КІБЕРСТІЙКІСТЬ БІЗНЕСУ ЯК ФАКТОР СТАЛОГО РОЗВИТКУ КОМПАНІЇ

CYBER RESILIENCE OF BUSINESS AS A FACTOR OF SUSTAINABLE COMPANY DEVELOPMENT

У статті досліджено кіберстійкість бізнесу як інтегральний управлінський феномен та ключовий чинник сталого розвитку компаній у цифрову епоху. Визначено, що традиційні підходи до інформаційної безпеки, побудовані на превентивних і реактивних заходах, виявляються недостатніми для протидії сучасним викликам. За результатами дослідження «Cyber Resilience 2025» встановлено, що компанії, які формують основу економіки та водночас є найбільш уразливими до кіберризиків, характеризуються наявністю базових політик безпеки, але демонструють низький рівень операційної дисципліни, системності відновлення та незалежної валідації захисту. Запропоновано секторальні «дорожні карти» для CEO та CISO, що відображають ключові ризики та пріоритетні управлінські рішення для різних галузей (енергетика, фінанси, промисловість, ритейл, освіта). Зроблено висновок, що кіберстійкість є системоутворюючиі фактором сталого розвитку бізнесу, адже забезпечує здатність організацій зберігати функціональну цілісність і досягати стратегічних цілей навіть в умовах кризи.

Ключові слова: *кіберстійкість, управління ризиками, сталий розвиток, корпоративне управління, бізнес-стратегії, цифрова трансформація, управлінські інструменти, міжнародні практики.*

The article explores business cyber resilience as an integrated managerial phenomenon and a crucial factor in sustainable company development in the digital era. It is argued that traditional approaches to information security, based on preventive and reactive measures, are insufficient to counter modern cyber threats. Instead, cyber resilience is positioned as a new managerial paradigm encompassing technical, organizational, legal, and strategic dimensions aimed at ensuring business continuity, protecting critical assets, and maintaining stakeholder trust. Based on the analysis of international and national initiatives, the study identifies the fragmentation of existing approaches to assessing and implementing cyber resilience, in particular the lack of methodologies adapted to the needs of executives without technical expertise. In this context, a conceptual and categorical framework for cyber resilience management is proposed, including key concepts, models, principles, control methods, and managerial decisions integrated into strategic, tactical, and operational planning. Special attention is devoted to the empirical survey "Cyber Resilience 2025" conducted among Ukrainian companies under wartime economic conditions. The results demonstrate that small and medium-sized enterprises, which constitute the backbone of the national economy yet remain the most vulnerable to cyber risks, usually adopt basic security policies but reveal low levels of operational discipline, recovery testing, and independent validation of protection. This highlights the urgent need for applied managerial tools that combine simplicity of use with the capacity to integrate cyber resilience into corporate strategies. The article further introduces sectoral "roadmaps" for CEOs and CISOs, outlining major risks and priority managerial responses across industries such as energy, finance, manufacturing, retail, and education. It is shown that embedding cyber resilience into corporate governance and decision-making not only minimizes the consequences of cyber incidents but also serves as a driver of innovation, productivity, and long-term competitiveness. The study concludes that cyber resilience should be regarded as a system-forming factor of sustainable business development, as it enables organizations to preserve functional integrity and achieve strategic goals even under conditions of digital turbulence and cyber threats.

Key words: *cyber resilience, risk management, sustainable development, corporate governance, business strategies, digital transformation, management tools, international practices.*

УДК 004:005.511:[330.34:334.72

DOI: https://doi.org/10.32782/dees.19-62

Омельченко Н.О.[1]
Віцепрезидентка,
ТОВ «ІТ-Інтегратор»;
Викладачка,
Бізнес-школа «МІМ-Київ»
Дугінець Г.В.[2]
д.е.н., професор,
Державний торговельно-економічний університет

Omelchenko Nadiia
IT-Integrator LLC;
MIM-Kyiv Business School
Duginets Ganna
State University of Trade and Economics

Постановка проблеми. У добу цифрової трансформації кіберстійкість стала стратегічним фактором безпеки та розвитку бізнесу. Вона визначає здатність компанії протидіяти технічним загрозам, зберігати стабільність і довгострокову конкурентоспроможність. Цифровізація бізнес-процесів спричинила зникнення понад половини компаній зі списку Fortune 500 з 2000 року [1]. Вже в 2004 році, за даними Всесвітнього економічного форуму, 91% CEO називали кіберінциденти головною загрозою, а 43% опитаних відзначали зростання складності атак [2].

В умовах російсько-української війни проблема загострюється: протягом 2022–2023 років зафіксовано понад 2 500 складних атак на критичну інфраструктуру [3], що ставило під загрозу безперервність бізнесу. Більшість із них мали ознаки гібридного впливу і були спрямовані на критичну інфраструктуру, що прямо впливає на можливість забезпечення безперервності бізнесу. Але для того, щоб управління кіберстійкістю перетворилося з відокремленого технічного питання на бізнес-питання, його необхідно мати можливість кількісно оцінити в грошовому

[1] ORCID: https://orcid.org/0009-0005-8635-8883
[2] ORCID: https://orcid.org/0000-0003-3708-3666

еквіваленті, інтегрувавши в систему управління ризиками компанії.

