УДК 332.122.54:338.14
JEL Classification: G 32, O 10, H 56, D 81
DOI: *http://doi.org/10.34025/2310-8185-2024-2.94.01*

Оксана Верстяк, к.е.н., доцент,
https://orcid.org/0000-0002-4222-4964
Чернівецький торговельно-економічний інститут ДТЕУ,
м. Чернівці

СТРАТЕГІЇ Й ТАКТИКИ ПІДВИЩЕННЯ БЕЗПЕКИ БІЗНЕСУ

Анотація

Актуальність. Постановка проблеми. У сучасному бізнес-середовищі безпека стала критичним фактором, який безпосередньо впливає на успіх і стійкість компаній. Кілька аспектів підкреслюють актуальність дослідження стратегій і тактик підвищення безпеки бізнесу: розвиток технологій та Інтернету призвів до збільшення кількості та складності кіберзагроз. Кіберзлочинці постійно удосконалюють свої методи атак, що вимагає від бізнесу постійного оновлення захисних заходів. В умовах глобалізації та економічної нестабільності зростає ризик фінансових махінацій, шахрайства і промислового шпіонажу. Ефективні стратегії безпеки допомагають мінімізувати ці ризики; зростаюча кількість законодавчих та регуляторних вимог у сфері безпеки (наприклад, GDPR в Європі) вимагає від компаній дотримання високих стандартів безпеки. Невиконання цих вимог може призвести до значних штрафів та втрати репутації; політична нестабільність, конфлікти, терористичні загрози створюють додаткові виклики для безпеки бізнесу. Компанії повинні бути готові до швидкого реагування на ці загрози.

Загрози для бізнесу мають багатовимірний характер, охоплюючи кібербезпеку, фізичну безпеку, інформаційну безпеку та економічні ризики. Це ускладнює розробку універсальних стратегій захисту. Часто безпека розглядається як окремий елемент, що не інтегрований у загальні бізнес-процеси компанії. Це призводить до неефективного використання ресурсів та низької ефективності заходів безпеки.

Актуальність та проблематика дослідження стратегій і тактик підвищення безпеки бізнесу обумовлені комплексністю сучасних загроз, необхідністю інтеграції безпеки у всі бізнес-процеси, динамічним характером ризиків та обмеженими ресурсами. Вивчення та впровадження ефективних стратегій безпеки є критично важливими для забезпечення стабільної та успішної діяльності компаній у сучасному світі.

Мета дослідження – створення практичних інструментів та рекомендацій, які допоможуть підприємствам ефективно захищати свої активи від різних загроз. Це сприятиме підвищенню стійкості та конкурентоспроможності компаній в умовах постійно змінюваного бізнес-середовища.

Методологія. Вирішення поставлених у статті завдань здійснено за допомогою загальнонаукових методів дослідження, а саме: аналізу, систематизації та узагальнення. Методологічну основу дослідження складають логічно-діалектичні методи наукового пізнання, методи системного аналізу, а також спеціальні методи, зокрема методи аналізу та синтезу.

Результати. У статті досліджено принципи кібербезпеки підприємства, а саме те, що безпека бізнесу вимагає комплексного підходу, який включає фізичну, інформаційну та фінансову безпеку. Ефективна стратегія повинна враховувати всі можливі загрози і вразливості, що можуть виникнути в бізнес-процесах. Висвітлено основні типи загроз, з якими стикається підприємство. Розглянуто розподіл викликів і загроз економічній безпеці. **Практичне значення**. Запропоновано практичні інструменти та рекомендації для захисту активів підприємств від загроз.

Перспективи подальших досліджень. Подальші дослідження передбачають дослідження методів інтеграції безпеки у стратегічне планування компаній, розробка моделей управління ризиками, які враховують безпеку як ключовий елемент бізнес-стратегії.

Ключові слова: кіберзагрози, сталий розвиток, інтеграція, соціальний, економічний розвиток.

Кількість джерел: 5; кількість рисунків: 1, кількість таблиць: 1.

Oksana Verstiak, Candidate of Economic Sciences,
Associate Professor,
https://orcid.org/0000-0002-4222-4964
Chernivtsi Institute of Trade and Economic of SUTE, Chernivtsi

STRATEGIES AND TACTICS FOR ENHANCING BUSINESS SECURITY

Summary

In the modern business environment, security has become a critical factor that directly impacts the success and resilience of companies. Several aspects underscore the relevance of researching strategies and tactics for enhancing business security: the development of technology and the Internet has led to an increase in both the number and complexity of cyber threats. Cybercriminals continuously refine their attack methods, requiring businesses to constantly update their protective measures; in the context of globalization and economic instability, the risk of financial fraud, scams, and industrial espionage is rising. Effective security strategies help minimize these risks; the growing number of legislative and regulatory requirements in the field of security (e.g., GDPR in Europe) demands that companies adhere to high security standards. Failure to comply can result in significant fines and damage to

reputation; political instability, conflicts, and terrorist threats pose additional challenges to business security.

