ЦИФРОВА ТРАНСФОРМАЦІЯ БІЗНЕС-ПРОЦЕСІВ: БЕЗПЕКОВИЙ АСПЕКТ

DIGITAL TRANSFORMATION OF BUSINESS PROCESSES: THE SECURITY ASPECT

УДК 658:338.242
DOI: https://doi.org/10.32782/dees.17-26

Глушко А.Д.[1]
к.е.н., доцент,
Національний університет «Полтавська політехніка імені Юрія Кондратюка»
Янко А.С.[2]
к.т.н., доцент,
Національний університет «Полтавська політехніка імені Юрія Кондратюка»
Білько С.С.[3]
доктор філософії,
Національний університет «Полтавська політехніка імені Юрія Кондратюка»

Hlushko Alina
National University "Yuri Kondratyuk Poltava Polytechnic"
Yanko Alina
National University "Yuri Kondratyuk Poltava Polytechnic"
Bilko Stanislav
National University "Yuri Kondratyuk Poltava Polytechnic"

Стаття присвячена обґрунтуванню адаптивних безпекових стратегій функціонування бізнесу в умовах цифрової трансформації. У рамках дослідження обґрунтовано важливість формування системи кіберстійкості як одного з ключових елементів управління інформаційними технологіями в умовах цифровізації. Доведено, що інтеграція таких систем сприяє зниженню ризику виникнення інцидентів, забезпечує безперервність бізнес-процесів навіть у кризових ситуаціях, а також підвищує рівень довіри до цифрової інфраструктури. Розглянуто два концептуальні підходи до забезпечення безпеки бізнесу в умовах цифрової трансформації, зокрема акцентовано увагу на доцільності впровадження принципу «стійкість за проєктом». Цей підхід дає змогу підприємствам ефективно планувати протидію сучасним загрозам, підтримувати безперервність функціонування та створювати надійні системи кіберстійкості. На основі концептуальних положень принципу «стійкості за проєктом» запропоновано модель безпекового підходу до функціонування бізнесу в умовах цифровізації. Візуалізовано систему кіберстійкості, що забезпечує ефективний захист економічних суб'єктів та сприяє підвищенню їх конкурентоспроможності у цифровому середовищі.
Ключові слова: *бізнес-середовище, інформаційні технології, безпекоорієнтоване середовище, адаптивна стратегія, кіберзагрози, кіберризики, цифрова екосистема бізнесу.*

The article is devoted to the substantiation of adaptive security strategies for business operation in the context of digital transformation. The digital economy is significantly changing traditional approaches to organizing business processes, where digital data is becoming the key factor of production and activities are focused on the creation, distribution and implementation of digital technologies. Amid the rapid growth of cyber threats, businesses are forced to quickly adapt their business models to ensure not only operational efficiency but also the security of digital assets. This necessitates the development of advanced security strategies that combine technical and organizational aspects of protection. Traditional methods focused on protecting physical assets and infrastructure no longer meet the challenges of the modern digital environment. The study substantiates the importance of forming a cyber resilience system as one of the key elements of information technology management in the context of digitalization. It is proved that the integration of such systems helps to reduce the risk of incidents, ensures the continuity of business processes even in crisis situations, and increases the level of trust in digital infrastructure. The article considers two conceptual approaches to ensuring business security in the context of digital transformation, with a particular focus on the feasibility of implementing the principle of 'resilience by design'. This approach allows enterprises to effectively plan to counter modern threats, maintain business continuity and create reliable cyber resilience systems. Based on the conceptual provisions of the principle of 'resilience by design', a model of a security approach to business functioning in the context of digitalization is proposed. The author visualizes a cyber resilience system that ensures effective protection of economic entities and helps to increase their competitiveness in the digital environment. The proposed system will enable a prompt response to real and potential threats, enhance the security level of business processes of economic entities, and ensure their cyber resilience.
Key words: *business environment, information technology, security-oriented environment, adaptive strategy, cyber threats, cyber risks, digital business ecosystem.*

Постановка проблеми. У сучасному світі цифрова трансформація стає важливим елементом стратегічного розвитку бізнесу, змінюючи традиційні підходи до організації бізнес-процесів і створюючи нові моделі роботи. Впровадження інноваційних технологій, таких як штучний інтелект (ШІ), Інтернет речей (IoT), хмарні обчислення, блокчейн і квантові технології, не лише забезпечує компаніям конкурентні переваги, а й відкриває нові горизонти для розвитку [1]. Штучний інтелект стає ядром багатьох змін, пропонуючи інструменти для автоматизації бізнес-процесів, аналізу великих обсягів даних і підтримки складних управлінських рішень. Він дозволяє компаніям швидко адаптуватися до мінливих умов ринку, забезпечуючи більшу точність і оперативність у прийнятті рішень. Наприклад, у фінансовому секторі ШІ використовується для виявлення шахрайства в режимі реального часу, в той час як у сфері маркетингу він сприяє створенню персоналізованих клієнтських пропозицій. IoT, у свою чергу, трансформує управління ланцюгами постачання, забезпечуючи прозорість і контроль за допомогою збирання та аналізу даних у реальному часі. Наприклад, компанії можуть відстежувати стан обладнання, оптимізувати маршрути доставки або виявляти потенційні проблеми до того, як вони стануть критичними. Це сприяє зниженню витрат