Світова практика свідчить про те, що є окремі управлінські та технологічні рішення, проте залишається не опрацьований системний підхід до побудови та підтримки кіберстійкості компаній як фактору її сталого розвитку. Оскільки в науковій літературі домінують технократичні моделі, в той час як розгляд кіберстійкості як категорії стратегічного управління і детермінанти стійкості компаній в умовах високої волатильності залишаються фрагментарними. Саме необхідність інтеграції принципів кіберстійкості у стратегії сталого розвитку компаній, яка потребує міждисциплінарного підходу і визначає актуальність обраного напряму дослідження.

Аналіз останніх досліджень і публікацій. Результати досліджень теоретичних і прикладних аспектів кіберстійкості компаній, її галузевої специфіки, особливостей управління та ролі в забезпеченні сталого розвитку можна поєднати в декілька груп. Так найбільша група науковців, а саме Coutu D., Халіна В., Абєлєнцев Є., Користін О., Демедюк С., Von Solms R., & Van Niekerk J., Björck F., Henkel M., Stirna J. та Zdravkovic J. окреслюють концептуальне розуміння резильєнтності, а саме її моделі, типологію та етапи розвитку поняття формуючи таким чином єдине теоретичне поле для подальших прикладних досліджень [4–8]. У межах корпоративного управління науковці приділяють значну увагу збереженню стратегічної стійкості підприємств у нестабільному середовищі, а саме Sabatino M., Загірняк Д., Данилко В., Іщенко С. та Лига Д. визначенню відмінності між економічною та стратегічною стійкістю [9; 10], Сподіна А., Тарасенко І.та Криклій О. ідентифікації сутність фінансової стійкості підприємства як інтегрального показника адаптаційної спроможності [11; 12]. В свою чергу Лібанова Е. зосереджуються на впливі різних типів криз (економічних, політичних, екологічних і кіберзагроз) на резильєнтність компаній, а також висвітлюють її конкретні наслідки: швидкість відновлення операцій, мінімізацію збитків, вплив на стратегічний розвиток та корпоративну культуру [13]. Окрему групу становлять роботи, що досліджують цифровізацію як основу кіберстійкості, а саме Ткаченко І., Hult F., Sivanesan G. Kott A. та Linkov I. [14–16]. Проведений огляд показує, що кіберстійкість дедалі частіше розглядається як детермінанта довгострокової стійкості бізнесу, його конкурентоспроможності та інноваційної активності. Проте системні підходи до оцінки кіберстійкості та інтеграції її показників у систему управління ризиками залишаються недостатньо розробленими, що формує наукову нішу для подальших міждисциплінарних досліджень.

Постановка завдання. Метою статті є поглиблення теоретичних положень, обґрунтування науково-практичних рекомендацій щодо управління кіберстійкістю компанії та вдосконалення цих процесів як передумови сталого розвитку компанії.

Виклад основного матеріалу дослідження. В сучасних умовах цифровізації, зростання взаємозалежностей і зростаючого рівня кіберризиків, традиційні підходи до забезпечення інформаційної безпеки, що базуються на превентивних та реактивних заходах, є недостатніми для захисту критичних функцій компаній. У зв'язку з цим, кіберстійкість постає як нова управлінська парадигма, що поєднує технічні, організаційні та стратегічні компоненти з метою забезпечення здатності компанії ідентифікувати загрози, адаптуватися до цифрових викликів, підтримувати безперервність операцій та мінімізувати наслідки кіберінцидентів.

Отже кіберстійкість слід трактувати не як суто IT-функцію, а як інтегральну характеристику управлінської системи, критично важливу для досягнення стратегічної стабільності та конкурентоспроможності бізнесу в умовах турбулентного цифрового середовища. Тому акцент слід зробити на необхідності зміни управлінського мислення – від класичного управління ризиками до системного підходу управління стійкістю, який включає проактивність, адаптивність, здатність до відновлення та безперервності.

Слід зазначити, що в XXI ст. в глобальному бізнес-середовищі, що швидко змінюється під впливом IT-технологій кращою практикою вдосконалення управління кіберстійкістю компанії є обмін досвідом CEO та CISO та спільне вивчення кращих практик. Для того, щоб стимулювати такий обмін, в рамках ініціативи «План кіберстійкості», спільної роботи Всесвітнього економічного форуму та Оксфордського університету, було зібрано групу експертів-кіберфахівців, які представляють різні сектори з різних країн, для обміну передовим досвідом та визначення того, як організації можуть вжити спільних заходів для подолання міжсекторальних та системних загроз для стійкості екосистеми в цілому [17]. Основні напрацювання експертної групи ґрунтуються на тематичному аналізі трьох віртуальних семінарів, одного очного семінару, п'яти менших віртуальних робочих груп та понад 40 напівструктурованих індивідуальних інтерв'ю. Загалом у дискусіях та інтерв'ю взяли участь 76 експертів з 71 організації. Хоча більшість учасників займали посади, безпосередньо пов'язані з наглядом за кібербезпекою – наприклад, керівники служб інформаційної безпеки (CISO) і технічні директори (CTO), – серед них були й інші фахівці, в тому числі виконавчі директори і консультанти. Було представлено 16 різних галузей промисловості та учасники з Європи, Північної Америки, Південної Америки, Азії та Африки (більш детально див. [17]). Ця ініціатива

визначила різні практики, які сьогодні впроваджуються організаціями, а також перспективи щодо основних практичних прогалин та викликів.

