КОНЦЕПТУАЛЬНІ ЗАСАДИ ТА ОСНОВНІ ХАРАКТЕРИСТИКИ КІБЕРСТІЙКОСТІ КОМПАНІЙ

CONCEPTUAL FRAMEWORK AND BASIC FEATURES OF THE COMPANY'S CYBER RESILIENCE

У статті проаналізовано сучасні наукові дослідження, що стосуються кіберстійкості в різних секторах економіки, з метою виявлення прогалин в існуючих підходах, а також наголошено на важливості інтеграції принципів кіберстійкості на всіх рівнях управління організацією. Розглянуто ключові виклики, з якими стикаються організації, такі як підвищена вразливість до кіберзагроз через технологічну залежність. Відсутність структурованого підходу до управління кіберзагрозами, що призводить до реактивного реагування, фінансових втрат та операційних перебоїв, визначено як основну проблему. Запропоновано авторське бачення кіберстійкості, наголошуючи на інтеграції адаптивних та інноваційних рішень. Представлено багаторівневу модель «Вежі стійкості», що охоплює технічні, організаційні та стратегічні аспекти. Висновки спрямовані на обґрунтування практичних інструментів та методологій, які допоможуть підвищити здатність компаній ефективно протидіяти сучасним кіберзагрозам та підтримувати свою конкурентоспроможність.

Ключові слова: *стійкість, кіберстійкість, кібербезпека, загрози, адаптивність, ризики, інновації, діджиталізація, технології, захист.*

The study analyzes the key aspects of cyber resilience in the modern digital environment, identifies the main challenges faced by companies, and substantiates the need to create a conceptual framework for effective cyber resilience. The author has reviewed current research on cyber resilience in various sectors of the economy, identified gaps in existing approaches, and determined the importance of integrating cyber resilience principles at all levels of organizational management. Particular attention is paid to the concept of resilience in the context of geopolitical conflicts, which strengthen the role of cyber threats as a tool for influencing the economy. The author reveals connections between cyber resilience and technological innovations, including Artificial Intelligence, IoT, cloud computing, and Blockchain, which not only create new opportunities, but also add complexity to systems and increase their vulnerability. Existing approaches to cybersecurity, including traditional methods such as antivirus protection and attack detection systems, are assessed as not effective enough in response to dynamic and complex threats. The author emphasizes the importance of transitioning to adaptive and dynamic solutions that take into account the specifics of modern risks and ensure the ability of companies to quickly recover from incidents. The emphasis is placed on the Resilience Tower multi-level model that covers technical, organizational, and strategic aspects. The importance of creating a culture of cyber resilience, which should combine technological, organizational, and strategic solutions, is emphasized. The conclusions suggest practical tools and methodologies that will help improve the ability of companies to effectively counter modern cyber threats and maintain their competitiveness. Such an approach should be general enough to cover a wide range of approaches, as well as specific and novel enough to be different from existing approaches, in particular, from classical risk management.

Key words: *resilience, cyber resilience, cybersecurity, threats, adaptability, risks, innovation, digitalization, technology, protection.*

УДК 004.056:005.511

DOI: https://doi.org/10.32782/dees.15-47

Омельченко Н.О.[1]
Віцепрезидентка,
ТОВ «ІТ-Інтегратор»;
викладачка,
Бізнес-школа «МІМ-Київ»

Omelchenko Nadiia
IT-Integrator LLC;
MIM-Kyiv Business School

Постановка проблеми. У цифровому середовищі, що швидко розвивається, компанії все більше покладаються на технології для ведення бізнес-операцій, управління даними та взаємодії зі стейкхолдерами. Однак ця залежність посилює їхню вразливість до кіберзагроз, зокрема витоку даних, атак з вимогами викупу та системних збоїв. Незважаючи на критичний характер цих ризиків, багатьом компаніям бракує чіткої концептуальної основи та практичних інструментів для розробки ефективних стратегій кіберстійкості.

Відсутність структурованого та дієвого підходу призводить до фрагментарного або реактивного реагування на кіберінциденти, що робить компанії вразливими до фінансових втрат, репутаційних збитків та операційних простоїв. Крім того, багатьом організаціям важко впроваджувати практичні заходи, такі як моніторинг загроз у режимі реального часу, навчання співробітників, планування реагування на інциденти та інтеграція кіберстійкості в процеси забезпечення безперервності бізнесу.

Динамічний характер кіберзагроз, зумовлений розвитком технологій і витонченістю зловмисників, ще більше ускладнює завдання. Це вимагає не лише концептуальної основи, але й набору практичних, адаптивних заходів, які забезпечать організаціям можливість ефективно протистояти кібератакам, відновлюватися після них та адаптуватися до них. Це дослідження спрямоване на усунення цих прогалин шляхом вивчення концептуальних засад, ключових особливостей та основних характеристик, необхідних для розуміння кіберстійкості компанії, з метою подальшого обґрунтування стратегій її посилення.