[1] ORCID: https://orcid.org/0000-0002-4086-1513
[2] ORCID: https://orcid.org/0000-0003-2876-9316
[3] ORCID: https://orcid.org/0000-0003-0259-4482

і підвищенню ефективності. Хмарні обчислення відіграють ключову роль у забезпеченні масштабованості бізнесу, дозволяючи організаціям швидко адаптувати свої ресурси відповідно до потреб. Ця технологія стає основою для впровадження нових бізнес-моделей, таких як «інфраструктура як послуга» або «платформа як послуга». Квантові обчислення здатні кардинально змінити способи вирішення складних завдань. Це стосується, наприклад, моделювання нових матеріалів, оптимізації логістики або розробки стійких до злому криптографічних алгоритмів.

Втім, впровадження цих технологій супроводжується численними викликами у сфері безпеки. Зокрема, зростання обсягів даних і їх доступність через підключення до мережі створюють сприятливі умови для кіберзагроз [2]. Витік даних, атаки зловмисників і збої в роботі систем можуть завдати серйозних збитків компаніям, аж до втрати довіри клієнтів і партнерів. Для успішного подолання цих викликів необхідний системний підхід до забезпечення безпеки, який враховує як технологічні, так і організаційні аспекти. Це передбачає впровадження ефективних механізмів захисту, таких як багаторівнева автентифікація, моніторинг мережевої активності та регулярні перевірки безпеки. Створення безпекоорієнтованого середовища, в якому цифрові інновації поєднуються з надійними системами захисту, стає ключовою умовою успішної цифрової трансформації бізнесу.

Аналіз останніх досліджень і публікацій. Безпека бізнесу в умовах цифрової трансформації та активного впровадження інноваційних технологій є предметом дослідження широкого кола науковців. Так, Т.М. Сібел у роботі [3] досліджує вплив новітніх технологій на бізнес-процеси та державне управління. Автор глибоко аналізує роль ключових інноваційних рішень, таких як хмарні обчислення, великі дані, ШІ та Інтернет речей (IoT), у трансформації бізнес-процесів в умовах цифрової епохи. Особливу увагу приділено аналізу прикладних кейсів, що ілюструють успішне використання зазначених технологій провідними світовими компаніями, такими як Enel, 3M, Royal Dutch Shell, а також Міністерством оборони США. Ці приклади демонструють, як інтеграція цифрових рішень сприяє підвищенню ефективності операційної діяльності, оптимізації управлінських процесів та стимулюванню інновацій. Такий підхід дозволяє зробити висновок, що використання цифрових технологій є не лише інструментом модернізації, а й стратегічною необхідністю для збереження конкурентоспроможності в умовах глобальних змін. Водночас перспективними напрямами подальших досліджень автор визначає забезпечення кібербезпеки та формування адаптивних безпекових стратегій інтеграції новітніх технологій у бізнес-процеси.

У дослідженні А. Свейна, К.П. Свейна, С.К. Паттнаїка, С.Р. Самала та Дж.К. Даса [4] проведено ґрунтовний аналіз сучасного стану кібербезпеки в контексті цифрової трансформації. Окрему увагу приділено ідентифікації основних загроз, пов'язаних із впровадженням новітніх технологій, а також розробці стратегічних рішень для мінімізації цих ризиків і забезпечення стабільності цифрових бізнес-процесів. А. Коралло, М. Лазой та М. Лецці [5] було розроблено структуровану класифікацію критично важливих промислових активів із врахуванням їхньої ролі в забезпеченні ефективності бізнес-процесів. Особливу увагу авторами приділено аналізу потенційних ризиків, пов'язаних із порушеннями кібербезпеки, які можуть негативно вплинути на продуктивність та стійкість підприємств. Зокрема, кіберзагрози розглядаються через призму трьох ключових аспектів: конфіденційності, цілісності та доступності даних. Враховуючи цінність проведених досліджень, правомірно відмітити об'єктивну необхідність розроблення нових підходів до забезпечення кібербезпеки бізнесу умовах постійного розвитку технологій.