Для досягнення мети дослідження необхідно чітко розділяти зутність «кіберстійкості» та «кібербезпеки». Так кіберстійкість охоплює IT та OT середовища, а також ризики ланцюгів постачання, правові й фінансові зобов'язання після порушень даних, маніпуляції в кіберпросторі (дезінформація, шахрайство), стратегічні й репутаційні ризики та навіть вплив на безпеку людей у системах, критичних до життя. Розширене трактування «кіберризику» як такого, що виникає як у власному цифровому середовищі організації, так і в її екосистемі/ланцюгу постачання, дозволяє охопити реалістичні сценарії впливу й правильно фокусуватися на зниженні наслідків, а не лише на запобіганні. Еволюційний огляд показує перехід від захисту інформації до ширшої парадигми стійкості як бізнес енейблера, що актуалізувалася на тлі великих інцидентів, уразливих ланцюгів постачання та проникнення нових технологій. При цьому кібербезпека не дорівнює кіберстійкості, але є її необхідним компонентом.

Слід зазначити, що для вітчизняного бізнесу одне з перших глобальних розумінь важливості вдосконалення кібербезпеки, а відповідно і кіберстійкості було зустріч з вірусом NotPetya у 2017 році, який вразив спочатку Україну, але швидко поширився на інші країн. Він став шоком для глобального бізнесу, оскільки продемонстрував, що навіть великі корпорації з розвиненими IT-відділами можуть зазнати катастрофічних збитків від кібератаки, спланованої на державному рівні. Після інциденту провідні компанії та урядові структури реалізували низку управлінських рішень, спрямованих на мінімізацію подібних ризиків у майбутньому. Ці заходи не лише зменшили ймовірність повторення атаки масштабу NotPetya, а й заклали основу для вдосконалення стандартів корпоративної кіберстійкості в Україні.

Слід зазначити, що агресія РФ в кіберпросторі є додатковим інструментом до звичайних засобів ведення війни проти України. Урядова команда реагування на комп'ютерні надзвичайні ситуації (CERT-UA) зазначає, що з початку повномасштабної агресії РФ значно активізувала спроби дестабілізувати функціонування державних інституцій у кіберпросторі. Кількість атак зростає з кожним роком. Найчастіше об'єктами кібератак стають міністерства, державні установи та об'єкти критичної інфраструктури, зокрема енергетичний сектор, IT-компанії та телекомунікаційні провайдери. Загалом у 2023 році кількість кібератак в Україні зросла на 15,9% порівняно з 2022 роком. У першій половині 2024 року кількість російських хакерських атак на українські об'єкти зросла на 19% порівняно з другою половиною 2023 року. Попри зменшення на 85% критичних інцидентів та інцидентів з високим рівнем ризику, кількість атак шкідливих програм зросла на 40% [18].

З цих причин уряди і бізнес все більше усвідомлюють необхідність підтримувати і захищати цифрові системи, а також обмежувати вплив кіберінцидентів на їхні основні цілі і завдання, незалежно від того, чи спричинені вони технічними збоями, аваріями, незапланованими відключеннями або стихійними лихами. Тому підтримка ефективної роботи бізнесу має включати досягнення кіберстійкості. Саме кіберстійкість дозволяє організації мінімізувати вплив значних кіберінцидентів на її основні цілі та завдання, що дозволяє їй підтримувати роботу критично важливих сервісів, зберігати довіру зацікавлених сторін та захищати стратегічні цінності, довіру зацікавлених сторін та захистити стратегічні цінності. Розглядаючи кіберстійкість у цих термінах, слід підкреслити, що мова йде про щось більше, ніж просто відновлення роботи у звичайному режимі. Першочергові цілі та завдання організації можуть включати її здатність надавати критичні послуги, утримувати частку ринку, збільшувати акціонерну вартість, зміцнювати довіру до бренду, серед іншого; іншими словами, все, що потрібно для забезпечення функціонування компанії.

Однак кіберстійкість в компанії – це не просто захисний контроль. Кіберстійка цифрова трансформація бізнесу має потенціал для того, щоб

стимулювати підприємницькі інновації, продуктивність та економічне зростання в державі. Щоб безпечно і стабільно використовувати цифрові можливості, організації повинні визначити кіберстійкість як пріоритет не лише як IT-питання, але і як ключове стратегічне питання. Інвестиції в кіберстійкість знижують економічні витрати від кіберподій (наприклад, витоку даних та втрати інтелектуальної власності), а також сприяють покращенню репутації організації (наприклад, виконання вимог клієнтів та брендування безпечних продуктів) [19]. Більше того, за деякими оцінками, більш стійкі компанії генерують прибуток для акціонерів, який приблизно на 50% вищий, ніж у менш стійких компаній [20].

