю.

Загальноприйнятим визначенням кіберстійкості є здатність систем захищатися від інцидентів кібератак та підтримувати належний рівень стабільності роботи систем за рахунок забезпечення критичної функціональності та своєчасного поновлення до рівня, який існував перед настанням кіберінцидента. Кіберстійкість являє собою здатність системи швидко та оперативно відновлюватися після кібератак або кіберінцидентів. Слушною є думка О. Копиці та Д. Узлова про те, що визначення пріоритетів у реагуванні на кіберзагрози дозволяє ефективно розподіляти ресурси та здійснювати попереджувальні заходи з кібербезпеки, що значною мірою відображається на стані забезпечення кіберстійкості [9].

За таких умов кіберстійкість особливо актуальна у питаннях забезпечення кібербезпеки, а умовною її мірою є адаптивна здатність чи спроможність реагувати на загрозу, підтримувати належну функціональність систем з метою її стабільної роботи, максимального зниження ризиків кібербезпеки, запобігання тяжким наслідкам від кібератак. Таким чином, цілком логічно враховувати ймовірні ризики для кібербезпеки, які надають змогу оцінити вірогідність настання події та її наслідки, які можуть виникнути на випадок скоєння кібератаки.

На стратегічному рівні розуміння забезпечення кіберстійкості зводиться до покриття збитків, спричинених програмними та іншими збоями із використанням системи попереднього страхування. Однак такий підхід до кіберстійкості має принаймні чотири важливі недоліки. По-перше, страхування покриває лише фінансову компенсацію та за своїм змістом не може покрити не фінансові побічні ефекти кібератаки, такі як втрата ділової репутації або знищення програмного продукту. По-друге, страхування покриває лише певну підмножину небезпек, тоді як малозначна шкода не покривається страховими гарантіями взагалі. По-третє, страхування – це процес, який жодним чином не призводить до зниження ймовірності та вірогідності повторення кібератаки. Нарешті, страхування залишається витратною справою, оскільки навіть якщо кібератаки не відбуваються, вимагається обов`язкова сплата страхових внесків [10].

Проблематика кіберстійкості та її забезпечення набуває актуальності у світових масштабах та глобальних вимірах. Оскільки кіберстійкість розглядається переважно як здатність інформаційних систем здійснювати штатне функціонування в умовах зовнішнього впливу комп’ютерних атак у кіберпросторі, то на цьому фоні ризики кібератак постійно та динамічно зростають: 80 % організацій по всьому світу вважають, що можуть зіткнутися із масштабним витоком даних клієнтів або службової інформації. Управління кіберстійкістю повністю базується на процесах управління ризиками та прив’язане до загальної стратегії розвитку кіберіндустрії. Ця категорія включає: управління кіберризиками, аудит кіберзахищенності, розробку стратегій кібербезпеки тощо.

Враховуючи зазначене, саме оцінка кіберстійкості являє собою важливий елемент здатності підтримувати важливі функції інформаційних систем під час кібератаки. Цей процес включає огляд безпекової політики, процедур та практик кібербезпеки з метою виявлення потенційних уразливостей та ризиків. Це допомагає виявляти проблеми у системах забезпечення кібербезпеки, вживати активні заходи з метою недопущення збоїв у штатній роботі інформаційно-комунікаційних систем та інформаційних ресурсів. Процес оцінки кіберстійкості включає виявлення критичних активів, таких як облікові та персональні данні, системи, мережі, моніторинг заходів, які діють з метою захисту

активів. Ця оцінка включає аналіз контролю доступу, бранмауери, системи виявлення та попередження вторгнень, плани оперативного реагування на кіберінциденти тощо. Процес оцінювання передбачає використання нормативних вимог та галузевих стандартів у цій сфері. Щоб захистити критично важливо активи даних від цифрових загроз та уразливостей, необхідно забезпечити кіберстійкість, яка має бути невід'ємною частиною не тільки технічних систем, але й архітектури кібербезпеки, кіберкоманд, організаційної субкультури.