Аналіз останніх досліджень і публікацій. Результати досліджень теоретичних та практичних аспектів кіберстійкості компанії, специфіки кіберстійкості в різних секторах економіки, а також особливості управління розкриті в наукових

[1] ORCID: https://orcid.org/0009-0005-8635-8883

працях іноземних (у більшості) та вітчизняних (у меньшості) вчених. Так Халт Г. і Сіванесан Дж. у своєму дослідженні наводять історичний розвиток у контексті кібербезпеки й описують, який вигляд має ефективна кіберстійкість [1]. Котт А. та Лінков І. оцінюють кіберстійкість систем і мереж, досліджуючи відмінність між безпекою, ризиком та стійкістю [2]. Автори описують наявні та можливі майбутні практики й методи забезпечення кіберстійкості, враховуючи технічні питання. З іншої сторони Андерсон Р. та ін., у своєму досліджені враховуючи економічні фактори і політику, оцінюють те, як інформаційна безпека повинна координуватися між членами Європейського Союзу [3]. Аннареллі А., та Паломбі Г. досліджують концептуальні можливості цифровізації для посилення кіберстійкості та визначають, що фундамент стійкості бізнесу, який полягає у підтримці конкурентоспроможності при одночасному забезпеченні безпеки бізнесу, вже не є «плюсом» або привабливим реченням, а реальною і послідовною потребою для всіх організацій [4].

Що стосується українських вчених, то слід зазначити, що загальні питання стійкості досліджуються не системно, наприклад Пирожков С., Божок Є., та Хамітов Н. здійснили ідентифікацію сутності національної стійкості (резильєнтність) країни в контексті формування стратегії і тактики випередження гібридних загроз [5]. Інша група вчених, а саме Загірняк Д., Данилко В., Іщенко С. та Лига Д. дослідили особливості діяльності підприємств в умовах нестабільного зовнішнього середовища, коли основне завдання підприємства – збереження стратегічної стійкості. За отриманими результатами було визначено основні відмінності між економічною і стратегічною стійкістю [6]. Сподіна А. та Тарасенко О. на основі аналізу теоретичних напрацювань дослідили сутність поняття «фінансова стійкість підприємства» як динамічної інтегральної характеристики, що характеризує спроможність підприємства як системи трансформувати ресурси та ризики, повноцінно виконувати свої функції [7], а Пікуліна О. з групою однодумців проаналізували вплив зовнішньої заборгованості на фінансову стійкість та національну економічну безпеку України, та визначили масштаби залежності української економіки від міжнародних кредиторів [8].

Питання кіберстійкості були розглянуті в роботах Гончар С. з Комаровим М., та групою науковців під керівництвом Іванченко Є. в контексті дослідження підходів до оцінки кіберстійкості об'єктів критичної інформаційної інфраструктури [9; 10]. А також через визначення теоретичного підґрунтя кіберстійкості у контексті еволюційного розвитку концепції стійкості в роботі Користіна О. та Демедюка С. [11]. В досліджені Столбового В. та Кисленко Д. було визначенно ключові заходи щодо посилення кіберстійкості/кібербезпеки на державному та корпоративному рівнях з урахуванням сучасного стану діджиталізації суспільства [12]. В свою чергу Криклій О. здійснив обґрунтування концепції забезпечення кіберстійкості банків у банківській сфері зважаючи на негативний фінансовий та нефінансовий вплив кібератак на банківську систему та економіку країни в цілому [13].

Отримані опрацьовування складають теоретичну та методологічну основу для проведення даного дослідження. Також проведений попередній аналіз показав, що наявні результати були отримані за іншими умови, які значно відрізняються від початку другої чверті XX ст. А саме в умовах геополітичних конфліктів, коли кіберзагрози стають інструментом впливу на економіку та бізнес-середовище. Тому не заперечуючи вагомості існуючих наукових результатів, слід зазначити, що ідентифікація концептуальних основ кіберстійкості компанії вимагає більш поглибленого дослідження. Особливо враховуючі те, що підвищення її рівня дозволить українським компаніям ефективніше захищати виробничі процеси, мінімізувати фінансові втрати та підтримувати стабільність функціонування в умовах російсько-української війни та подальшого повоєнного відновлення економіки країни.

Постановка завдання. Метою статті є визначення концептуальних засад та ідентифікація основних характеристик кіберстійкості компаній. Отримані результати будуть сприяти обґрунтуванню практичних інструментів формування культури кіберстійкості на всіх рівнях управління вітчизняного бізнесу.