Неспроможність забезпечити кіберстійкість може порушити бізнес-операції і навіть призвести до краху організації [20]. Особливо серйозним може бути вплив на малі та середні підприємства (МСП): за деякими оцінками, 60% МСП, що стали жертвами кібератаки, закриваються впродовж наступних шести місяців [21].

Наведене вище свідчить про важливість розуміння в керівних ланках організацій приватного та публічного секторів необхідності посилення кіберстійкості. Саме лідерство відіграє вирішальну роль у забезпеченні кіберстійкості всієї організації. Це вимагає більше, ніж просто спроможної команди

з кібербезпеки; це вимагає культури, в якій кіберстійкість є пріоритетом у ключових рішеннях, що приймаються на найвищому рівні.

Організації рад директорів з усього світу, включаючи Національну асоціацію корпоративних директорів США, Європейську конференцію асоціацій директорів, Японську федерацію бізнесу та інші, нещодавно випустили рекомендації, які пропагують більш комплексний погляд на кібербезпеку, що сприяє розумінню цього питання з точки зору стійкості [22]. Крім того, незалежні дослідження Всесвітнього економічного форуму та Массачусетського технологічного інституту (MIT) задокументували, що таке ширше розуміння того, що вважається ефективною кіберпрактикою на рівні ради директорів, призводить до значних результатів у сфері безпеки, в тому числі до кращого управління кіберризиками та тіснішого узгодження кіберпроблем з бізнес-результатами, що дозволяє розвивати культуру безпеки і потенційно зменшити кількість кіберподій на 85% [23].

Формуючи та демонструючи менталітет кіберстійкості, просуваючи проактивні підходи, залишаючись в курсі нових загроз та розуміючи ширший вплив кіберризиків на бізнес, CEO та CISO можуть гарантувати, що їхні організації залишатимуться стійкими та добре підготовленими до потенційних викликів. Концепція кіберстійкості може здатися здоровим глуздом, але їй не завжди приділяється належна увага. Бізнес та уряди намагаються мінімізувати вплив на свої основні цілі та надавати свої послуги в умовах кіберінцидентів. Стійкість занадто важлива, щоб залишати її на волю випадку, але занадто багато організацій не змогли підготуватися до неї. Це підкреслює необхідність повного розкриття концепції кіберстійкості та вироблення спільного розуміння її значення.

Таким чином з метою формування науково обґрунтованої бази для ухвалення стратегічних управлінських рішень на рівні CEO та CISO було розроблено анкету та проведене опитування «Cyber resilience 2025», метою якого є визначення рівня технологічної та управлінської зрілості компаній, оцінка масштабів впровадження кращих практик і стандартів, а також формування рекомендацій для ухвалення обґрунтованих управлінських рішень на рівні CEO та CISO (табл. 1).

Зазначимо, що для CEO результати дослідження є підґрунтям для формування стратегій розвитку, інвестиційних рішень та управління

Таблиця 1

Опитувальник «Cyber Resilience 2025»: рішення для CEO і CISO

Блок анкети	Мета	Приклади використання результатів	
		для CEO	для CISO
1	2	3	4
1. Загальна характеристика компанії та респондента	Виявлення залежностей між характеристиками бізнесу та його здатністю до адаптивного управління ризиками	Формування галузевих бенчмарків для визначення конкурентних переваг у стійкості	Вибір релевантних стандартів і технологій кіберзахисту для компанії
2. Оцінка поточного рівня кіберзагроз та ролі підрозділу	Аналіз сприйняття та інтенсивності загроз, а також ролі бізнес-підрозділів у забезпеченні кіберстійкості	Коригування бізнес-стратегії з урахуванням зростання ризиків у ключових сегментах	Оптимізація ресурсів для підрозділів, що перебувають під найбільшим загроз
3. Технологічна інфраструктура та використання Індустрії 4.0	Оцінка цифрової зрілості та зв'язку між впровадженими технологіями й ефективністю управління ризиками	Планування інвести-цій у цифрову трансформацію з урахуванням кіберризиків	Оновлення карти активів та підвищен-ня пріоритетності захисту технологій
4. Управління безперервністю бізнесу та аварійним відновленням (BC/DR)	Визначення рівня інтеграції планів BC/DR у стратегічне та операційне управління	Забезпечення готовності компанії до роботи в умовах кризи без втрати ринкових позицій	Перевірка ефективності та частоти тестування планів відновлення
5. Залучення зовнішніх ресурсів та послуг	Аналіз впливу аутсорсингу та кооперацій-них моделей на гнучкість бізнес-процесів у сфері кіберзахисту	Оцінка доцільності інвестицій у власний SOC або використання SOC-as-a-Service	Вибір оптимальної моделі взаємодії із зовнішніми поста-чальниками безпеки
6. Політики, стандарти та сертифікація	Визначення рівня інституціоналізації кіберзахисту через стандарти, політики та сертифікати	Підвищення приваб-ливості для інвесторів та партнерів через підтверджену відпо-відність стандартам	Формування карти відповідності міжнародним вимогам (ISO, NIST, тощо)
7. Інвестиції, навчання та планування	Оцінка інтеграції кіберзахисту в інвестиційні та кадрові стратегії компанії	Прийняття рішень про розподіл бюджету між розвитком і захистом	Аргументація збільшення фінан-сування на кібер-захист і навчання персоналу