Загалом в контексті організації кіберстійкості існують такі основні кіберризики: атаки "людина посередині"; програми-вимагачі; фішинг; безфайлові атаки; бот-мережі. Так, наприклад, атака "людина посередині" (*Man-in-the-Middle*) – коли зловмисник здійснює атаку, щоб витягти інформацію з певного з'єднання з Інтернетом. Вони розривають з'єднання на дві частини, створюючи своє власне зашифроване з'єднання між користувачем та сервером, до якого відбувається звернення. Атака формату Man-in-the-Middle вважається застарілою загрозою, оскільки більшість додатків можуть успішно фільтрувати такі спроби перехопити трафік і викрасти ключі. Атака Man-in-the-Middle – це особливий спосіб прослуховування, який передбачає включення третьої сторони в спілкування двох. У комп'ютерному світі таке прослуховування може відбуватися, коли хтось іззовні (насамперед суб'єкт загрози) може бачити пакети, надіслані від клієнта до сервера. Шляхи реалізації цієї атаки, як і можливі прибутки, можуть бути дуже різними – залежно від того, на що розраховують хакери. Більш просунутий приклад атаки MitM – це коли зловмисник не просто викрадає пакети в мережі, але також діє як посередник у з'єднанні між користувачем і сервером. Такий підхід вимагає більш досконалого програмного забезпечення, але значно підвищує ефективність такої атаки. Окрім того, зловмисник також повинен мати повний контроль над мережею – в ідеалі, спеціальну прошивку для роутера.

Підставою для цієї атаки може бути точка доступу, розміщена в людному місці, яка вже має мережу "Wi-Fi". Зловмисник називає свою мережу так само, як легальну, і чекає підключення. Необізнані гості підключаться, вважаючи цю мережу альтернативною тій, яку пропонує заклад. Іноді заклади так дійсно роблять, щоб розвантажити маршрутизатори та дозволити всім гостям користуватися стабільним з'єднанням. Тому таке маскування досить ефективне. Повний доступ до мережі дозволяє шахраям бачити надіслані пакети. Вони отримують усі запити, які клієнт надсилає на сервер, а також відповіді сервера. Отже, коли потенційна жертва намагається підключитися до сервера (тобто відкрити певний сайт) і отримати відкритий ключ, шахраї отримують усі ці запити. Потім вони надсилають ці запити на сервер, видаючи себе за оригінального користувача. Сервер не може відокремити шахрая від законного користувача, тому він просто надсилає відкритий ключ і запитувану інформацію. Таким чином, посередник досить легко прочитає пакети, оскільки вони не були зашифровані.

Фішинг (від англ. *fishing*) – атака, спрямована на те, щоб змусити користувача поділитися конфіденційною інформацією, такою як пароль або номер кредитної картки. Жертва отримує електронний лист або текстове повідомлення, що видає себе за певну особу або організацію, якій жертва довіряє, наприклад, колезі, співробітнику банку або представнику державної установи. Коли одержувач, який нічого не підозрює, відкриває цей електронний лист або повідомлення, він виявляє текст, спеціально розроблений для придушення здорового глузду, який вимагає від потерпілого зайти на сайт і негайно виконати певні дії, щоб уникнути небезпеки або будь-яких серйозних наслідків. Якщо користувач натискає на посилання, він потрапляє на сайт, що імітує законний Інтернет-ресурс. На цьому веб-сайті користувача просять "увійти", використовуючи ім'я

облікового запису та пароль. Якщо він достатньо довіряє і надає згоду, введені дані надходять безпосередньо до зловмисників, які потім використовують їх для крадіжки конфіденційної інформації або грошей з банківських рахунків, а також кіберзлочинці можуть продавати персональні дані на чорному ринку у мережі Даркнет.

Безфайлові атаки (від англ. *filelessattacks*) – це новий тип кібератак, який не використовує традиційні віруси або шкідливі програми, що записуються на жорсткий диск, а замість цього використовує вразливості в операційній системі та її програмах. Ці атаки називаються безфайловими, оскільки зловмисники використовують вбудовані скрипти та інструменти в системі, щоб виконувати свої зловмисні дії, не залишаючи слідів на жорсткому диску. За допомогою безфайлових атак, зловмисники можуть отримати доступ до комп'ютера та мережі, викрадати конфіденційну інформацію, виконувати шпигунські дії, а також розповсюджувати інші шкідливі програми. Ці атаки важко виявляти, оскільки вони не залишають уявних слідів на жорсткому диску, тому можуть залишатися непоміченими протягом тривалого часу. З метою захисту від безфайлових атак, компанії можуть використовувати антивірусні програми та інші захисні механізми, які можуть виявляти та блокувати небезпечні процеси в системі. Також важливо підтримувати всі програми та операційну систему оновленими до останніх версій, щоб усунути вразливості, які можуть використовувати зловмисники.