У роботі Р. Бугріменка та П. Смірнової [6] проаналізовано вплив цифрової трансформації на функціонування підприємств, а також визначено ключові тенденції та виклики, що виникають у цьому процесі. Зокрема, розглядаються переваги цифровізації, серед яких підвищення продуктивності, зміцнення конкурентоспроможності, створення нових бізнес-моделей, а також ухвалення стратегічних управлінських рішень щодо адаптації підприємств до змін у сучасному бізнес-середовищі. Окрім того, обґрунтовано важливість дотримання етапів цифрової трансформації, що сприяють успішному впровадженню та розвитку підприємств у цифровому середовищі. У праці Н.О. Іванченко, Ж.В. Кудрицької, К.В. Рекачинської [7] досліджено досвід міжнародних корпорацій у впровадженні нових технологій. Колективом авторів розглянуто цифрову трансформацію бізнес-моделей в контексті збереження економічними суб'єктами лідируючих позицій у галузі за рахунок створення технологічних перепон. Поряд з цим, важливим питанням залишається створення автоматизованих систем моніторингу кіберзагроз, розробка стійких до атак алгоритмів захисту даних, інтеграція інструментів машинного навчання для прогнозування ризиків.

Питанням цифрової трансформації бізнесу присвячені аналітичні огляди та дослідження світових організацій. Так, фахівці Gartner у звіті [8] підкреслюють важливість адаптації до нових викликів, таких як поширення генеративного штучного інтелекту, дефіцит кваліфікованих кадрів у сфері безпеки та зростання використання хмарних технологій. Компанія рекомендує лідерам у сфері безпеки та управління ризиками впроваджувати гнучкі та адаптивні стратегії для ефективного захисту

цифрових екосистем. McKinsey & Company у аналітичному огляді за підсумками 2023 року [9] зазначає, що архітектури довіри та цифрова ідентичність стали ключовими напрямами, демонструючи зростання майже на 50% порівняно з попереднім роком. Це свідчить про підвищену увагу до безпеки, конфіденційності та стійкості в різних галузях.

Враховуючи активну інтеграцію цифрових технологій у бізнес-процеси, виникає необхідність у розробленні адаптивних підходів до забезпечення безпеки бізнес-середовища в умовах цифрової трансформації.

Постановка завдання. Метою дослідження є обґрунтування адаптивних безпекових стратегій функціонування бізнесу в умовах цифрової трансформації. Це дозволить оперативно реагувати на реальні та потенційні загрози, підвищити рівень безпеки бізнес-процесів економічних суб'єктів та забезпечити їх кіберстійкість.

Методи і матеріали досліджень. У ході дослідження застосовано широкий спектр методів, що сприяли глибокому аналізу проблематики забезпечення безпеки економічних суб'єктів в умовах цифрової трансформації бізнес-процесів. Використання методу контекстуального аналізу дозволило виявити двоїстий вплив сучасних технологій, що є важливим для обґрунтованої оцінки ризиків і переваг їх впровадження. Застосування методу критичного аналізу дало змогу оцінити існуючі підходи до формування безпекових стратегій, визначити їх сильні та слабкі сторони, а також підтвердити необхідність впровадження підходу «стійкості за проєктом». Метод порівняння та аналізу первинних даних забезпечив можливість дослідження ефективних практик використання новітніх технологій для розвитку бізнесу та одночасного зміцнення кібербезпеки. Інтеграція зазначених методів сформувала системний підхід до дослідження, що сприяло отриманню достовірних результатів і формуванню практичних рекомендацій для підвищення рівня захищеності економічних суб'єктів в умовах цифровізації.

Виклад основного матеріалу дослідження. Технології, що розвиваються, створюють нові можливості для бізнесу та суспільства, але одночасно значно збільшують площу цифрових атак [10]. Так, різке зростання кількості пристроїв IoT, яке за прогнозами перевищить 32 мільярди до 2030 року, відкриває незліченну кількість точок доступу для кібератак. Це ставить під загрозу як приватні, так і корпоративні мережі, де кожен підключений пристрій може стати слабкою ланкою. Нерегульований характер екосистем Інтернету речей вимагає надійних інфраструктур безпеки для захисту проти зломів і запобігання зловмисникам від використання цих пристроїв.