Виклад основного матеріалу дослідження. В другому десятилітті XXI ст. кожна організація має IT-систему та потребу в інструментах кібербезпеки для захисту інформації та діджиталізованих процесів від спроб шахрайства та актів вандалізму. Функціональність цієї системи побудована відповідно до складності та рівня діджиталізації бізнесу, а також цінності, яку він приносить соціальному та економічному контексту [14]. Останні десять років хакерство, бомбардування, вторгнення та інфікування становлять реальну небезпеку для багатьох країн, їхніх громадян, бізнесу та світової економіки в цілому, і їм можна протистояти шляхом впровадження кіберстійкої системи. Здатність реагувати на ці атаки, а також розробляти та впроваджувати більш надійну організацію нагадує концепцію стійкості, відому у фізиці як припущення про те, що система може витримувати аварії без руйнувань. В управлінських науках стійкість визначається як здатність організації адаптуватися до несподіваних руйнівних змін або внутрішня здатність системи змінювати своє функціонування до, під час і після руйнівних змін або неприємностей, щоб мати можливість продовжувати необхідні операції як в очікуваних, так і в несподіваних умовах.

Концептуальні основи та основні характеристики кіберстійкості компаній формують основу для забезпечення їхньої здатності функціонувати в умовах сучасних кіберзагроз. За результатами проведеного попереднього аналізу було визначено, що в світовій науці було сформовано теоретичне підґрунтя для традиційної оцінки ризиків, що включає в себе розрахунок добутку загроз, вразливостей і наслідків для небезпек і їх подальшого впливу [15]. Але у сфері кібербезпеки, а й відповідно кіберстійкості, як наступної сходинки управління, оцінка ризиків стає обмеженою, оскільки необхідні підходи для усунення загроз і вразливостей, які стають інтегрованими в широкий спектр взаємозалежних обчислювальних систем та супутньої архітектури [16; 17].

Для дуже складних та взаємопов'язаних економічних систем стає надзвичайно складно провести оцінку ризиків, яка б адекватно враховувала потенційні каскадні ефекти, що можуть виникнути через збій або втрати, які поширюються на інші системи. Крім того, непередбачуваність, надзвичайна невизначеність та швидка еволюція потенційних кіберзагроз роблять зусилля з оцінки ризиків ще більш нездатними адекватно реагувати на проблеми кібербезпеки критично важливих інфраструктурних систем. Саме тому кіберстійкість означає здатність системи готуватися, поглинати, відновлюватися та адаптуватися до несприятливих впливів, особливо тих, що пов'язані з кібератаками. З іншої сторони термін «кіберстійкість» можна визначити як здатність безперервно досягати запланованих результатів, незважаючи на несприятливі кіберподії [18]. Ми ж вважаємо, що термін «кіберстійкість» слід використовувати для позначення переважно властивості стійкості економічної системи, а також позначення особливостей або компонентів конкретної структурної одиниці системи, яка забезпечує кіберстійкість. Отже кіберстійкість визначається як здатність компанії ефективно передбачати, протистояти, швидко відновлюватися та адаптуватися до кіберзагроз, атак чи компрометації систем, зберігаючи безперервність бізнес-процесів та захист даних. Це включає як технічні заходи, так і організаційні стратегії, спрямовані на забезпечення стійкості до кіберризиків у динамічному середовищі. Це поняття є ключовим для підтримки бізнес-процесів і мінімізації ризиків в умовах динамічного розвитку технологій Індустрії 4.0, таких як штучний інтелект, хмарні обчислення, IoT, Blockchain, Big Data та інші. Висока структурна складність сучасних кіберсистем, їхні вразливості та загрози, пов'язані зі «сплячими» цифровими бомбами, роблять їх уразливими до масових кібератак.

Сучасні методи кібербезпеки, включаючи антивірусний захист, сканери вразливостей, системи виявлення та попередження атак, виявляються недостатньо ефективними для забезпечення необхідного рівня захисту. Класичні підходи до забезпечення надійності, такі як структурне резервування, реконфігурація систем та N-кратне резервування, не відповідають потребам сучасного кіберпростору. Замість цього потрібен перехід до адаптивних і динамічних рішень, що враховують складність сучасних загроз.

Концептуальні основи кіберстійкості включають кілька ключових елементів. Конструкт кіберстійкості охоплює методи, завдання, принципи проектування, які формують системний підхід до забезпечення стійкості. Контроль кіберстійкості базується на впровадженні заходів безпеки, таких як моніторинг, тестування та розробка протоколів реагування, спрямованих на досягнення цілей стійкості. Принципи проектування включають вибір рішень, що забезпечують надійність, гнучкість і адаптивність системи. Підходи до реалізації кіберстійкості включають інтеграцію сучасних технологій, що дозволяють створювати адаптивні системи, здатні до швидкого відновлення після атак.