Бот-мережі (ботнет) – це мережа комп'ютерів, інфікована шкідливим програмним забезпеченням. Кіберзлочинці використовують ботнет-мережі, які складаються з великої кількості комп'ютерів для різних зловмисних дій без відома користувачів. За допомогою ботнетів часто надсилається спам, встановлюються шпигунські програми або здійснюється викрадення облікових даних користувачів. Масштабний ботнет може використовуватися для атак типу DDoS (Distributed Denial of Service) для спрямування додаткового трафіку на сайт та сповільнення роботи або збоїв підключення. Шкідливі програми формату ботнет розповсюджуються за допомогою вкладень електронної пошти та через завантаження файлів і підроблених програм. Зловмисники також націлюються на такі уразливі місця, як своєчасно не оновлене програмне забезпечення та відсутність системного захисту в мережі Інтернет. Все частіше під приціл зловмисників потрапляють камери, смарт-телевізори та навіть електрокари. Загально відомими ризиками, пов'язаними із даними, є нездатність упереджено виявляти атаки нульового дня та нездатність своєчасно зупинити більшість віроломних кібератак. Операційні ризики включають неготовність до боротьби з витоком даних та затримки під час тестування і встановлення виправлень безпеки.

Серед двох основних ризиків для кіберінфраструктури залишаються й Хмарні обчислення. За цим напрямком витрачаються значні ресурси на управління ризиками третіх сторін, таких як постачальники Хмарних послуг. Основні ризики безпеки для IT-інфраструктури включають в себе організаційні невідповідності і складності, а також інфраструктуру Хмарних обчислень та її постачальників. Крім того, серед ключових операційних ризиків є відтік клієнтів, порушення або пошкодження критичної інфраструктури. Серед основних викликів забезпечення готовності реагувати на загрози кібербезпеки є обмежені можливості менеджерів з безпеки, яким не вистачає повноважень та ресурсів, а також труднощі для організацій під час освоєння технологій, достатніх для захисту інформаційних активів та IT-інфраструктури. Наслідки кібератак становлять операційні ризики, до яких відносяться: пошкодження або знищення критичної інфраструктури; зниження показників продуктивності систем та ресурсів; репутаційні збитки тощо. Запобігання кібератакам передбачає вжиття контрзаходів, включаючи кіберпастки (*honeypots*), щоб отримати інформацію про вид або тип атаки.

Виключно суб'єкти з надійною системою кібербезпеки можуть оцінювати ризики, захищатися від них, виявляти загрози, реагувати на кіберінциденти та поновлюватися після потужних кібератак.

Розуміючи масштаби актуалізації питань необхідності посилення кібербезпеки, світова спільнота, останнім часом, переймається питаннями розробки методології та критеріїв оцінки стану кіберстійкості, хоча на міжнародно-правовому рівні ще й досі це питання залишається неурегульованим. Життєво важливою складовою підвищення кіберстійкості є визначення способу її вимірювання. Таким чином, цей процес передбачає визначення кроків, які потрібно зробити. Алгоритми визначення кіберстійкості надають можливість проводити реальну її оцінку та формувати рекомендації щодо найкращих практик, які допомагають підготуватися до негараздів, вистояти, відновитися та адаптуватися до них, від кібератак до стихійних лих. Оцінка кіберстійкості є важливим аспектом та включає готовність будь-якої організації подолати наслідки кібератак. Процес оцінки надає змогу виявляти пробіли у системах кібербезпеки та схвалювати проактивні заходи для їх вирішення.

В сучасній міжнародній практиці існують різні методики оцінки кіберстійкості, однією з яких є Огляд стану кіберстійкості (Cyber Resilience Review - CRR) [11] – сучасна розробка, методологічна документація, видавництва Міністерства внутрішньої безпеки США. Ця оцінка призначена для вимірювання стану кіберстійкості будь-якої структури або організації, а також для проведення аналізу недоліків з метою покращення її стану. Періодичні оцінки планів, безпекових політик і процедур кібербезпеки гарантують, що програми відповідають своїм цілям і готові до використання в разі кібератаки. Огляд стану кіберстійкості – це комплексна оцінка здатності організації протистояти будь-якому кіберінциденту та максимально швидко відновлюватися після нього. Перевірки стану кіберстійкості допомагають організаціям самостійно визначати уразливі та слабкі місця в своїх системах і розробляти плани їх усунення та мінімізації. Завдяки алгоритму CRR здійснюється оцінка корпоративних програм та практик у таких сферах, як: - управління активами; - управління засобами контролю; - управління конфігурацією та змінами; - управління уразливістю; - управління інцидентами; - управління ризиками; - управління залежностями; - управління зовнішніми уразливостями; - навчання та усвідомлюваність; - ситуаційна обізнаність.

Огляд стану кіберстійкості – це оцінка операційної стійкості будь-якої організації та практик кібербезпеки, завдяки якій формується розуміння здатності керувати кіберризиками під час звичайних операцій та під час операційного стресу або настання кризи. Критерії оцінки надають змогу покращити усвідомлення необхідності ефективного управління кібербезпекою, проведення огляду потенційних можливостей, найважливіших для забезпечення безперервності критично важливих послуг під час операційного стресу та кризи; каталізатор для діалогу між учасниками з різних функціональних областей, комплексний підсумковий звіт із використанням визнаних стандартів для визначення відносної зрілості процесів організаційної стійкості в кожному із вказаних 10 доменів.

