DOI: https://doi.org/10.32782/2524-0072/2024-64-37

УДК 336.658

КІБЕРБЕЗПЕКА В СИСТЕМІ ФОРМУВАННЯ БІЗНЕС-МОДЕЛІ ПІДПРИЄМСТВА В УМОВАХ ЦИФРОВОЇ ЕКОНОМІКИ

CYBER SECURITY IN THE SYSTEM OF FORMING THE BUSINESS MODEL OF THE ENTERPRISE IN THE CONDITIONS OF THE DIGITAL ECONOMY

Шостак Людмила Василівна
кандидат економічних наук, доцент,
Волинський національний університет імені Лесі Українки
ORCID: https://orcid.org/0000-0001-8786-9582

Федонюк Анатолій Ананійович
кандидат фізико-математичних наук, доцент,
Волинський національний університет імені Лесі Українки
ORCID: https://orcid.org/0000-0003-0942-227X

Помазун Олена Олександрівна
асистент,
Луцький інститут розвитку людини Університету «Україна»
ORCID: https://orcid.org/0009-0003-0803-6307

Shostak Liudmyla, Fedoniuk Anatolii
Lesya Ukrainka Volyn National University

Pomazun Olena
Lutsk Institute of Human Development of the University "Ukraine"

Дана стаття присвячена проблемі забезпечення кібербезпеки в системі формування бізнес-моделі в умовах цифрової економіки, що стало особливо актуальним в останні роки військових дій на території нашої держави. Саме збільшення кількості кібератак зумовлює формування інноваційних систем захисту вітчизняного бізнесу. Авторами статті значна увага приділяється дослідженню особливостям цифрової економіки, яка характеризується активним використанням цифрових технологій для створення, розповсюдження і використання товарів та послуг, стрімко змінює ландшафт сучасного бізнесу. В дослідженні зазначається, що інноваційні бізнес-моделі, засновані на цифрових технологіях, стимулюють економічне зростання та забезпечують конкурентоспроможність підприємств. Однак, поряд із цими можливостями зростають і ризики, пов'язані з кібербезпекою. В умовах сучасної економіки питання захисту цифрових активів набуває стратегічного значення.

Ключові слова: кібербезпека, бізнес-модель, цифрова економіка, цифрова трансформація, кібератака, інформаційна безпека.

This article is devoted to the problem of ensuring cyber security in the system of forming a business model in the conditions of the digital economy, which has become especially relevant in recent years of military operations on the territory of our country. It is the increase in the number of cyberattacks that determines the formation of innovative systems for the protection of domestic business. The authors of the article pay considerable attention to the study of the features of the digital economy, which is characterized by the active use of digital technologies for the creation, distribution and use of goods and services, rapidly changing the landscape of modern business. The study notes that innovative business models based on digital technologies stimulate economic growth and ensure the competitiveness of enterprises. However, along with these opportunities, the risks associated with cyber security are also growing. In the conditions of the modern economy, the issue of protection of digital assets acquires strategic importance. Every year, the number of cyber attacks increases. Companies are increasingly being targeted by hackers who use a variety of methods, from phishing to sophisticated zero-day attacks. An important problem for domestic business is the fact that the technologies used by cybercriminals are constantly improving, which makes

it difficult to detect and neutralize them. Cyberattacks can cause significant financial losses, both direct (ransom payments, data recovery) and indirect (loss of customer trust, reputational damage). Unfortunately, attacks can lead to a temporary stoppage of business processes, which also affects the company's revenue and productivity. Many countries are introducing laws requiring companies to maintain a certain level of cybersecurity. Failure to comply with these requirements may result in fines and other sanctions. The application of cloud technologies, the Internet of Things (IoT) and big data (Big Data) require special attention, which creates new attack vectors that require appropriate measures of modern protection. The relevance of cyber security research in the system of business model formation in the conditions of the digital economy is due to the need to protect digital assets, ensure business continuity and fulfill regulatory requirements. Cybersecurity is becoming not only a technical issue, but also a strategic factor for business success in the digital age. Therefore, the study and implementation of effective cyber security measures is critically important for modern enterprises that seek to ensure their stability and competitiveness in the market.