Хоча технологія блокчейну забезпечує підвищену безпеку даних завдяки децентралізації, її використання в бізнес-процесах також не позбавлене ризиків. У корпоративному середовищі вразливі місця в смарт-контрактах можуть стати джерелом серйозних загроз, дозволяючи зловмисникам маніпулювати умовами угод або отримувати фінансову вигоду. Це може спричинити значні економічні втрати для компаній, які інтегрують блокчейн у бізнес-процеси. Крім того, децентралізована структура блокчейну в бізнес-процесах, хоч і забезпечує прозорість, одночасно створює труднощі для моніторингу та контролю транзакцій. Псевдонімність учасників мережі може ускладнити ідентифікацію сторін, що стає перешкодою для забезпечення відповідності законодавчим вимогам. Зокрема, це викликає занепокоєння щодо потенційного використання блокчейну в незаконних операціях, таких як відмивання грошей чи фінансування злочинної діяльності.

Інтеграція штучного інтелекту у бізнес-процеси значно підвищує їхню ефективність, але водночас створює специфічні загрози, які можуть вплинути на кібербезпеку компаній. Наприклад, такі уразливості, як отруєння даних (data poisoning), можуть призводити до внесення шкідливих змін у навчальні набори даних, що спотворює результати роботи моделей. Маніпулювання моделлю штучного інтелекту дозволяє зловмисникам змінювати алгоритми для отримання вигоди або порушення бізнес-процесів. Штучний інтелект також може бути використаний для здійснення агресивних атак, таких як автоматизовані фішингові кампанії, що створюють персоналізовані повідомлення для обману співробітників або клієнтів. Здатність ШІ генерувати реалістичні глибокі фейки (deepfakes) додає новий рівень складності до загроз, зокрема у сфері комунікацій і репутаційного ризику. Крім того, автоматизовані експлойти, керовані ШІ, дозволяють зловмисникам швидко знаходити й використовувати вразливості в системах, збільшуючи масштаб можливих атак.

Таким чином, складний характер нових технологій створює унікальні виклики безпеці, які вимагають цілеспрямованих стратегій і рішень. Традиційний концепт «безпеки за проєктом», який орієнтується на інтеграцію функцій безпеки на ранніх етапах впровадження інноваційних технологій у бізнес-процеси, більше не відповідає сучасним викликам, зумовленим складністю та динамікою загроз. Відповідно, виникає потреба у впровадженні підходу «стійкості за проєктом», який передбачає не лише захист інформаційних систем, але й їхню здатність витримувати атаки, мінімізувати наслідки від можливих порушень та швидко відновлюватися після них [11]. Такий підхід базується на кількох ключових принципах. По-перше, системи мають бути побудовані з урахуванням моделювання ризиків, де пріоритет надається не лише виявленню можливих слабких

місць, але й активному плануванню сценаріїв реагування. Сценарії реагування можуть охоплювати як превентивні заходи, так і тактичні кроки для швидкого відновлення після інцидентів. По-друге, безпека повинна бути інтегрована у всі етапи життєвого циклу технології, від початкової розробки до експлуатації та модернізації. Процес інтеграції включає розробку архітектури системи з урахуванням потенційних ризиків і створення «модульної» структури, яка спрощує локалізацію та мінімізацію впливу атак; проведення стрес-тестів і симуляцій кіберзагроз, що дозволяє виявити вразливі місця ще до впровадження системи; постійний моніторинг функціонування системи, швидке реагування на інциденти та адаптація до змінюваних умов; оновлення інструментів безпеки й удосконалення захисних механізмів відповідно до еволюції загроз. По-третє, критичну роль відіграє впровадження засобів штучного інтелекту для моніторингу загроз у реальному часі, що дозволяє системам адаптуватися до нових умов і атак.

Підхід «стійкості за проєктом» також потребує міждисциплінарної співпраці. Необхідно об'єднувати зусилля вчених, інженерів, фахівців з кібербезпеки та політиків, аби забезпечити гармонійний розвиток технологій, мінімізуючи ризики. Лише така інтеграція дозволить створити інноваційні рішення, які будуть одночасно прогресивними та захищеними від сучасних і майбутніх загроз. Технології, спроєктовані за принципом «стійкості за проєктом», здатні змінювати свою поведінку залежно від нових викликів, що підвищує їхню актуальність у довгостроковій перспективі. Завдяки здатності до швидкого відновлення інформаційні системи можуть працювати навіть за умов часткових пошкоджень, що знижує вплив інцидентів на бізнес-процеси.

Графічна інтерпретація моделі «стійкості за проєктом» представлена на рисунку 1. Ключові компоненти та їх взаємозв'язки ілюструють, як система функціонує, реагує на загрози та забезпечує адаптивність і стійкість.

Такий безпековий підхід дозволить бізнесу ефективно планувати заходи для протистояння сучасним загрозам, забезпечувати безперервність роботи та формувати довіру до цифрової інфраструктури.