Основні характеристики кіберстійкості визначають її практичну реалізацію (рис. 1). Адаптивність забезпечує здатність систем змінювати стратегії відповідно до нових загроз, передбачати потенційні

Рис. 1. Основні характеристики кіберстійкості

Джерело: складено автором

вразливості та оперативно реагувати на виклики. Гнучкість дозволяє системам продовжувати функціонувати навіть у разі серйозних порушень, забезпечуючи мінімізацію втрат. Непередбачуваність систем додає додатковий рівень захисту, ускладнюючи дії зловмисників і знижуючи ефективність атак. Надійність досягається завдяки побудові архітектур без єдиної точки відмови та використанню резервних механізмів, що забезпечують безперервність операцій. Інтегрованість кіберстійкості з фізичними та людськими системами створює комплексний захист, що враховує всі аспекти роботи компанії. Динамічність дозволяє швидко адаптуватися до нових викликів, включаючи зміни векторів атак і впровадження нових технологій. Цілісність систем спрямована на захист критичних даних і забезпечення їхньої недоторканності, уникаючи втрат чи спотворень інформації.

Сучасні інформаційні системи мають динамічний дизайн, що створює сприятливий ґрунт для зловмисників, які знаходять нові режими збоїв і вектори атак. Висока вартість особистої та фінансової інформації, а також даних про безпеку, робить їх привабливою ціллю для кіберзловмисників. Їхня втрата або викрадення можуть призвести до катастрофічних наслідків для бізнесу. Змагальний характер кіберзагроз підкреслює необхідність урахування адаптивності зловмисників, які постійно вдосконалюють свої методи атак, щоб обійти захисні заходи.

Три основні компоненти стратегії кібербезпеки дозволяють ефективно реагувати на сучасні виклики. Оборонні заходи включають традиційні методи захисту, такі як обмеження доступу, базова кібергігієна та виправлення помилок. Проактивні заходи передбачають створення фальшивих баз даних або мережевих з'єднань для відволікання зловмисників, а також потенційно ризиковані превентивні дії, спрямовані на нейтралізацію загроз. Ретроактивні заходи використовуються для оцінки збитків і виявлення недоліків системи, зокрема через криміналістичні методи або моніторинг витоку даних.

Успішна інтеграція кіберстійкості в бізнес-процеси компанії передбачає поєднання захисних механізмів із бізнес-стратегіями. Організації повинні визначити свою схильність до ризику, інвестуючи у превентивні заходи, які відповідають їхнім цінностям і пріоритетам. Збалансованість між захистом, реагуванням і відновленням є критично важливою для забезпечення безперервності бізнесу навіть у кризових ситуаціях.

Дослідження показують, що недоінвестування в кіберстійкість часто є наслідком надмірної самовпевненості або недооцінки реальних ризиків [19; 20]. Це вимагає зміни підходів, спрямованих на проактивне впровадження рішень, що дозволяють компаніям ефективно функціонувати навіть у нестабільному середовищі. Наприклад, використання адаптивних систем, які постійно вдосконалюються, забезпечує стійкість до нових і непередбачуваних викликів. Інтеграція стандартів, таких як ISO/IEC 27000, забезпечує основи для побудови систем, що відповідають міжнародним вимогам і забезпечують необхідний рівень захисту.

Високий рівень кіберстійкості також вимагає залучення всіх рівнів організації, включаючи керівництво, співробітників та зовнішніх партнерів. Це дозволяє інтегрувати кібербезпеку в бізнес-планування, що, своєю чергою, сприяє підвищенню загальної ефективності системи та забезпеченню стійкості бізнесу. Організації повинні зосередитися на розробці стратегій, які не лише відповідають поточним викликам, а й здатні передбачати майбутні ризики. Але з іншої сторони значним обмеженням для рішень у сфері кібербезпеки є те, що багато рішень, як минулих, так і теперішніх, є суто реактивною реакцією на відомі вразливості та атаки. Тобто вже по факту появи загрози. Це призводить до впровадження рішень, які зменшують ці вразливості, використовуючи такі методи, як виправлення, шифрування та брандмауери, але все одно залишають чутливі системи вразливими до виявлених атак. Крім того, інноваційні рішення, що використовувалися для вирішення минулих проблем безпеки, можуть швидко застаріти, оскільки технології вдосконалюються та розвиваються. Покладання на класичну методологію підвищення кібербезпеки призвело до того, що дехто називає «гонкою озброєнь» [21; 22; 23; 24].