Keywords: cyber security, business model, digital economy, digital transformation, cyber attack, information security.

Постановка проблеми. Цифрова економіка кардинально змінює підходи до ведення бізнесу, де ключовими факторами виробництва є дані в цифровому вигляді та діяльність по створенню, розповсюдженню і використанню цифрових технологій. В умовах постійно зростаючої кількості кіберзагроз, бізнес змушений швидко адаптувати свої бізнес-моделі для забезпечення ефективного функціонування та захисту своїх цифрових активів.

Проте під час кризи, цифровізації бізнес не лише знаходить нові можливості для ефективного розвитку, але щоб протистояти новим неочікуваним викликам, підприємцям доводиться швидко та докорінно змінювати підходи до ведення бізнесу. Це вимагає від них впровадження нових стратегій, підвищення гнучкості та адаптивності бізнес-моделей, а також інвестування в кібербезпеку.

Аналіз останніх досліджень і публікацій. Розгляду кіберзагроз та протидії їм присвячено багато наукових досліджень, проведених вітчизняними науковцями, такими як О. Баранов, М. Гончар, Р. Грищук, В. Дудикевич, К. Молодецька, А. Ребець, О. Ткаченко, К. Яковів та іншими.

Однак їхні роботи переважно зосереджуються на правовому регулюванні та формуванні системи інформаційної безпеки в Україні. Маловивченими залишаються питання впливу кібербезпеки на формування та розвиток цифрової економіки та формуванні бізнес-моделей вітчизняного бізнесу.

Це вимагає подальшого дослідження для розуміння того, як забезпечення кібербезпеки може підтримувати та стимулювати зростання цифрової економіки, зокрема через аналіз впливу на бізнес-моделі, технологічні інновації та загальну конкурентоспроможність підприємств у цифровій епосі.

Виділення невирішених раніше частин загальної проблеми. Прискорений розвиток цифровізації вимагає не лише переорієнтацію підприємств у цифрове середовище та трансформацію бізнес-моделей, але й комплексне врізання систем захисту кібербезпеки у використовувані моделі розвитку вітчизняного бізнесу.

Формулювання цілей статті (постановка завдання). Метою даного дослідження є встановлення місця цібербезпеки в системі формування бізнес-моделі підприємства в умовах цифровізації суспільства, використання позитивних а негативних наслідків діджиталізації при створенні комплексного захисту від кібератак та усестороннього захисту бізнесу.

Виклад основного матеріалу дослідження. Сучасні технологічні тенденції, такі як електронна комерція, блокчейн, Інтернет речей, комп'ютерний інжиніринг, сучасні технології бездротового зв'язку, поширення нових бізнес-моделей в умовах використання передових цифрових технологій, хмарні обчислення, аналіз великих даних створюють всі можливості для нової якості ведення бізнесу. В той же час, поряд з інноваційністю, з'являється деяке ускладнення і прискорення в умовах цифрового середовища, що викликає проблему становлення цифрової безпеки в умовах воєнного стану в Україні [1].

Поряд з пріоритетністю захисту вітчизняного бізнесу від активних кібератак постало питання осучаснення механізму формування бізнес-моделей вітчизняного бізнесу та обов'язкове врахування кібербезпеки, як незаперечного чинника ефективного захисту підприємства.

Формування бізнес-моделі підприємства в умовах цифрової економіки вимагає врахування усіх чинників інформатизації, вміння обробляти великі масиви інформації, вио-

кремлення найбільш важливою та достовірної інформації.

Формування бізнес-моделі підприємства в умовах цифрової економіки має свої особливості, які визначають успішність функціонування та розвиток підприємства. Цифрова трансформація сприяє активній автоматизації процесів, що підвищує ефективність та знижує витрати. У свою чергу інтеграція інноваційних технологій, таких як штучний інтелект, машинне навчання та блокчейн.