Динамічний ландшафт загроз в умовах цифровізації вимагає постійного моніторингу та адаптації стратегій кібербезпеки для забезпечення їх ефективності. Практичний приклад Schneider Electric демонструє, як організація може ефективно використовувати новітні технології для підвищення кібербезпеки, одночасно керуючи пов'язаними ризиками. Schneider Electric, світовий лідер промислових технологій, забезпечує кіберстійкість завдяки наявності у штаті компанії команди, яка займається технологіями та інноваціями в галузі кібербезпеки, а також пов'язаним процесом перевірки технологій. Ця спеціалізована команда постійно перевіряє можливості компанії щодо захисту даних як для базової цифрової інфраструктури, так і для нових технологій. Фахівці формують дорожню карту з урахуванням результатів аудиту та тестування на проникнення, аналітики вразливостей та інцидентів, звітів оціночних агентств і запитів клієнтів. Для забезпечення цілісної оцінки ризиків усі нові цифрові активи

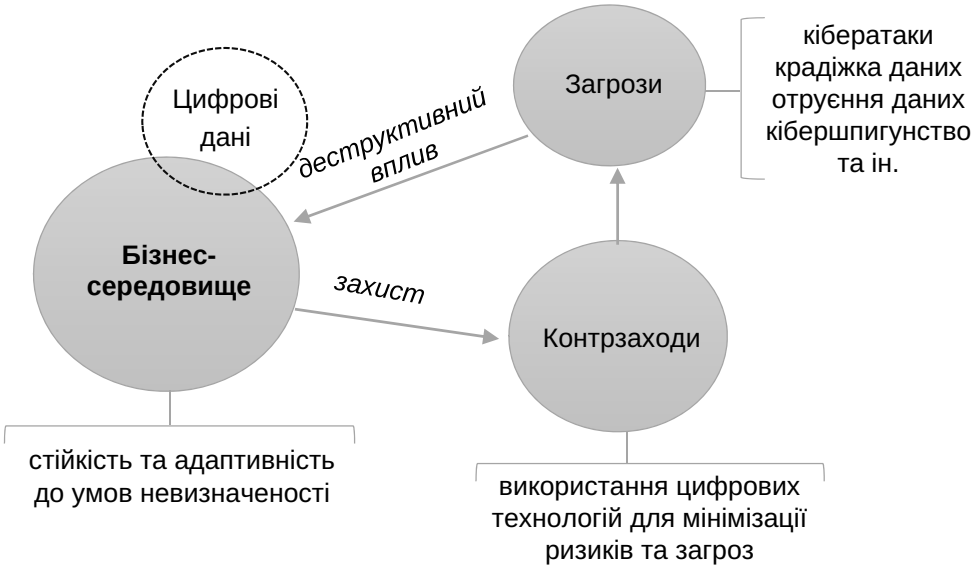

Рис. 1. Модель безпекового підходу «стійкості за проєктом» до функціонування бізнесу в умовах цифровізації

Джерело: складено авторами

проходять перевірку перед впровадженням у бізнес-процеси. Команда формує безпечну цифрову організацію діяльності бізнес-підрозділів компанії.

Одним із практичних прикладів впровадження передових заходів кібербезпеки Schneider Electric є використання генеративного штучного інтелекту для створення коду програмованих логічних контролерів у промислових системах керування. Це рішення дозволяє автоматизувати процес генерації коду, що сприяє підвищенню його якості та скороченню часу розробки. Застосування штучного інтелекту в цьому контексті не лише підвищує ефективність роботи, але й сприяє посиленню заходів кібербезпеки. Автоматизація кодування за допомогою генеративного ШІ дозволяє мінімізувати людські помилки, які часто стають причиною вразливостей у системах [12]. Крім того, у поєднанні з проактивними заходами кібербезпеки, такими як аудит, моделювання загроз і впровадження багаторівневого моніторингу, компанія створює середовище, що забезпечує безпечну інтеграцію інноваційних технологій у бізнес-процеси.

Враховуючи концептуальні засади підходу «стійкості за проєктом», візуалізація системи кіберстійкості економічних суб'єктів може бути представлена в наступному вигляді (рис. 2).