Огляд стану кіберстійкості – це добровільна експертиза операційної стійкості та практик кібербезпеки, яку використовують оператори критичної інфраструктури. Огляд стану кіберстійкості надає змогу краще зрозуміти поточний стан кібербезпеки тієї чи іншої структури (організації). За наслідками проведення Огляду стає можливим: - поліпшення обізнаності всієї організації щодо необхідності ефективного управління кібербезпекою; - відбувається перевірка успішності організації менеджменту кібербезпеки; - формується комплексний підсумковий звіт, який відображає зрілість процесів організаційної кіберстійкості тощо. Організація може використовувати звіт про перевірку

кіберстійкості з метою створення перспективного плану дій з метою усунення слабких сторін і використання виявлених сильних сторін у питаннях забезпечення кібербезпеки. Одним із базових принципів CRR є використання організацією своїх активів (людей, інформацію, технології та засоби) для підтримки конкретних оперативних місій (або послуг). Оцінка призначена для вимірювання існуючої організаційної стійкості, а також з метою аналізу виявлених прогалин з метою розробки моделей її покращення.

У сучасному світі кіберстійкість визначено як невід'ємну частину не лише технічних систем, але й важливою складовою для людського фактору – команд CERT, організаційної субкультури та щоденних операцій у кіберпросторі. У січні 2022 року за результатами проведення Всесвітнього економічного форуму у Давосі було опубліковано доповідь "Перспективи глобальної кібербезпеки", у якій акцентовано увагу на глибокому і зростаючому розриві у сприйнятті бізнесом і кіберлідерами щодо стійкості до кібербезпеки у світових масштабах, необхідності управління ризиками кібервразливості. При цьому, за матеріалами Всесвітнього економічного форуму визначається два базових компоненти оцінки кіберстійкості: "The Cyber Resilience Framework" - CRF (див. Рис.) та Індекс кіберстійкості "Cyber Risk Index" - CRI [12].

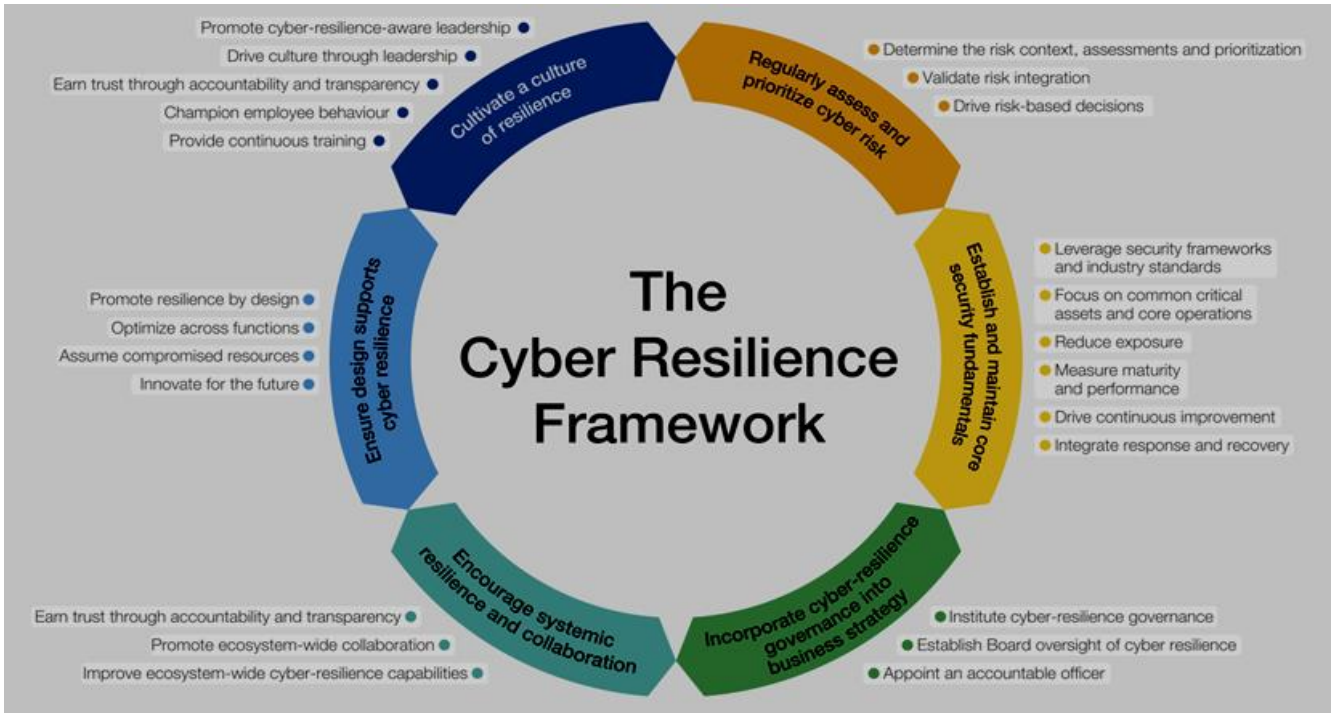

Рис.