Цифрове переосмислення розвитку підприємств передбачає використання сучасних технологій та трансформацію бізнес-моделей, шляхом використання нових розробок типу інжинірингу, використання у виробництві робот-технологій, штучного інтелекту, блокчейну, хмарних технологій.

Незважаючи на переваги і новий горизонт можливостей розвитку бізнесу, вдосконалена операційна модель несе в собі і додаткові уразливості, збільшуючи придатну для кібератак «площу» IT-систем. Нездатність адекватно інвестувати в безпеку в потрібних областях може привести до того, що весь бізнес опиниться під загрозою. Навіть спочатку закриті промислові IT-системи, які не були призначені для підключення до інтернету, з настанням ери загальної мережевої пов'язаності стали доступні для віддаленої атаки з будь-якої точки світу в будь-який час [2].

При зборі та аналізі великого масиву даних для створення персоналізованих клієнтських пропозицій та покращення клієнтського досвіду варто використовувати соціальні мережі, мобільні додатки й інші цифрові платформи для взаємодії зі споживачами.

Формування сучасних цифрових бізнес-моделей характеризується гнучкістю та адаптивністю, тобто можливостями швидко адаптуватись до змін ринку та нових технологічних викликів, а використання агентських моделей управління бізнесом дозволяють швидше приймати рішення та впроваджувати ефективні зміни.

Ми живемо в світі, де якщо щось не знаходиться в Інтернеті, то це існує лише уявно. У цифрову епоху бізнеси змушені модифікувати свої бізнес-моделі, щоб відповідати новій реальності. Цифрова сфера створила попит на нові бізнес-моделі, які допомагають клієнтам швидко та зручно отримувати доступ до будь-якого продукту чи сервісу онлайн. Це допомагає компаніям залишатися актуальними та забезпечувати відповідну якість обслуговування [3].

Сучасні бізнес-моделі обов’язково повинні враховувати необхідність розвиток онлайн-продажів та платформ для електронної комерції та оптимізації процесів доставки й управління запасами як основного критерію ефективного розвитку бізнесу в умовах цифрової економіки.

Використання хмарних технологій для зберігання даних та обчислювальних ресурсів можливе при забезпеченні кібербезпеки та захисту конфіденційної інформації.

При використанні аналітичних інструментів для аналізу ринкових тенденцій та прогнозування розвитку бізнесу передбачається прийняття рішень щодо захисту від кібератак з використанням цифрових масивів даних.

Використання IoT для моніторингу та управління виробничими процесами, шляхом збору даних з підключених пристроїв для аналізу та оптимізації процесів.

Ці особливості формування бізнес-моделі в умовах цифрової економіки дозволяють підприємствам бути конкурентоспроможними, ефективними та готовими до швидких змін у ринковому середовищі.

Визначені елементи макету бізнес-моделі можуть бути так званою точкою «старту» при здійсненні моделювання діяльності бізнесу. Цифрова трансформація дозволяє адаптувати бізнес-модель під будь-які зміни зовнішнього та внутрішнього середовища, визначити ступінь зрілості на кожному етапі життєвого циклу, адаптації до нових концепцій цифровізації. Практичне застосування бізнес-моделей можливе за умови достовірного статистичного підґрунтя її формування та коригування, залучення фахівців-практиків у обраній галузі для уточнення її ефективності. Варто зазначити, що загальна структура бізнес-моделі є універсальною, з можливістю до удосконалення [4].

Саме в контексті постійної динамічності економічної національної системи та постійних викликів для діяльності підприємства варто постійно переглядати основні компоненти бізнес-моделей та трансформувати їх в залежності від пріоритетності загроз. Останніми роками особливої уваги вимагають кіберзагрози та атаки, причому в умовах цифрової трансформації, де у відкритий доступ потрапляє не лише фінансова звітність підприємства, але й з’являється можливість «отримати» й закриту інформацію необхідно створювати комплексну систему захисту, яка буде корелюватись зі стратегією розвитку та бізнес-моделлю розвитку бізнесу.