Розширення концепцій кіберстійкості в умовах Четвертої промислової революції стає все більш актуальним. Використання інноваційних інформаційно-комунікаційних технологій є основою для функціонування критично важливих систем у фінансових центрах, охороні здоров'я, уряді, армії та інших секторах. Водночас основним обмеженням сучасних підходів є те, що багато рішень є реактивною відповіддю на виявлені вразливості. Це створює потребу в фундаментальному перегляді стратегій, що передбачає впровадження багаторівневих систем, здатних до адаптації та забезпечення стабільності в умовах постійних змін. При цьому головним питанням залишається захист будь яких даних компанії. Врахування ключових характеристик кіберстійкості та викликів глобальної цифровізації дозволяє нам запропонувати модель «Башти стійкості», яка є структурованим підходом до забезпечення стійкості організації в умовах викликів та змін (рис. 2). Вона характеризується багаторівневим підходом, що охоплює базові елементи, такі як технології та процеси, а також стратегічні аспекти, зокрема управління й інновації. Всі компоненти моделі є взаємопов'язаними, що створює єдину інтегровану систему забезпечення стійкості. Вона

Рис. 2. Модель «Башти стійкості»

Джерело: складено автором

є гнучкою, що дозволяє адаптуватися до нових умов і викликів. Цей підхід ідеально підходить для компаній, які прагнуть ефективно протистояти викликам, забезпечувати стабільність та зміцнювати свої позиції на ринку.

Згідно цієї моделі майбутнє кіберстійкості полягає у використанні багатофункціональних систем, які поєднують складність і стабільність. Ці системи повинні бути непередбачуваними для зловмисників і одночасно стабільними для користувачів. Вони мають забезпечувати адаптацію до змін, порушуючи кіберцикл, у якому зловмисники використовують вразливості, а захисники постійно намагаються їх усунути. У підсумку кіберстійкість стає не лише захистом, а й стратегічною перевагою, яка дозволяє компаніям ефективно конкурувати та розвиватися у сучасному цифровому світі.

Зазначимо, що кіберстійкість зачіпає бізнес, окремих людей, уряди тощо. Дійові особи вбудовані одна в одну й обирають стратегії, засновані на переконаннях та перевагах, які впливають на кіберстійкість і чинять на неї вплив. Суб'єкти, які не становлять загрози і прагнуть набути кіберстійкості, відрізняються від суб'єктів, які чинять загрози. Дійові особи володіють ресурсами, компетенцією, технологіями та інструментами. Вони роблять вибір, який впливає на кіберстійкість усіх учасників, включно з ними самими. Кіберстійкість пов'язана з кіберстрахуванням через вхідні вимоги або попередні умови для укладення кіберконтрактів, потреба в різних послугах, таких як реагування на інциденти, збір даних, та обмеження в покритті. Кіберстійкість пов'язана з Інтернетом речей, який, як очікують, має спростить життя завдяки штучному інтелекту та машинному навчанню, але водночас буде вразливим через велику поверхню атаки, недостатній рівень технологій, складну роботу з даними, можливу високу довіру до комп'ютерів і програмного забезпечення, а також етичні норми.

Висновки. В другій чверті XXI ст. кіберстійкість стає ключовим фактором для забезпечення безперервності бізнес-процесів в умовах постійного зростання кількості та складності кіберзагроз. Вона визначається як здатність організацій адаптуватися до несприятливих умов, включаючи кібератаки, та продовжувати досягати запланованих результатів. Традиційні підходи до кібербезпеки, такі як антивірусний захист і системи виявлення атак, виявляються недостатньо ефективними для протидії новим викликам. Це потребує переходу до адаптивних і динамічних рішень, які враховують складність сучасних загроз і мінімізують потенційні втрати. Основними компонентами кіберстійкості є надійність, адаптивність, гнучкість, інтегрованість і динамічність систем. Успішна інтеграція кіберстійкості в бізнес-процеси передбачає збалансованість між захистом, реагуванням та відновленням. Отже підсумовуючі аналіз наявних теоретичних та практичних напрацювань в обраній площині дослідження, слід зазначити, що в цілому бракує загальної та адаптованої до конкретних умов методологічного підходу, що є відтворюваним, сертифікованим і піддаватися аудиту, зокрема, щоб зробити його практично застосовним та науково прийнятним. Такий підхід має бути