Індекс "The Cyber Resilience Framework" (CRF) надає змогу окреслити параметри надійності організаційної кіберстійкості та спрямований на впровадження більш ефективних практик у цифрових екосистемах. CRF пропонує гнучку та чітко визначену основу для встановлення певного рівня розуміння та визначення надійної кіберстійкості в рамках певних операцій. Це сприятиме розповсюдженню кращих практик кіберстійкості в різних галузях. CRF служить вичерпним посібником для впровадження ефективної кіберстійкості, охоплюючи шість фундаментальних принципів, пов'язані з ними практики та їх підпрактики. Завдяки цій структурі кіберлідери мають змогу чітко розуміти наскільки надійною є організаційна кіберстійкість. Основна мета системи кіберстійкості полягає в тому, щоб відповідальні суб'єкти були здатні витримати

кібератаку та швидко компенсувати будь-які завдані збитки. Це може бути встановлення набору вказівок, політик і процедур, яких необхідно дотримуватися з метою організації захисту своїх критичних активів та підтримувати свою діяльність у разі настання кібератаки. CRF також допомагає визначати та оцінювати ризики й вразливості кібербезпеки, впроваджувати ефективні заходи для їх пом'якшення. Одне із основних застосувань структури кіберстійкості – це забезпечення структурованого підходу до управління кіберризиками. Дотримуючись цієї структури можливо оцінити потенційний вплив кібератаки на ці активи та визначити пріоритети своїх зусиль для їх захисту.

Кожен із 6 принципів CRF супроводжується набором практик, які надають можливість кіберспеціалістам розвивати й оцінювати поточний стан кіберстійкості:

- принцип № 1: регулярне оцінювання та визначення пріоритетів кіберризиків;
- принцип № 2: встановлення і підтримка основ безпеки інформаційних систем та ресурсів;
- принцип № 3: інтеграція управління кіберстійкістю в бізнес-стратегію організацій та підприємств;
- принцип № 4: заохочення системної кіберстійкості;
- принцип № 5: гнучкість та адаптованість стратегії кіберстійкості відповідно до викликів та загроз;
- принцип № 6: розвиток субкультури кіберстійкості.

Відповідність принципам і практикам Cyber Resilience Framework вимірюється індексом Cyber Resilience Index. Основна мета CRI – створення оціночного розуміння змісту та завдань кіберстійкості для екосистеми кібербезпеки. Такий механізм надає змогу визначати слабкі місця та стимулює розробляти методологію покращення стану кібербезпеки, щоб досягти наступного рівня стійкості: управляти загрозами та вразливістю систем.

Також у 2022 році було розроблено та схвалено світовою спільнотою показник — "Індекс кіберстійкості", який має на меті стати еталонною одиницею для оцінки дотримання розроблених критеріїв з метою забезпечення видимості практик кіберстійкості в різних галузях. Процес вивчення захищеності компаній від кіберзагроз ускладнюється тим, що відсутні будь-які об'єктивні критерії, за якими можна порівняти. Щоб вирішити цю проблему, Trend Micro спільно з Інститутом Понемона (Ponemon Institute) розробили Індекс кіберризику (Cyber Risk Index – CRI) – методику оцінки захищеності, яка допомагає порівняти рівень захищеності кіберсистем між IT-гігантами. В контексті цього індексу кіберстійкість передбачає здатність будь-якого державного органу або приватної організації долати будь-які ризики, загрози, посягання, збої, небезпеки та виклики для своїх кіберресурсів всередині організації та її екосистеми, архітектури кібербезпеки з метою налагодження безперебійної роботи та гарантування належного рівня кіберзахисту.