На думку авторів, при формуванні цифрової бізнес-моделі необхідно враховувати наступні компоненти кібезбезпеки, які мають досить суттєві наслідки для функціонування вітчизняного бізнесу:

1) Інформаційна безпека, яка передбачає захист даних, шляхом використання шифрування та інших технологій для захисту конфіденційної інформації, а також контроль доступу через встановлення чітких політик доступу до інформаційних ресурсів підприємства;

Статистикою підтверджено, що 96 % кібератак і витоку даних розпочинається з e-mail. E-mail захищений так само, як поштова листівка, адже електронні листи “проходять” через вразливі та потенційно небезпечні поштові сервери. При цьому, SSL/TSL не гарантує безпеки. Сьогодні перехоплення даних та “взлом” можливі всього за $ 200, а мережеві імпланти для перехоплення трафіку коштують всього від $ 60. Не дивно, що браузери надзвичайно вразливі до “взломів”. Email інфраструктура не верифікує відправника. Засоби захисту периметру компанії не захищають e-mail після відправки листів [1].

2) Операційна безпека, яка може забезпечуватись моніторингом та управлінням інцидентами для виявлення та реагування на кіберзагрози та плануванням відновлення після інцидентів можна через розробку планів відновлення для мінімізації втрат у випадку кіберінцидентів.

Реагування на інциденти означає здатність організації реагувати на ситуацію, що виникла, якомога швидше та ефективніше; тоді як кризове управління означає здатність організації належним чином управляти кризою, щоб усі сторони, зокрема зовнішні суб'єкти, розуміли поточний стан організації та її план дій. Комунікація з внутрішніми і зовнішніми партнерами, а також управління повідомленнями, пов'язаними з кіберподією, є невід'ємною частиною плану управління кризою та реагування на неї [5].

3) Інфраструктурна безпека, яку необхідно забезпечувати безпекою мережі з використанням фаєрволів, VPN та інших засобів для захисту мережевої інфраструктури. Паралельно варто забезпечувати захист хмарних сервісів, що можливе впровадженням засобів захисту для забезпечення безпеки даних, що зберігаються у хмарі;

Інфраструктурна безпека з одного боку полегшується цифровізацією бізнес-середовища, але з іншого боку – режими он-лайн роблять будь-яку систему уязвимою до кібератак.

Цифровізація бізнес-середовища передбачає взаємозв’язок між учасниками процесів у режимі он-лайн, який проявляється через матрицю електронного простору. Її особливістю є взаємодія суб’єктів цифрового бізнес-середовища – між представниками бізнесу, споживачами та державними органами [6].

4) Управління ризиками, шляхом оцінки кіберзагроз та вразливостей, а також впровадженням заходів для зменшення впливу імовірних кіберзагроз;

5) Навчання та підготовка персоналу щодо найкращих практик кібербезпеки й проведення регулярних тренувань для підготовки персоналу до реагування на кіберзагрози.

Так зване врізання перелічених компонентів у бізнес-модель підприємства дасть можливість захистити інформацію та діяльність підприємства від кібератак та негативних можливих наслідків.

При формуванні сучасної бізнес-моделі підприємства в умовах цифрової економіки необхідно проаналізувати можливі варіанти кібератак та їх наслідки для вітчизняного бізнесу. Кібератаки можуть мати значний вплив на бізнес-моделі підприємств, створюючи серйозні ризики та виклики (табл. 1).

Виходячи з можливих кібератак авторами пропонується застосовувати стратегії мінімізації ризиків, які досить вдало корелюватимуться з будь-якими бізнес-моделями, підлягатимуть правкам та враховуватимуть особливості цифровізації.