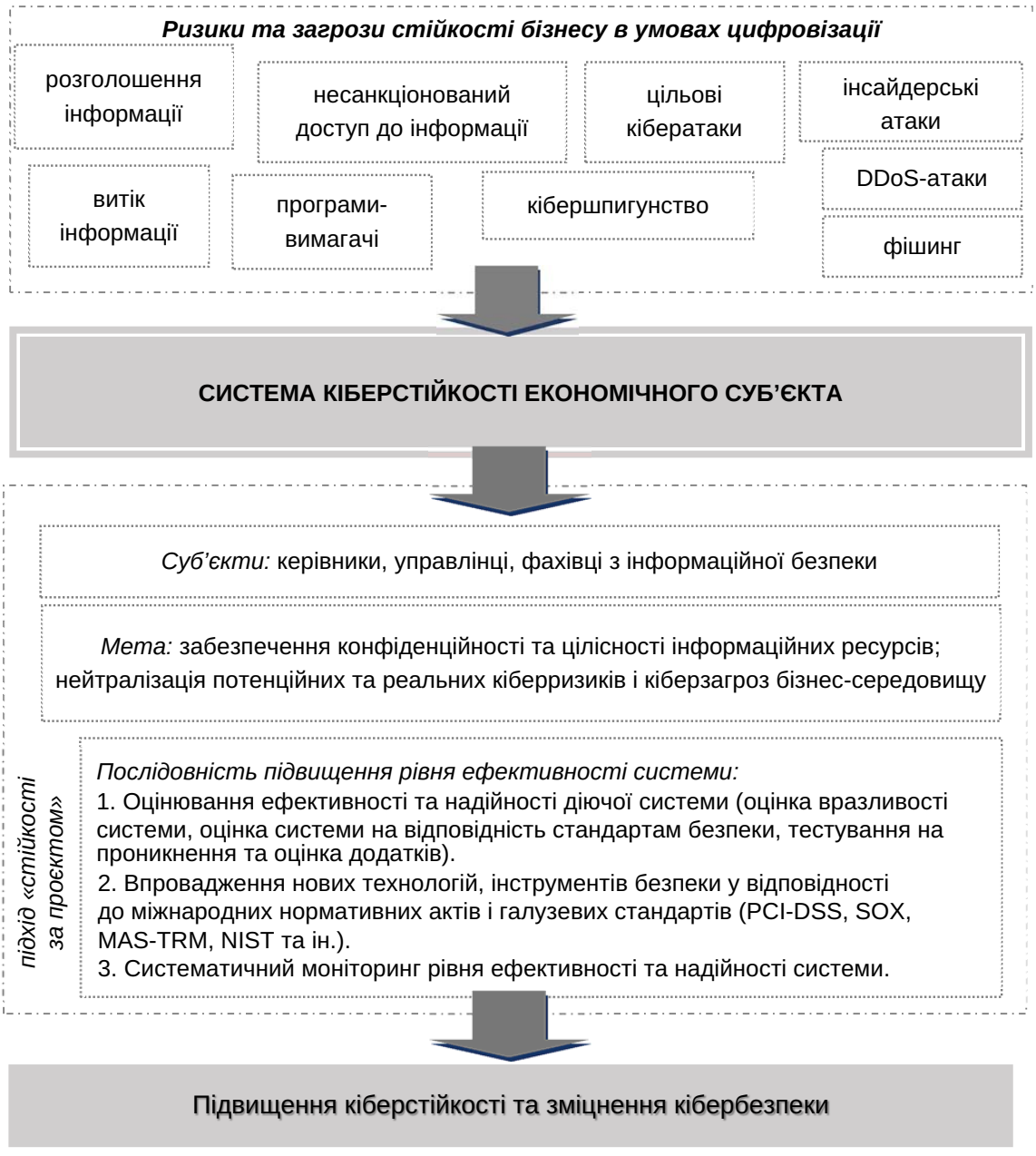

Рис. 2. Візуалізація системи кіберстійкості економічних суб'єктів на основі підходу «стійкості за проєктом»

Джерело: складено авторами

На сьогодні системи кібербезпеки економічних суб'єктів спрямовані на оброблення та збереження потужного масиву конфіденційних даних (клієнт-транзакції, інформація про облікові записи та приватні персональні дані платіжних карток, платіжні процесори та інше). Втім, їх ефективне функціонування ускладнює постійна зміна обсягу, швидкості і різноманітності атак, які варіюються від відмови в обслуговуванні до зловмисного викрадення зсередини. Наслідки витоку даних далекосяжні та критичні [13]. Зі збільшенням кількості резонансних порушень систем кібербезпеки, підвищення рівня фінансових втрат у випадку реалізації загроз, для власників та керівників питання побудови безпекоорієнтованого бізнес-середовища є першочерговим.

Таким чином, перехід від концепції «безпеки за проектом» до «стійкості за проектом» є необхідним етапом еволюції кібербезпеки, який відповідає сучасним реаліям. Цей підхід дозволяє створювати системи, що не лише захищають, але й забезпечують безперервність бізнес-процесів навіть в умовах кризових ситуацій.