Закінчення таблиці 1

1	2	3	4
8. Перешкоди та шляхи підвищення кіберстійкості	Ідентифікація бар'єрів у впровадженні кращих практик і визначення пріоритетних заходів оптимізації.	Усунення управлінських та фінансових бар'єрів у підвищенні стійкості.	Розробка планів дій для подолання технологічних і організаційних обмежень.
9. Ринковий контекст та кращі практики	Виявлення еталонних моделей кіберстійкості та стратегічних гравців ринку безпеки.	Формування партнерств з лідерами галузі та інтеграція кращих практик.	Аналіз ринку поста-чальників і конку-рентів для коригу-вання власних стратегій захисту.
10. Підходи до Business Resilience Management (BRM)	Оцінка ступеня інтеграції кіберзахисту в комплексне управління стійкістю бізнесу.	Стратегічне планува-ння стійкості з ураху-ванням фінансових, репутаційних та операційних ризиків	Узгодження кіберзахисту з іншими напрямами управління ризиками.

Джерело: розроблено авторкою

ризиками, зокрема – для збалансування витрат на кіберзахист із загальною бізнес-стратегією, інтеграції кіберстійкості в корпоративне управління та комунікації зі стейкхолдерами. В свою чергу, для CISO ці дані дадуть змогу аргументувати потребу в ресурсах, обґрунтувати вибір технологічних і організаційних заходів, адаптованих до специфіки бізнесу, та визначити пріоритети в посиленні захисту як у власному периметрі, так і в ланцюгах постачання.

Опитування за запропонованою авторкою методологією було здійснено з період з січня по травень 2025 року за допомогою Accord Group спільно з підкомітетом з кібербезпеки Європейської Бізнес Асоціації. Серед респондентів переважали власники/CEO/CIO/CISO та керівники підрозділів вітчизняних компаній в різних сферах економічної діяльності (рис. 1).

Що стосується розмірів компаній то серед респондентів більше половини представляли компанії з річним доходом до 2 млн. євро на рік, і лише 5% респондентів з компанії з доходом понад 50 млн. євро на рік.

Слід зазначити, що структура вибірки релевантна реальному складу економіки воєнного часу: домінування мікро- та малих підприємств (79%) збігається з фактом, що саме МСП формують основну масу роботодавців і підрядників у ланцюгах постачання, а отже є «точкою входу» для більшості кіберзагроз і водночас мають найбільші обмеження ресурсів на захист. Переважання респондентів із секторів «Оптова та роздрібна торгівля», «Сільське, лісове та рибне господарство», «Освіта», «Постачання електроенергії, газу, пари та кондиційованого повітря», а також перетину «Переробної промисловості (в т.ч. оборонного призначення)» і «Будівництва» (сукупно 73%) підвищує зовнішню валідність висновків саме для МСП поза IT-сферою. Таке секторне ядро добре репрезентує різні рівні цифрової зрілості – від базової автоматизації (облік, CRM, POS) у торгівлі та агро до специфічних OT/ICS-середовищ в енергетиці,

Рис. 1. Розподіл респондентів за сферою діяльності, %

Джерело: складено авторкою

а також даномістких процесів в освіті, де ризики витоку персональних даних поєднуються з низьким рівнем захищеності кінцевих точок.

Завдяки цій різнорідності вибірка «захоплює» найтиповіші для не-IT бізнесу вектори атак – фішинг, мережеві вторгнення, компрометацію облікових записів, інциденти з резервним копіюванням та, для критичної інфраструктури, порушення в OT-сегментах – і дозволяє екстраполювати спостереження на широку групу суб'єктів, які зазвичай недостатньо представлені у спеціалізованих IT-опитуваннях (що підтверджено отриманими результатами).

Водночас така конфігурація чесно «підсвічує» системні обмеження МСП: розрив між наявністю базових політик і дисципліною регулярних перевірок BCP/DRP, обмежене залучення зовнішніх аудитів і лабораторій, фрагментарність інвестицій, що орієнтовані радше на мінімальну відповідність нормам, ніж на зниження залишкового ризику. Саме тому збалансованість за розміром підприємств і фокус на поза-IT секторах роблять отримані результати прикладними для більшості українських компаній у реальних воєнних умовах, але водночас вимагають обережності при перенесенні висновків на великі, високо регульовані організації фінансового чи ІКТ-секторів, де інші масштаби бюджету, інший регуляторний тиск і вищий ступінь формалізації контролів.

Профіль респондентів очікувано «технічний» (53% – фахівці з кібербезпеки; 23% – топ-менеджери), із гендерним та віковим перекосом, типовим для ринку: ~71% – чоловіки; домінує вікова група 25–44 роки. Результати опитування переконливо фіксують «розрив виконання» між наявністю базових політик/контролів і системністю ризик орієнтованого управління: стратегічні документи та базова гігієна вже є у багатьох, але операційна дисципліна відновлення, незалежна валідація захисту та фінансові рішення, прив'язані до вимірюваної зрілості, відстають. Для нефінансових секторів це означає нагальну потребу в: піднятті ролі CISO на рівень, співставний із CIO; закріпленні періодичності DR перевірок у KPI правління; переході від «відповідності стандарту» до управління залишковим ризиком; розгортанні SOC аналітики з покриттям ідентичностей і даних; системній просвіті користувачів щодо фішингу та витоків. Коротко, «ядро» стійкості вже зібране – тепер вирішальними стають керованість процесів, дисципліна відновлення та зв'язок інвестицій із вимірюваною зрілістю і впливом на ризик.