достатньо загальним, щоб охоплювати широкий спектр підходів, а також достатньо специфічним та новим, щоб відрізнятися від існуючих підходів, зокрема, від класичного управління ризиками. Він повинен враховувати як сучасний стан науки, так і найкращі практики в світі, а також широко відкривати двері для вкрай необхідних подальших інновацій в управлінських рішеннях щодо розвитку кіберстійкості. Саме цьому будуть присвячені подальші дослідження авторів.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Hult F., Sivanesan G. What good cyber resilience looks like. *Journal of business continuity & emergency planning*. 2014. Vol. *7*(2). P. 112–125. URL: https://www.ingentaconnect.com/contentone/hsp/jbcep/2014/00000007/00000002/art00004
2. Kott A., Linkov,I. (Eds.). *Cyber resilience of systems and networks* (Vol. 1). New York, NY: Springer International Publishing. URL: https://link.springer.com/book/10.1007/978-3-319-77492-3
3. Anderson R., Bohme R., Clayton R., Moore T. *Security economics and the internal market.* 2018. URL: https://www.enisa.europa.eu/publications/archive/economics-sec/
4. Annarelli A., Palombi G. Digitalization capabilities for sustainable cyber resilience: a conceptual framework. *Sustainability.* 2021. Vol. 13(23). 13065. DOI: https://doi.org/10.3390/su132313065
5. Пирожков С.І., Божок Є.В., Хамітов Н.В. Національна стійкість (резильєнтність) країни: стратегія і тактика випередження гібридних загроз. *Вісник НАН України*. 2021. № 8. С. 74–82. URL: http://dspace.nbuv.gov.ua/handle/123456789/181385
6. Загірняк Д., Данилко В., Іщенко С., Лига Д. Стратегічна стійкість в умовах глобалізації економіки як антикризовий інструмент. *Вісник Національного технічного університету «Харківський політехнічний інститут» (економічні науки)*. 2020. Вип. 3. С. 98–101. DOI: https://doi.org/10.20998/2519-4461.2020.3.102
7. Сподіна А.О. Тарасенко І.О. Фінансова стійкість підприємства: сутність та фактори впливу. *Міжнародний науковий журнал «Інтернаука»*. 022. №12(131). С. 24–31. URL: https://www.inter-nauka.com/uploads/public/16704889827423.pdf#page=25
8. Пікуліна О., Огданський К., Пікуліна,Н. Аналіз впливу зовнішньої заборгованості на фінансову стійкість та національну економічну безпеку України. *Економіка та суспільство*. 2023. Вип. 56. DOI: https://doi.org/10.32782/2524-0072/2023-56-2
9. Гончар С.Ф., Комаров М Ю. Підходи до оцінки кіберстійкості об'єктів критичної інформаційної інфраструктури. *SIST-2021*, 2012. 43. URL: http://bit.nau.edu.ua/wp-content/uploads/2021/07/Zbirnyk-tez-Koblevo-2021.pdf#page=43
10. Ivanchenko Y., Korchenko O., Zarytskyi O., Zybin S., Vishnevska N. Аналіз поняття кіберстійкості критичної інфраструктури. *Ukrainian Information Security Research Journal*. 2023. Vol. 25(4). P. 221–233. DOI: https://doi.org/10.18372/2410-7840.25.18228
11. Користін О.Є., Демедю, С.В. Актуалізація кіберстійкості та історичні витоки концепції «стійкість». *Аналітично-порівняльне правознавство*. 2023. Вип. 6. С. 708–713. DOI: https://doi.org/10.24144/2788-6018.2023.06.122
12. Столбовий В.М., Кисленко Д.П. Заходи з підвищення кібербезпеки на державному та корпоративному рівнях в умовах діджеталізації суспільства. *Scientific notes of Lviv University of Business and Law*. 2023. Vol. 37. P. 175–183. URL: https://nzlubp.org.ua/index.php/journal/article/view/802
13. Криклій О.А. Теорія та практика забезпечення кіберстійкості банків. *Ефективна економіка*. 2020. № 10. DOI: https://doi.org/10.32702/2307-2105-2020.10.50
14. Von Solms R., Van Niekerk J. From information security to cyber security. *Computers & security*. 2013. Vol. *38*. P. 97–102. DOI: https://doi.org/10.1016/j.cose.2013.04.004
15. Kaplan S., Garrick B.J. On the quantitative definition of risk. *Risk analysis*. 1981. Vol. 1(1). P. 11–27. DOI: https://doi.org/10.1111/j.1539-6924.1981.tb01350.x
16. Malatji M., Marnewick A.L., Von Solms S. Cybersecurity capabilities for critical infrastructure resilience. *Information and Computer Security*, 2022. Vol. 30 No. 2, pp. 255–279. DOI: https://doi.org/10.1108/ICS-06-2021-0091
17. DiMase D., Collier Z. A., Heffner K., Linkov I. Systems engineering framework for cyber physical security and resilience. *Environment Systems & Decisions*, 2015. Vol. 35(2). P. 291. URL: https://link.springer.com/article/10.1007/s10669-015-9540-y
18. Björck F., Henkel M., Stirna J., Zdravkovic J. Cyber Resilience – Fundamentals for a Definition. In: Rocha, A., Correia, A., Costanzo, S., Reis, L. (eds) New Contributions in Information Systems and Technologies. *Advances in Intelligent Systems and Computing*. 2015. Vol. 353. DOI: https://doi.org/10.1007/978-3-319-16486-1_31
19. Cyber Risk and CFOs: Over-Confidence is Costly 2022 Edition. URL: https://www.kroll.com/-/media/kroll-images/pdfs/cyber-risk-cfos-report.pdf
20. Half of France's Data Swiped in Viamedis and Almerys Cyber Attack. *EM360.* URL: https://em360tech.com/tech-articles/half-frances-data-swiped-viamedis-and-almerys-cyber-attack#:~:text=Viamedis%20and%20Almerys%20Breached,access%20to%20its%20internal%20systems
21. Armstrong R., Mayo J., Siebenlist F. Complexity science challenges in cybersecurity. *Sandia National Laboratories SAND Report*. 2009. URL: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=ec5f02125bd83e8d0cb03a7d26e72575160199c3
22. McMorrow, D. Science of cyber-security. *MITRE Corporation report*. JASON, MITRE Corporation, McLean, VA, Tech. Rep. 2010. URL: https://apps.dtic.mil/sti/pdfs/ADA534220.pdf
23. Lin H.S., Goodman S.E. *Toward a safer and more secure cyberspace*. Committee on Improving Cybersecurity Research in the United States, National Academy of Engineering, Washington, D.C., Tech.