Застосування новітніх технологій, таких як штучний інтелект, квантові обчислення, є критично важливим для зміцнення національної безпеки та підвищення конкурентоспроможності економічних суб'єктів. Водночас, їх впровадження вимагає постійних інвестицій в системи захисту від кіберзагроз. Запропонована стратегія кіберстійкості на основі підходу «стійкості за проєктом» передбачає превентивні заходи щодо запобігання несанкціонованому доступу до систем, виявлення та усунення потенційних вразливостей, а також створення умов для адаптивного реагування на нові загрози. Цей підхід демонструє, як інноваційні технології можуть бути інтегровані у бізнес-процеси з урахуванням вимог кібербезпеки, забезпечуючи одночасно ефективність, надійність і захист інфраструктури. Водночас реалізація підходу «стійкості за проєктом» пов'язана з низкою викликів, зокрема високими початковими витратами на розробку та впровадження інфраструктури; складністю забезпечення міждисциплінарної співпраці між технічними, бізнесовими та правовими фахівцями; необхідністю постійного навчання й підвищення кваліфікації персоналу для роботи з новими технологіями.

Висновки. Проривні досягнення у штучному інтелекті, хмарних технологіях, інтернет-речах, продуктивності та природі обчислювальних засобів, можливостях зберігання обробки та передачі великих масивів даних та інформації (Big Data), засобах і технологіях їх реалізації вимагають принципово нових підходів до забезпечення інформаційної безпеки економічних суб'єктів. Можливості і вразливості сучасних інформаційно-комунікаційних та кібернетичних систем все більше залежать від зростання взаємозв'язків між ними в багатопараметричному, багатовимірному кіберпросторі та їх інформаційно-кібернетичного взаємопроникнення, взаємодії і взаємозалежності, тощо. Таким чином, умови цифрової трансформації вимагають впровадження нового безпекового підходу до функціонування бізнесу. Цей підхід орієнтований не лише на безпеку в поточний момент, а на перспективну стійкість суб'єктів та їх адаптивність, здатність оперативно реагувати на новий ландшафт загроз. В його основі безперервний моніторинг та постійне вдосконалення задля формування стійкої цифрової екосистеми бізнесу.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Onyshchenko S., Yanko A., Hlushko A. and Maslii O. Economic cybersecurity of business in Ukraine: strategic directions and implementation mechanism, in Economic and cyber security. Kharkiv: PC TECHNOLOGY CENTER, 2023. Pp. 30–58. DOI: https://doi.org/10.15587/978-617-7319-98-5.ch2

2. Krasnobayev V., Yanko A., Hlushko A. Information Security of the National Economy Based on an Effective Data Control Method. *Journal of International Commerce, Economics and Policy*. 2023. Vol. 14(03). DOI: https://doi.org/10.1142/S1793993323500217

3. Siebell T. M. Digital Transformation: Survive and Thrive in an Era of Mass Extinction. New York: RosettaBooks, 2019. 256 p.

4. Swain A., Swain K.P., Pattnaik S.K., Samal S.R., Das J.K. Cybersecurity in Digital Transformations. In: Mohanty, M.N., Das, S. (eds) Advances in Intelligent Computing and Communication. *Lecture Notes in Networks and Systems*. 2022. Vol. 430. DOI: https://doi.org/10.1007/978-981-19-0825-5_26

5. Corallo A., Lazoi M., Lezzi M. Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. *Computers in industry*. 2020. Vol. 114.

6. Бугріменко Р., Смірнова П. Вплив розвитку цифрової трансформації на діяльність підприємства. *Економіка та суспільство*. 2024. № 59. DOI: https://doi.org/10.32782/2524-0072/2024-59-29

7. Іванченко Н.О., Кудрицька Ж.В., Рекачинська К.В. Бізнес-модель в умовах цифрових трансформацій. *Вчені записки ТНУ імені В. І. Вернадського*. 2020. №3. С. 185–190.

8. Gartner. Top Cybersecurity Trends and Strategies for Securing the Future. 2024. URL: https://www.gartner.com/en/cybersecurity/topics/cybersecurity-trends

9. McKinsey & Company. Technology Trends Outlook 2023. URL: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-top-trends-in-tech-2023

10. Onyshchenko S., Zhyvylo Ye., Hlushko A., Bilko S. Cyber risk management technology to strengthen the information security of the national economy. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*. 2024. Vol. 5. P. 136–142. DOI: https://doi.org/10.33271/nvngu/2024-5/136

11. World Economic Forum, Navigating cyber resilience in the age of emerging technologies: Collaborative solutions for complex challenges, 2024. URL: https://www3.weforum.org/docs/WEF_Navigating_Cyber_Resilience_ in_the_Age_of_Emerging_ Technologies_2024.pdf

12. Shefer O., Laktionov O., Pents V., Hlushko A., and Kuchuk N. Practical Principles of Integrating Artificial Intelligence into the Technology of Regional Security Predicting. *Advanced Information Systems*. 2024. Vol. 8(1). P. 86–93. DOI: https://doi.org/10.20998/2522-9052.2024.1.11

13. Буряк А.А., Маслій О.А. Трансформація загроз економічній безпеці та безпеці інформаційного середовища України в умовах повномасштабної війни. *Держава та регіони. Серія : Економіка та підприємництво*. 2023. № 3 (129). С. 28–32.