Для того щоб вирішите це питання було здійснено систематизацію принципів BRM у практичні дії для різних секторів економіки, поєднуючи стратегічні рішення CEO (табл. 2) та тактико-операційні кроки CISO (табл. 3).

Для кожної галузі вони фіксують ключові ризики, управлінські інтервенції (інвестиції, політики, SCRM, кризові плани) та очікуваний ефект у метриках стійкості (RTO/RPO, MTTR, безперервність сервісів, довіра клієнтів).

Це не вичерпні чек-листи, а «дорожні карти» пріоритетів, які дозволяють узгодити бюджет,

Таблиця 2

Карта реалізації тактичних та операційних кроків CEO для реалізації програм кіберстійкості.

Сектор	Ключові ризики	Стратегічні управлінські рішення CEO	Очікуваний результат
Енергетика	Атаки на SCADA, збої в промислових мережах	Інвестувати в резервні системи; диверсифікувати постачальників; затвердити кризові плани	Зменшення часу простою, стабільність постачання
Фінансовий сектор	Викрадення даних клієнтів, атаки на платіжні системи	Cyber stress tests; KPI кібербезпеки; SOC і SIEM	Безперервність сервісів, довіра клієнтів
Промисловість	Атаки на виробництво, IoT	Аудит кіберризиків; план реагування; кіберстрахування	Стійкість виробництва
Телеком та IT	DDoS, збої у хмарних сервісах	SOC або MSSP; Zero Trust; резервування каналів	Стійкість сервісів
Транспорт і логістика	Атаки на GPS, цифрові платформи	Кібераудит постачальників; моніторинг загроз; тестування планів реагування	Безпека ланцюгів постачання
Рітейл	Злом POS, e-commerce, витік даних	Бюджет на захист продажів; відповідність PCI DSS, GDPR; кіберризик-менеджмент у ланцюгах постачання	Довіра клієнтів, безпека транзакцій
Освіта	Атаки на освітні платформи, викрадення персональних даних студентів і викладачів	Інвестувати у кіберзахист LMS і баз даних; впровадити політику безпечного доступу; навчати персонал кібергігієні	Захист даних, безперервність навчання

Джерело: складено авторкою

Таблиця 3

Карта реалізації тактичних та операційних кроків CISO для реалізації програм кіберстійкості

Сектор	Ключові ризики	Тактичні та операційні рішення CISO	Очікуваний результат
Енергетика	Атаки на SCADA, OT/IT інтеграцію	Сегментація мереж; захист промислових протоколів; тестування відновлення	Захист критичної інфраструктури
Фінансовий сектор	Викрадення платіжних даних, шахрайство	MFA; моніторинг транзакцій; DLP; відповідність DORA, GDPR	Захист активів і даних
Промисловість	Атаки на IoT та IIoT	Інвентаризація активів; контроль доступу; безпечні оновлення ПЗ	Зниження вразливостей
Телеком та IT	DDoS, компро-метація акаунтів	SOC або MSSP; Zero Trust; IDS/IPS; SIEM	Безперервність сервісів
Транспорт і логістика	Збої GPS, плат-форми управління	Моніторинг навігаційних систем; безпека у договорах	Стійкість логістики
Рітейл	POS-злом, витік даних, e-commerce атаки	PCI DSS; WAF; сегментація мереж; захист мобільних застосунків	Захист транзакцій та даних
Освіта	Атаки на LMS, витік персо-нальних даних	MFA для студентів і викладачів; резервне копіювання; моніторинг загроз; шифрування баз даних	Безпека нав-чального про-цесу та даних

Джерело: складено авторкою

архітектуру та процеси реагування із специфікою сектору й вимогами регуляторики. В обох версіях рітейл буде інтегрований на рівні з іншими секторами (енергетика, фінанси, промисловість, телеком та IT, транспорт і логістика).

Висновки. У результаті проведеного дослідження обґрунтовано, що кіберстійкість бізнесу слід розглядати не лише як похідну категорію інформаційної безпеки, а як інтегральний управлінський феномен, що визначає здатність компанії підтримувати сталість функціонування та забезпечувати конкурентні переваги в умовах цифрової турбулентності. Еволюція парадигми від традиційної інформаційної безпеки до комплексної кіберстійкості відображає глибинні зміни у логіці функціонування сучасних організацій, де безперервність операцій, адаптивність та швидкість відновлення постають ключовими критеріями стратегічної життєздатності.