На нашу думку, найбільш вдалими стратегіями є наступні:

– стратегія захисту даних, яка передбачає використання шифрування, регулярне резервне копіювання даних та інших методів захисту даних;

– стратегія кібербезпеки, шляхом впровадження сучасних систем кібербезпеки та антивірусного програмного забезпечення, а також постійний моніторинг та аналіз загроз;

– стратегія відновлення, яка забезпечуватиметься розробкою планів відновлення після інцидентів та регулярне їх тестування, впровадженням систем швидкого відновлення даних та інфраструктури;

– стратегія нульової довіри – перехід до широкої моделі безпеки, яка дозволить підприємствам обмежити доступ до цінних застосунків, даних і середовища компанії. Це буде зроблено таким чином, щоб не загро-

Таблиця 1

Кібератаки: характеристика та наслідки

Вид кібератаки	Опис	Наслідки
Фішинг	Спроба отримати конфіденційну інформацію шляхом маскування під надійне джерело	Крадіжка облікових даних, фінансових ресурсів та конфіденційної інформації
Зловмисне програмне забезпечення (Малваре)	Шкідливе програмне забезпечення, яке може включати віруси, трояни, шпигунські програми тощо	Пошкодження даних, порушення роботи систем, крадіжка інформації
Атаки типу «відмова в обслуговуванні» (DDoS)	Перевантаження системи або мережі, що робить її недоступною для користувачів	Втрати доходів через простої, зниження продуктивності та погіршення репутації.
Атаки на ланцюг постачання	Злом постачальників або партнерів для отримання доступу до основної компанії	Порушення роботи ланцюгів постачання, втрати даних
Інсайдерські атаки	Атаки з боку співробітників або інших осіб з доступом до внутрішніх систем	Втрати конфіденційної інформації, фінансові втрати
Вимагальне програмне забезпечення (Рансомваре)	Програмне забезпечення, яке блокує доступ до систем або даних до сплати викупу	Втрати даних, фінансові втрати, пошкодження репутації

Джерело: сформовано авторами

жувати продуктивності працівників або користувацькому досвіду [7].

Реалізація цих стратегій допоможе підприємствам знизити ризики кібератак та мінімізувати їх наслідки, забезпечуючи безперебійну роботу та захист своїх активів.

Висновки. В умовах цифрової економіки кібербезпека стає невід'ємною частиною формування бізнес-моделі будь-якого підприємства. Ефективний кіберзахист дозволяє бізнесу не лише захищати свої активи, але й підвищувати свою конкурентоспроможність на ринку.

Успішний бізнес – це ціль, до якої прагне будь-який підприємець. Вона також важлива для споживачів, які хочуть отримати задоволення від володіння або використання певного продукту; для послідовників, які надихаються ідеями для створення чи підвищення рівня власних сервісів; і, звичайно ж, для конкурентів, які прагнуть зупинити ріст та розвиток.

Багато компаній щонайменше один раз на рік зазнають зовнішньої атаки або стикаються з внутрішніми інцидентами інформаційної безпеки.

Бізнес повинен сформувати більш глибоке розуміння сучасних кібер-ризиків, забезпечити належний моніторинг та розробити плани швидкого реагування, не обмежуючись лише заходами запобігання ризикам.

Кібербезпека – це складний процес, але вона є обов'язковою складовою успішного бізнесу. У сучасну епоху Інтернету кожна організація стає цифровою, використовуючи новітні технології та процеси, а також застосовуючи нові принципи організації праці. Кожна складова бізнес-процесів є лише окремою ланкою в нескінченному ланцюзі взаємопов'язаних елементів. Сьогодні компаніям складніше ніж будь-коли чітко визначити критичні точки у власній багатогранній інфраструктурі, через яку вони взаємодіють із зовнішнім світом. Такі умови створюють підґрунтя для хакерських атак.

Зловмисники можуть націлюватися на компанії різного масштабу та галузей діяльності. Найчастіше заходи безпеки визначаються рівнем загроз і ризиків. На жаль, кіберпростір насичений загрозами, тому заходи для запобігання атакам повинні відповідати рівню ризику, оскільки тактика і методи кіберзлочинців постійно змінюються.