14. Янко А.С., Вигівський Р.А. Система захисту комп'ютерної мережі. *Системи управління, навігації та зв'язку. Збірник наукових праць*. 2022. Т. 2, № 68. С. 91–94. DOI: https://doi.org/10.26906/sunz.2022.2.091

REFERENCES:

1. Onyshchenko S., Yanko A., Hlushko A. and Maslii O. (2023). Economic cybersecurity of business in Ukraine: strategic directions and implementation mechanism, in Economic and cyber security. Kharkiv: PC TECHNOLOGY CENTER, 2023, pp. 30–58. DOI: https://doi.org/10.15587/978-617-7319-98-5.ch2

2. Krasnobayev V., Yanko A., Hlushko A. (2023). Information Security of the National Economy Based on an Effective Data Control Method. *Journal of International Commerce, Economics and Policy*, vol. 14(03). DOI: https://doi.org/10.1142/S1793993323500217

3. Siebell T. M. (2019) Digital Transformation: Survive and Thrive in an Era of Mass Extinction. New York: RosettaBooks, 256 p.

4. Swain A., Swain K.P., Pattnaik S.K., Samal S.R., Das J.K. (2022). Cybersecurity in Digital Transformations. In: Mohanty, M.N., Das, S. (eds) Advances in Intelligent Computing and Communication. *Lecture Notes in Networks and Systems*, vol 430. DOI: https://doi.org/10.1007/978-981-19-0825-5_26

5. Corallo A., Lazoi M., Lezzi M. (2020). Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. *Computers in industry*, vol. 114.

6. Buhrimenko R., Smirnova P. (2024). Vplyv rozvytku tsyfrovoi transformatsii na diialnist pidpryiemstva [The impact of digital transformation on the company's operations]. *Ekonomika ta suspilstvo*, no. 59. DOI: https://doi.org/10.32782/2524-0072/2024-59-29

7. Ivanchenko, N. O., Kudrytska, Zh. V. and Rekachyns'ka, K. V. (2020) Biznes-model v umovakh tsyfrovykh transformatsii [Business model in the conditions of digital transformations]. *Vcheni zapysky TNU imeni V. I. Vernads'koho*, no. 3, pp. 185–190.

8. Gartner (2024). Top Cybersecurity Trends and Strategies for Securing the Future. Available at: https://www.gartner.com/en/cybersecurity/topics/cybersecurity-trends (accessed 10 April 2025)

9. McKinsey & Company (2023). Technology Trends Outlook 2023. Available at: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-top-trends-in-tech-2023 (accessed 10 April 2025)

10. Onyshchenko S., Zhyvylo Ye., Hlushko A., Bilko S. (2024). Cyber risk management technology to strengthen the information security of the national economy. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*, no. 5, pp. 136–142. DOI: https://doi.org/10.33271/nvngu/2024-5/136

11. World Economic Forum, Navigating cyber resilience in the age of emerging technologies: Collaborative solutions for complex challenges, 2024. Available at: https://www3.weforum.org/docs/WEF_Navigating_Cyber_Resilience_ in_the_Age_of_Emerging_ Technologies_2024.pdf (accessed 10 April 2025)

12. Shefer O., Laktionov O., Pents V., Hlushko A., and Kuchuk N. (2024). Practical Principles of Integrating Artificial Intelligence into the Technology of Regional Security Predicting. *Advanced Information Systems*, vol. 8(1), pp. 86–93. DOI: https://doi.org/10.20998/2522-9052.2024.1.11

13. Buriak A.A., Maslii O.A. (2023). Transformatsiia zahroz ekonomichnii bezpetsi ta bezpetsi informatsiinoho seredovyshcha Ukrainy v umovakh povnomasshtabnoi viiny [Transformation of Threats to Economic Security and Security of the Information Environment of Ukraine in the Context of a Full-Blown War]. *Derzhava ta rehiony. Seriia : Ekonomika ta pidpryiemnytstvo*, vol. 3 (129), p. 28–32.

14. Yanko A.S., Vyhivskyi R.A. (2022). Systema zakhystu kompiuternoi merezhi. Systemy upravlinnia, navihatsii ta zviazku [Computer network protection system]. *Zbirnyk naukovykh prats*, vol. 2(68), pp. 91–94. DOI: https://doi.org/10.26906/sunz.2022.2.091