Rep. 2007. URL: https://nap.nationalacademies.org/catalog/11925/toward-a-safer-and-more-secure-cyberspace

24. Seetharaman A., Patwa N., Jadhav V., Saravanan A.S., Sangeeth, D. Impact of Factors Influencing Cyber Threats on Autonomous Vehicles. *Applied Artificial Intelligence.* 2020. Vol. 35(2). P. 105–132. DOI: https://doi.org/10.1080/08839514.2020.1799149

REFERENCES:

1. Hult F., Sivanesan G. (2014). What good cyber resilience looks like. *Journal of business continuity & emergency planning*, vol. *7*(2), pp. 112–125. Available at: https://www.ingentaconnect.com/contentone/hsp/jbcep/2014/00000007/00000002/art00004

2. Kott A., Linkov I. (2019)Cyber resilience of systems and networks New York, NY: Springer International Publishing, vol. 1. Available at: https://link.springer.com/book/10.1007/978-3-319-77492-3

3. Anderson R., Bohme R., Clayton R., Moore T. (2008). Security economics and the internal market. Available at: https://www.enisa.europa.eu/publications/archive/ economics-sec/

4. Annarelli A., Palombi G. (2021). Digitalization capabilities for sustainable cyber resilience: a conceptual framework. *Sustainability*, vol. 13(23), 13065. DOI: https://doi.org/10.3390/su132313065

5. Pyrozhkov S.I., Bozhok Ye.V., Khamitov N.V. (2021). Natsionalna stiikist (rezylientnist) krainy: stratehiia i taktyka vyperedzhennia hibrydnykh zahroz [National stability (resilience) of the country: strategy and tactics of preempting hybrid threats]. *Visnyk NAN Ukrayiny*, no. 8, pp. 74–82. Available at: http://dspace.nbuv.gov.ua/handle/123456789/181385

6. Zahirniak D., Danylko V., Ishchenko S., Lyha D. (2020) Stratehichna stiikist v umovakh hlobalizatsii ekonomiky yak antykryzovyi instrument [Strategic stability in the context of economic globalization as an anti-crisis tool. Bulletin of the National Technical University "Kharkiv Polytechnic Institute" (Economic Sciences)]. *Visnyk Natsionalnoho tekhnichnoho universytetu "Kharkivskyi politekhnichnyi instytut" (ekonomichni nauky)*, vol. 3, pp. 98–101. DOI: https://doi.org/10.20998/2519-4461.2020.3.102

7. Spodina A., Tarasenko I. (2022) Finansova stiykist pidpryyemstva: sutnist ta faktory vplyvu [Financial sustainability of an enterprise: essence and factors of influence]. *Mizhnarodnyy naukovyy zhurnal "Internauka"*, no. 12 (131), pp. 24–31. Available at: https://www.inter-nauka.com/uploads/public/16704889827423.pdf#page=25

8. Pikulina O., Ogdanskyi K., Pikulina N. (2023). Analiz vplyvu zovnishn'oyi zaborhovanosti na finansovu stiykist ta natsionalnu ekonomichnu bezpeku Ukrayiny [Analysis of the impact of external debt on financial sustainability and national economic security of Ukraine]. *Ekonomika ta suspilstvo*, no. 56. DOI: https://doi.org/10.32782/2524-0072/2023-56-2