Проведений аналіз міжнародних ініціатив та емпіричні результати опитування українських компаній засвідчили, що попри формування базових політик і впровадження окремих технічних рішень, існує суттєвий розрив між номінальною відповідністю стандартам і практичною реалізацією принципів кіберстійкості. Особливо критичним це є для МСП, які становлять основу національної економіки, але характеризуються обмеженістю ресурсів для побудови системної моделі управління ризиками. За отриманими результатами опитування в Україні можна визначити, що кіберстійкість бізнесу стає системоутворюючим фактором сталого розвитку компаній, оскільки забезпечує їхню здатність зберігати функціональну цілісність, захищати ключові цінності та підтримувати довіру стейкхолдерів в умовах масштабних криз. Перспективи подальших наукових розвідок полягають у розробленні кількісних моделей вимірювання зрілості кіберстійкості, інтеграції її індикаторів у нефінансову звітність компаній та бенчмаркингу найкращих міжнародних практик для адаптації до українського контексту повоєнного відновлення.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. WEF, 2016, Annual Report 2016–2017. URL: https://www3.weforum.org/docs/WEF_Annual_Report_2016_17.pdf

2. WEF, 2024, Global Cybersecurity Outlook 2024 p. 7–9. URL: https://www.weforum.org/reports/global-cybersecurity-outlook-2024

3. ДССЗЗІ, 2023 Кібератаки в Україні. URL: https://cip.gov.ua/news/kiberataki-v-ukrayini-u-2023-roci-sprobuvali-zlamati-ponad-2500-obiektiv

4. Coutu D. L. How resilience works. *Harvard business review*. 2002. № 80 (5). P. 46–56. URL: https://kempstreetpartners.com.au/wp-content/uploads/2022/02/Coutu-Diane-L.-2002.-How-Resilience-Works-HBR-May-2002.pdf

5. Халіна В., Абєлєнцев Є. Теорія адаптації бізнесу до умов невизначеності. *Економіка та суспільство*. 2023. № 55. DOI: https://doi.org/10.32782/2524-0072/2023-55-6

6. Користін О. Є., Демедюк С. В. Актуалізація кіберстійкості та історичні витоки концепції «стійкість». *Аналітично-порівняльне правознавство*, 2023. № 6. С. 708–713. DOI: https://doi.org/10.24144/2788-6018.2023.06.122

7. Von Solms R., Van Niekerk J. From information security to cyber security. *Computers & security*. 2013. No. 38. P. 97–102. DOI: https://doi.org/10.1016/j.cose.2013.04.004

8. 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. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-16486-1_31

9. Sabatino M. Economic crisis and resilience: Resilient capacity and competitiveness of the enterprises. *Journal of Business Research*. 2016. № 69(5). P. 1924–1927. DOI: https://doi.org/10.1016/j.jbusres.2015.10.081

10. 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. № 3. С. 98–101. DOI: https://doi.org/10.20998/2519-4461.2020.3.102

11. Сподіна А. О., Тарасенко І. О. Фінансова стійкість підприємства: сутність та фактори впливу. *Міжнародний науковий журнал «Інтернаука»*. 2022. № 12 (131). С. 24–31. URL: https://www.inter-nauka.com/uploads/public/16704889827423.pdf#page=25

12. Криклій О. А. Теорія та практика забезпечення кіберстійкості банків. *Ефективна економіка*. 2020. № 10. DOI: https://doi.org/10.32702/2307-2105-2020.10.50

13. Лібанова Е. Резильєнтність соціоекономічної системи України до шоків, спричинених війною: специфіка формування і реагування. *Demography and social economy*. 2024. № 58(4). С. 3–23. DOI: https://doi.org/10.15407/dse2024.04.003

14. Ткаченко І. П. Резильєнтність бізнесу України: як підтримати виробництво та інновації в умовах війни. *Економічний вісник Дніпровського державного технічного університету*. 2024. № 2 (9). С. 125–135. DOI: https://doi.org/10.31319/2709-2879.2024iss2(9).319091pp125-135

15. Hult F., Sivanesan G. What good cyber resilience looks like. *Journal of business continuity & emergency planning*. 2014. № 7 (2). С. 112–125. URL: https://www.ingentaconnect.com/contentone/hsp/jbcep/2014/00000007/00000002/art00004

16. Kott A., Linkov I. *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

17. Global Cyber Security Capacity Centre URL: https://gcscc.ox.ac.uk/cyber-resilience-blueprint

18. CERT-UA URL: https://cert.gov.ua/

19. Saeed S., Altamimi S. A., Alkayyal N. A., Alshehri E., Alabbad D. A. Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors*. 2023. Vol. 23(15). P. 1–20. DOI: https://doi.org/10.3390/s23156666.

20. Hatami H., Segel L. Six CEO priorities for 2023. McKinsey & Co. 2023. URL: https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/six-ceo-priorities-for-2023

21. Leigh D. 60% of SMEs that suffer a cyber attack go out of business within six months. TechRound. 2023. URL: https://techround.co.uk/news/60-of-smes-that-suffer-a-cyber-attack-go-out-of-business-within-six-months/.

22. National Association of Corporate Boards. (2023, March 24). NACD directors' handbook on cyber-risk oversight. URL: https://www.nacdonline.org/all-governance/governance-resources/governance-research/director-handbooks/nacddirectors-handbook-on-cyber-risk-oversight/.