Отже, кібербезпека є не лише технічним аспектом, але й стратегічним фактором, що впливає на всі елементи бізнес-моделі. Захист цифрових активів, забезпечення безперервності бізнес-процесів та збереження довіри клієнтів є ключовими для успішного функціонування бізнесу в умовах цифрової економіки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Краус К. М., Краус Н. М., Штепа О. В. Цифрова трансформація кібербезпеки на мікрорівні в умовах воєнного стану. *Innovation and Sustainability.* 2022. № 3. С. 26–37.
2. Кібербезпека: як захистити підприємство в епоху Індустрії X.0. URL: https://www.telesphera.net/blog/kiberbezpeka-indystrii-x-0.html
3. Шостак Л. В., Більо І. О., Ульяницький А. О. Бізнес-моделі підприємства у цифрову епоху: зарубіжний досвід. *Економіка та суспільство*. 2024. № 60. URL: https://economyandsociety.in.ua/index.php/journal/article/view/3702
4. Шостак Л. В., Федонюк А. А., Бегун С. І. Статистичне підґрунтя формування бізнес-моделі підприємства в умовах цифрової трансформації. *Приазовський економічний вісник*. 2023. № 4 (36). URL: http://pev.kpu.zp.ua/vypusk-36
5. Чотири елементи сильної стратегії кібербезпеки. URL: https://www.bdo.ua/uk-ua/insights-2/information-materials/2024/four-elements-of-a-strong-cybersecurity-strategy
6. Шостак Л., Більо І., Микитюк Є. Потенціал цифровізації вітчизняного бізнес-середовища. *Економічний аналіз*. 2021. Том 31. № 1. С. 245–251.
7. Захист бізнесу: як убезпечити підприємство від кіберзлочинів? URL: https://www.bdo.ua/uk-ua/insights-2/information-materials/2024/business-security-how-to-protect-your-company-from-cybercrime

REFERENCES:

1. Kraus K. M., Kraus N. M., Shtepa O. V. (2022) Tsyfrova transformatsiia kiberbezpeky na mikrorivni v umovakh voiennoho stanu [Digital transformation of cyber security at the micro level in martial law]. *Innovation and Sustainability*. № 3. P. 26–37.
2. Kiberbezpeka: yak zakhystyty pidpryiemstvo v epokhu Industrii X.0 [Cyber security: how to protect the enterprise in the era of Industry X.0]. Available at: https://www.telesphera.net/blog/kiberbezpeka-indystrii-x-0.html
3. Shostak L. V., Bilo I. O., Ulianytskyi A. O. (2024) Biznes-modeli pidpryiemstva u tsyfrovu epokhu: zarubizhnyi dosvid [Business models of the enterprise in the digital age: foreign experience]. *Ekonomika ta suspilstvo*. № 60. Available at: https://economyandsociety.in.ua/index.php/journal/article/view/3702
4. Shostak L. V., Fedoniuk A. A., Behun S. I. (2023) Statystychne pidgruntia formuvannia biznes-modeli pidpryiemstva v umovakh tsyfrovoi transformatsii [The statistical basis of the formation of the business model of the enterprise in the conditions of digital transformation]. *Pryazovskyi ekonomichnyi visnyk*. № 4 (36). Available at: http://pev.kpu.zp.ua/vypusk-36
5. Chotyry elementy sylnoi stratehii kiberbezpeky [The four elements of a strong cybersecurity strategy]. Available at: https://www.bdo.ua/uk-ua/insights-2/information-materials/2024/four-elements-of-a-strong-cybersecurity-strategy
6. Shostak L., Bilo I., Mykytiuk Ye. (2021) Potentsial tsyfrovizatsii vitchyznianoho biznes-seredovyshcha [The potential of digitization of the domestic business environment]. *Ekonomichnyi analiz*. Tom 31. № 1. P. 245–251.
7. Zakhyst biznesu: yak ubezpechyty pidpryiemstvo vid kiberzlochyniv? [Business protection: how to protect an enterprise from cybercrimes]. Available at: https://www.bdo.ua/uk-ua/insights-2/information-materials/2024/business-security-how-to-protect-your-company-from-cybercrime