Основна мета CRI – надати кіберлідерам інструмент і наочність, щоб зрозуміти рівень стану кіберстійкості своєї організації та системи. CRI розроблено з урахуванням гнучкості та з метою покращення загального стану кібербезпеки. Основним критерієм оцінки стану кіберстійкості є Індекс CRI, Він є довідковою основою для забезпечення кіберстійкості у різних галузях державного та приватного секторів, забезпечуючи загальну основу, практики та механізми для вимірювання ефективності роботи ІКТ-систем, інформаційних ресурсів, комунікаційних та технологічних систем, що забезпечують функціонування органів державної влади. Індекс CRI залишається корисним інструментом, щоб допомогти державному сектору та приватним компаніям краще зрозуміти свої кіберризики. Він являє собою числову шкалу від 10 до 10, де 10 –

найбільший рівень ризику. Поточний глобальний індекс складає – 0,41, що відповідає "підвищеному ризику". Найбільш високий ризик зафіксований в США (– 1,07) за рахунок недостатньої кіберготовності систем захисту від кібератак у порівнянні з іншими регіонами. Індекс кіберризику розраховується як відмінність між індексом кіберготовності (cyber preparedness index) та індексом кіберзагроз (cyber threat index). При цьому індекс кіберготовності демонструє який рівень підготовленості організації до захисту від кібератак, а індекс кіберзагроз представляє стан ланшафту загрози на момент проведення розрахунків.

В сучасних умовах понад 50 країн світу використовують цей індекс для оцінки стану кіберстійкості та його одночасно застосовують для визначення ступеню вразливості з боку загроз кіберзлочинності у показниках від 0 до 1. Індекс кіберризику прогнозує майбутній ризик стати жертвою кіберзлочинності в залежності від країни проживання: чим вищий індекс, тим вищий ризик. Таким чином, компанії по всьому світу можуть використовувати Індекс CRI для визначення пріоритетів своєї стратегії безпеки та зосередження інформаційних ресурсів на оптимальному управлінні кіберризиками. Такі документи стають все більш корисними, оскільки зловмисні інциденти безпеки продовжують залишатися проблемою для підприємств будь-якого розміру та галузей. Оскільки об'єктивних критеріїв, що демонструють рівень захищеності компанії від кібератак, досі що не розроблено, для побудови індексу кіберризику використовується опитування, яке проводиться серед професіоналів у галузі ІТ та ІБ.

У 2023 році до складу включили респондентів із країн Європи та Азіатсько-Тихоокеанського регіону, що дозволяє констатувати, що показник CRI вийшов на глобальний рівень. Результати опитування стали основою для формування індексу, який засвідчує готовність реагувати на кібератаки. Загалом Індекс CRI розраховується як відмінність між Індексом кіберготовності (cyber preparednessindex) та Індексом кіберзагроз (cyber threatindex). Індекс кіберготовності показує, який рівень готовності організації до захисту від кібератак, а індекс кіберзагроз представляє стан ландшафту загроз на момент розрахунку показників. Їхнє поєднання надає змогу на підставі результатів та розрахунку показника CRI мінімізувати ризики, запроваджуючи кращі методи забезпечення безпеки, до яких відносяться: побудова системи безпеки на основі критичних даних шляхом управління ризиками та загрозами, які можуть бути спрямовані на ці дані; мінімізація складності інфраструктури та покращення узгодженості кібербезпеки; покращення існуючих рішень за рахунок використання новітніх технологій для виявлення актуальних загроз, такі як програми-вимагачі та бот-мережі, формування функціональної, динамічної архітектури ІТ-безпеки. Індекс CRI, який розроблений компанією Trend Micro – корисний інструмент для компаній, який надає змогу ефективно розпізнавати існуючі кіберризики. Навколо світу ІТ-компанії можуть використовувати Індекс CRI для покращення стратегії захисту та більш ефективної підготовки своїх засобів захисту від кібератак.

На підставі узагальнення показників за Індексом CRI основними глобальними ризиками кібербезпеки є: неузгодженість та складність ІТ-систем; необережність співробітників; інфраструктура хмарних обчислень та її постачальники; нестача кваліфікованих кадрів; неправомірні дії зловмисників – інсайдерів. Спільне використання Індексів CRF і CRI створюють унікальний тандем загальної оцінки стану кіберстійкості з метою формування переліку можливих загроз у цифрових екосистемах і різноманітних галузях. Завдяки цим показникам компанії та державні органи можуть оцінювати кіберризики, оперативно та адекватно реагувати на кіберінциденти та захищатися від них,

швидко оновлювати систему після скоєних серйозних кібератак. На підставі оціночних показників стає можливим визначити умовну міру сттійкості – адаптивну здатність реагувати на загрозу та підтримувати належну функціональність. Під час оцінки кіберстійкості необхідно враховувати ризики для кібербезпеки, які надають змогу провести оцінку виникнення події та її наслідки, які можуть виникнути у випадку скоєння кібератаки. При цьому, кіберстійкість визначається як здатність системи захищатися від інцидентів кібератак та підтримувати належний рівень продуктивності операційних систем за рахунок підтримки критичної функціональності та своєчасного відновлення до рівня, який існував до кіберінциденту. За наслідками кібератак за результатами проведення оцінки стану кіберстійкості можливі такі сценарії: інформаційні відмови; відмови апаратного забезпечення; відмова взаємодії апаратного та програмного забезпечення.