23. World Economic Forum. (2022, November 15). As cyber attacks increase, here's how CEOs can improve cyber resilience. URL: https://www.weforum.org/agenda/2022/11/as-cyber-attacks-increase-heres-how-ceos-can-improve-cyber-resilience/

REFERENCES:

1. WEF, 2016, Annual Report 2016–2017. Available at: https://www3.weforum.org/docs/WEF_Annual_Report_2016_17.pdf

2. WEF, 2024, Global Cybersecurity Outlook 2024 p. 7–9. Available at: https://www.weforum.org/reports/global-cybersecurity-outlook-2024

3. State Service of Special Communications and Information Protection of Ukraine, 2023 Cyberattacks in Ukraine. Available at: https://cip.gov.ua/news/kiberataki-v-ukrayini-u-2023-roci-sprobuvali-zlamati-ponad-2500-obiektiv

4. Coutu D. L. (2002) How resilience works. *Harvard business review*, no. 80 (5), pp. 46–56. Available at: https://kempstreetpartners.com.au/wp-content/uploads/2022/02/Coutu-Diane-L.-2002.-How-Resilience-Works-HBR-May-2002.pdf

5. Halina V., Abelentsev E. (2023). Teoriya adaptatsiyi biznesu do umov nevyznachenosti. [The theory of business adaptation to conditions of uncertainty]. *Economy and society*, no. 55. DOI: https://doi.org/10.32782/2524-0072/2023-55-6

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

7. Von Solms R., Van Niekerk J. (2013) From information security to cyber security. *Computers & security*, no. 38, pp. 97–102. DOI: https://doi.org/10.1016/j.cose.2013.04.004

8. 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

9. Sabatino M. (2016) Economic crisis and resilience: Resilient capacity and competitiveness of the enterprises. *Journal of Business Research*, no. 69(5), pp. 1924–1927. DOI: https://doi.org/10.1016/j.jbusres.2015.10.081

10. Zahirnyak D., Danylko V., Ishchenko S., Liga D. (2020). Stratehichna stiykist v umovakh hlobalizatsiyi ekonomiky yak antykryzovyy instrument. [Strategic stability in the conditions of economic globalization as an anti-crisis tool]. *Visnyk Natsionalnoho tekhnichnoho universytetu "Kharkivskyy politekhnichnyy instytut" (ekonomichni nauky)*, no. 3, pp. 98–101. DOI: https://doi.org/10.20998/2519-4461.2020.3.102

11. Spodina A., Tarasenko I. (2022) Finansova stiykist' pidpryyemstva: sutnist' ta faktory vplyvu.

Mizhnarodnyy naukovyy zhurnal "Internauka". [Financial sustainability of the enterprise: essence and influencing factors]. *International scientific journal "Internauka",* no. 12 (131), pp. 24–31. Available at: https://www.inter-nauka.com/uploads/public/16704889827423.pdf#page=25

12. 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

13. Libanova, E. (2024). Rezilyentnost sotsioekonomicheskoy sistemy Ukrainy k shokam, vyzvannym voynoy: spetsifika formirovaniya i reagirovaniya [Resilience of the socioeconomic system of Ukraine to shocks caused by the war: specifics of formation and response]. *Demography and social economy*, vol. *58*(4), pp. 3–23. DOI: https://doi.org/10.15407/dse2024.04.003

14. Tkachenko, I. P. (2024). Rezylyentnist biznesu Ukrayiny: yak pidtrymaty vyrobnytstvo ta innovatsiyi v umovakh viyny. Ekonomichnyy visnyk Dniprovs'koho derzhavnoho tekhnichnoho universytetu, [Business resilience of Ukraine: how to support production and innovation in war conditions]. *Ekonomichnyi visnyk Dniprovskoho derzhavnoho tekhnichnoho universytetu*, vol. 2 (9), pp. 125–135. DOI: https://doi.org/10.31319/2709-2879.2024iss2(9).319091pp125-135

15. 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

16. Kott A., Linkov I. 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

17. Global Cyber Security Capacity Centre (2025) Available at: https://gcscc.ox.ac.uk/cyber-resilience-blueprint

18. CERT-UA. Available at: https://cert.gov.ua/

19. Saeed S., Altamimi S. A., Alkayyal N. A., Alshehri E., Alabbad D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors*, vol. 23(15), pp. 1–20. DOI: https://doi.org/10.3390/s23156666.

20. Hatami H., Segel L. (2023, April 6). Six CEO priorities for 2023. McKinsey & Co. Available at: https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/six-ceo-priorities-for-2023

21. Leigh D. (2023, March 14). 60% of SMEs that suffer a cyber attack go out of business within six months. TechRound. Available at: https://techround.co.uk/news/60-of-smes-that-suffer-a-cyber-attack-go-out-of-business-within-six-months/.

22. National Association of Corporate Boards. (2023, March 24). NACD directors' handbook on cyber-risk oversight. Available at: https://www.nacdonline.org/all-governance/governance-resources/governance-research/director-handbooks/nacddirectors-handbook-on-cyber-risk-oversight/.

23. World Economic Forum. (2022, November 15). As cyber attacks increase, here's how CEOs can improve cyber resilience. Available at: https://www.weforum.org/agenda/2022/11/as-cyber-attacks-increase-heres-how-ceos-can-improve-cyber-resilience/