9. Honchar S., Komarov M. (2021) Pidkhody do otsinky kiberstiykosti ob'yektiv krytychnoyi informatsiynoyi infrastruktury [Approaches to assessing the cyber resilience of critical information infrastructure objects]. *SIST-2021*, no. 43. Available at: http://bit.nau.edu.ua/wp-content/uploads/2021/07/Zbirnyk-tez-Koblevo-2021.pdf#page=43

10. Ivanchenko Y., Korchenko O., Zarytskyi O., Zybin S., Vishnevska N. (2023). Analiz ponyattya kiberstiykosti krytychnoyi infrastruktury [Analysis of the concept of cyber resilience of critical infrastructure]. *Ukrainian Information Security Research Journal*, vol. 25(4), pp. 221–233. DOI: https://doi.org/10.18372/2410-7840.25.18228

11. Korystin O. E., Demediuk S. I. (2023). Aktualizatsiya kiberstiykosti ta istorychni vytoky kontseptsiyi "stiykist' [An update on cyber resilience and the historical origins of the concept of "resilience"]. A*nalitychno-porivnyal'ne pravoznavstvo*, no. 6, pp. 708–713. DOI: https://doi.org/10.24144/2788-6018.2023.06.122

12. Stolbovy V., Kislenko D. (2023). Zakhody z pidvyshchennya kiberbezpeky na derzhavnomu ta korporatyvnomu rivnyakh v umovakh didzhetalizatsiyi suspil'stva. [Measures to increase cyber security at the state and corporate levels in the context of digitalization of society]. *Scientific notes of Lviv University of Business and Law*, no. 37, pp. 175–183

13. Kryklii O. (2020) Teoriya ta praktyka zabezpechennya kiberstiykosti bankiv [Theory and practice of ensuring cyber resilience of banks]. *Efektyvna ekonomika*, no. 10. DOI: https://doi.org/10.32702/2307-2105-2020.10.50

14. Von Solms R., Van Niekerk J. (2013). From information security to cyber security. *Computers & security*, vol. *38*, pp. 97–102. DOI: https://doi.org/10.1016/j.cose.2013.04.004

15. Kaplan S., Garrick B.J. (1981). On the quantitative definition of risk. *Risk analysis*, vol. 1(1), pp. 11–27. DOI: https://doi.org/https://doi.org/10.1111/j.1539-6924.1981.tb01350.x

16. Malatji M., Marnewick A.L., Von Solms S. (2022) Cybersecurity capabilities for critical infrastructure resilience. *Information and Computer Security*, vol. 30, no. 2, pp. 255–279. DOI: https://doi.org/10.1108/ICS-06-2021-0091

17. DiMase D., Collier Z.A., Heffner K., Linkov I. (2015). Systems engineering framework for cyber physical security and resilience. *Environment Systems & Decisions*, vol. 35(2), p. 291. Available at: https://link.springer.com/article/10.1007/s10669-015-9540-y

18. Björck F., Henkel M., Stirna J., Zdravkovic J. (2015). Cyber Resilience – Fundamentals for a Definition. In: Rocha, A., Correia, A., Costanzo, S., Reis, L. (eds) New Contributions in Information Systems and Technologies. Advances in Intelligent Systems and Computing, vol 353. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-16486-1_31

19. Cyber Risk and CFOs: Over-Confidence is Costly 2022 Edition. Available at: https://www.kroll.com/-/media/kroll-images/pdfs/cyber-risk-cfos-report.pdf

20. Half of France's Data Swiped in Viamedis and Almerys Cyber Attack. *EM360.* Available at: https://em360tech.com/tech-articles/half-frances-data-swiped-viamedis-and-almerys-cyber-attack#:~:text=Viamedis%20and%20Almerys

%20Breached,access%20to%20its%20internal%20systems

21. Armstrong R., Mayo J., Siebenlist F. (2009). Complexity science challenges in cybersecurity. *Sandia National Laboratories SAND Report*. Available at: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=ec5f02125bd83e8d0cb03a7d26e72575160199c3

22. McMorrow D. (2010). Science of cyber-security. *MITRE Corporation report*. JASON, MITRE Corporation, McLean, VA, Tech. Rep. Available at: https://apps.dtic.mil/sti/pdfs/ADA534220.pdf

23. Lin H.S., Goodman S.E. (2007). Toward a safer and more secure cyberspace. Committee on Improving Cybersecurity Research in the United States, National Academy of Engineering, Washington, D.C., Tech. Rep. Available at: https://nap.nationalacademies.org/catalog/11925/toward-a-safer-and-more-secure-cyberspace

24. Seetharaman A., Patwa N., Jadhav V., Saravanan A.S., Sangeeth D. (2020) Impact of Factors Influencing Cyber Threats on Autonomous Vehicles. *Applied Artificial Intelligence*, vol. 35(2), pp. 105–132. DOI: https://doi.org/10.1080/08839514.2020.1799149