На підставі комплексної оцінки стану кіберстійкості у подальшому доцільно проводити аудит кібербезпеки – один із ключових елементів у формуванні надійної системи захисту ІТ-інфраструктури як держави так і приватного сектору.

Враховуючи викладене, на наш погляд, завданнями кіберстійкості є: - передбачення, що включає виявлення слабких місць, проведення стратегічного планування на випадок настання загроз, забезпечення можливостей розслідувати наявні вразливості або компрометації; втримання – використання сервісів, систем та ресурсів у період критичності їхніх функцій, організації безперебійної роботи в умовах кібератаки; відновлення, тобто запуск процесів, які нададуть змогу оновити стан, який був до скоєння кібератаки, при цьому важливо, щоб відновлення автоматично не оновлювало кіберзагрозу; адаптація – це адекватне реагування на постійно динамічний ландшафт кіберзагроз, організація штатної роботи систем та ресурсів в надзвичайних або критичних умовах. За таких умов після кіберінциденту та його розслідування доцільно внести зміни до системи оповіщення, що називається налаштуваннями видимості. Саме завдяки кіберстійкості має потенційно зменшитися кількість помилкових реакцій та спрацьовувань, які можуть значно сповільнити якісну роботу ІТ-систем.

Висновки.

Кіберстійкість є важливою складовою екосистеми кібербезпеки, що означає управління кіберризиками та впровадження дієвих заходів системного кіберзахисту. З цією метою в експертному середовищі активно використовується єдина таксономія кіберінцидентів як інструмент для обміну інформацією щодо таких та шкала для вимірювання їхньої критичності, заснована на загальному підході. Для світової ІТ-спільноти революційним здобутком стала поява індексів кіберстійкості, який надає змогу на підставі об`єктивних критеріїв проводити оцінку та порівняння стану загроз в контексті забезпечення та гарантування кіберстійкості, визначати перспективні шляхи удосконалення.

Методи та показники оцінки кіберстійкості – це адаптовані ресурси для допомоги системним адміністраторам державних структур та приватного сектору, менеджерам програм та іншим особам, які підтримують управління кіберризиками. Система підрахунку балів і набір кількісно-якісних показників мають лише значення в контексті програмних та інженерних рішень, для припущення щодо визначення ризику (зокрема, припущення щодо кіберзагроз, а також припущення щодо збоїв у штатній роботі). Оцінки та показники виробляються під час аналізу і надають змогу формувати рішення щодо подальшої необхідності посилення стану кібербезпеки. Результатами проведення оцінки стану кіберстійкості є сприятлива можливість порівнювати стан кіберзахищенності певної компанії або державного органу між собою.

Основна мета проведення оцінки кіберстійкості – мінімізація кіберризиків, запровадження кращих методик забезпечення кібербезпеки, до яких відносяться: побудова системи безпеки на основі критичних даних шляхом концентрації уваги на управлінні ризиками та загрозами; мінімізація ризиків для ІТ-інфраструктури; перевірка існуючих рішень безпеки з використанням сучасних технологій для виявлення актуальних загроз, таких як програми-вимагачі та бот-мережі; формування функціональної та динамічної безпеки інформаційних систем та кібербезпеки.

Беручи до уваги поточну ситуацію щодо викликів та ризиків, узагальнюючи результати, отримані у процесі розрахунку індексу CRI, стає можливим значно мінімізувати кіберризики, запроваджуючи кращі методики забезпечення кібербезпеки шляхом: побудови системи безпеки на основі аналізу критичних даних шляхом управління ризиками та загрозами; мінімізації складності інфраструктури та покращення узгодженості з усіх безпекових питань; швидка адаптація до змін ландшафту кіберзагроз; перевірка існуючих рішень у сфері кібербезпеки із використанням новітніх технологій для виявлення актуальних загроз; формування функціональної та динамічної інфраструктури ІТ-безпеки.

Для України в умовах війни одним із найважливіших завдань державної безпекової політики є забезпечення кіберстійкості об’єктів критичної інформаційної інфраструктури, національних інформаційних ресурсів, комунікаційних та технологічних систем. Активне використання в Україні сучасної методології та світових індексів для проведення оцінки стану кіберстійкості надасть змогу значно посилити стан забезпечення кібербезпеки на державному рівні, надасть сприятливі можливості та розуміння зменшення уразливості ІТ-систем та ресурсів за наслідками кібератак, які здійснює держава-агресор, а також мотивовані Кремлем хакери та кіберзлочинці.

Розуміючи актуалізацію питань забезпечення кіберстійкості Постановою Кабінету Міністрів України від 08.03.24 р. № 276 було затверджено положення про Міжвідомчу робочу групу з питань залучення міжнародної допомоги для забезпечення кібербезпеки та кіберстійкості держави [13]. Міжвідомча робоча група з питань залучення міжнародної допомоги для забезпечення кібербезпеки та кіберстійкості держави є тимчасовим консультативно-дорадчим органом Кабінету Міністрів України. Нормативно встановлено, що основними завданнями Міжвідомчої робочої групи є сприяння забезпеченню координації дій органів виконавчої влади з питань організації взаємодії із урядами іноземних держав та міжнародними організаціями в частині залучення міжнародної допомоги з метою забезпечення кібербезпеки та кіберстійкості держави, а також у започаткуванні та реалізації проектів (програм) міжнародної технічної допомоги щодо підвищення рівня кіберстійкості державних інформаційних ресурсів.

Використана література

1. Онищенко С.В. Глушко А.Д., Маслій О.А. Кіберстійкість як основа національної безпеки України. *Innovations and prospects of world science:* Proceedings of XI International Scientific and Practical Conference, Vancouver, Canada, 22-24 June 2022. Vancouver: Perfect Publishing, 2022. P. 551-556. URL: https://reposit.nupp.edu.ua/bitstream/PoltNTU/10642/1/INNOVATIONS-AND-PROSPECTS-OF-WORLD-SCIENCE-22-24.06.22-551-556.pdf

2. Трусова Н.В, Чкан І.О. Кіберзахист банківської системи України в умовах цифрової трансформацій: *збірник наукових праць Таврійського державного агротехнологічного університету імені Дмитра Моторного (економічні науки)*. 2023. № 47. Т. 1. С. 151-163. URL: https://oj.tsatu.edu.ua/index.php/zbirnyk/article/view/538/510

3. Криклій О.А. Теорія та практика забезпечення кіберстійкості банків. *Ефективна економіка*. 2020. № 10. URL: http://www.economy.nayka.com.ua/pdf/10_2020/52.pdf

4. Мальцева І.Р., Черниш Ю.О., Овсянніков В.В. Аналіз методик оцінки кіберстійкості критичної інфраструктури. *Кібербезпека: освіта, наука, техніка.* 2021. № 12. Т. 4. С. 29-35. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/250/224

5. Комаров М.Ю, Гончар С.Ф, Дімітрієва Д.О. Дослідження проблеми кіберживучості об`єктів критичної інформаційної інфраструкутури. *Ядерна та радіаційна безпека.* 2021. № 1(89). С. 59-66.

6. Гончар С.Ф. Оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури: монографія. Київ: "Альфа Реклама", 2019. 176 с.

7. Мохор В.В., Гончар С.Ф., Дибач О.М. Методи оцінки сумарного ризику кібербезпеки об'єктів критичної інфраструктури. *Ядерна та радіаційна безпека.* 2019. № 2 (82). С. 4-8.

8. Барченко Н.Л., Любчак В.О., Лаврик Т.В. Модель індикаторів оцінки національного рівня цифровізації та кібербезпеки держав світу. *Кібербезпека: освіта, наука, техніка.* 2022. № 2(18). С. 73-85.

9. Копиця О., Узлов Д. Методи визначення категорій кіберінцидентів та оцінки ризиків інформаційної безпеки. *Комп'ютерні науки та кібербезпека.* 2024. № 2. С. 33-42.

10. Daniel A. Estay. A systematic review of cyber-resilience assessment frameworks. *Computers & Security*. 2020. V. 97. URL: https://doi.org/10.1016/j.cose.2020.101996; https://www.sciencedirect.com/science/article/abs/pii/S0167404820302698?via%3Dihub

11. Cyber Resilience Review (CRR). URL: https://www.cisa.gov/resources-tools/services/cyber-resilience-review-crr

12. The Cyber Resilience Framework and Index: A Blueprint to Improve the Organization's Cyber Attack Defendability. URL: https://www.nopsec.com/resources/whitepapers-ebooks/the-cyber-resilience-framework-and-index-a-blueprint-to-improve-the-organizations-cyber-attack-defendability/

13. Про утворення Міжвідомчої робочої групи з питань залучення міжнародної допомоги для забезпечення кібербезпеки та кіберстійкості держави: Постанова Кабінету Міністрів України від 08.03.24 р. № 276. URL: https://zakon.rada.gov.ua/laws/show/276-2024-%D0%BF#n36

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~