Companies must be prepared to respond swiftly to these threats. Business threats are multidimensional, encompassing cybersecurity, physical security, information security, and economic risks. This complexity makes it difficult to develop universal protection strategies. Security is often viewed as a separate element, not integrated into the company's overall business processes. This leads to inefficient use of resources and low effectiveness of security measures. The relevance and challenges of researching strategies and tactics for enhancing business security are driven by the complexity of modern threats, the need to integrate security into all business processes, the dynamic nature of risks, and limited resources. Studying and implementing effective security strategies is critically important for ensuring stable and successful business operations in the modern world.

The aim of the article is to create practical tools and recommendations that will help enterprises effectively protect their assets from various threats. This will enhance the resilience and competitiveness of companies in a constantly changing business environment. The tasks outlined in the article are addressed using general scientific research methods, namely analysis, systematization, and generalization. The methodological basis of the research includes logical-dialectical methods of scientific knowledge, methods of system analysis, as well as special methods, in particular, methods of analysis and synthesis.

Keywords: sustainable development, Integration, economic development.
Number of sources – 6, number of tables – 1, number of drawings – 1.

Постановка проблеми. Постановка проблеми безпеки бізнесу включає в себе визначення багатогранних загроз та розробку комплексних підходів до їхнього подолання. Вирішення цих питань є критично важливим для забезпечення стійкості та конкурентоспроможності компаній у сучасному динамічному бізнес-середовищі.

Аналіз останніх досліджень і публікацій. Базою для наукового дослідження слугували роботи вітчизняних і зарубіжних вчених-економістів, що вивчають проблематику кібербезпеки підприємств, загроз ведення бізнесу у дослідженнях багатьох вчених, зокрема це: Новікова О. Ф. (вивчала питання безпеки бізнесу з акцентом на розробку стратегій та тактик, спрямованих на підвищення його стійкості та захисту від різних загроз), Вдовічен А. А. (досліджує вивчення ризиків для підприємств у сучасних умовах та розробку стратегій для їхнього мінімізації), Королюк Ю. Г. (досліджує питання безпеки бізнесу з акцентом на методи

державного управління та економічної безпеки підприємств), Limba T. (питання безпеки бізнесу з акцентом на цифрові аспекти та використання інформаційних технологій для підвищення стійкості та безпеки підприємств), Plėta T. (питання безпеки бізнесу з акцентом на стратегії управління ризиками та кібербезпеку, особливо в контексті малих і середніх підприємств), Agafonov K. (питання стратегії і тактики підвищення безпеки бізнесу, зокрема питання кібербезпеки та організаційної стійкості), Damkus M. (стратегії та тактики підвищення безпеки бізнесу, зокрема в контексті цифрової трансформації та кібербезпеки) та інші.

Формулювання цілей статті й аргументування актуальності поставленого завдання. Метою статті є створення практичних інструментів та рекомендацій, які допоможуть підприємствам ефективно захищати свої активи від різних загроз. Для досягнення поставленої мети слід виконати такі завдання: виявити та класифікувати основні типи загроз, з якими стикаються підприємства, включаючи кіберзагрози, фізичні загрози, економічні ризики та соціально-політичні фактори.

Виклад основного матеріалу дослідження. Обов'язковим принципом кібербезпеки підприємств є кібергігієна (корпоративна та національна). Основні навички кібергігієни: людський фактор, технічні знання, приналежність, зовнішні фактори; регуляції та закони, інвентаризація активів, аналіз ризиків (кількісний та якісний) (рис. 1).

Важливою складовою економічної безпеки підприємства, що визначається в широкому контексті поняття «безпека», є його здатність до адаптації та утримання стабільності в умовах невизначеності та ризиків. Ураховуючи змінені обставини, важливо визначити стратегії, які дозволяють підприємствам ефективно функціонувати, зберігаючи високий рівень економічної безпеки [6].

Зупинимось більш детально на принципі аналізу ризиків. Підприємства стикаються з різними типами загроз, які можна класифікувати за кількома основними категоріями.

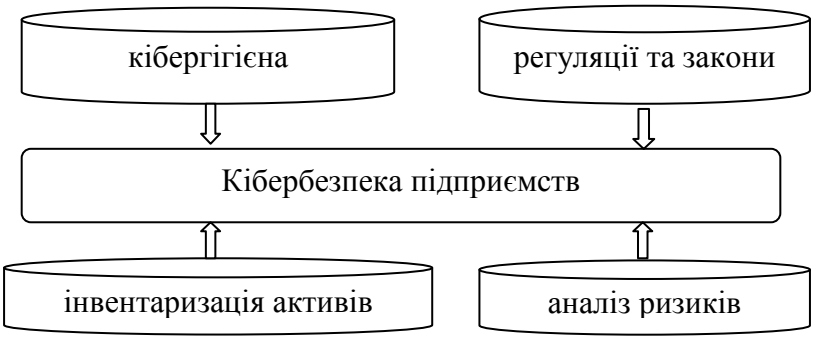

Рис. 1. Принципи кібербезпеки підприємств

Розуміння цих загроз є критично важливим для розробки ефективних стратегій та тактик безпеки. Основні типи загроз, з якими стикаються підприємства:

1. Кіберзагрози: *шкідливе програмне забезпечення* (віруси, трояни, черв'яки, шпигунські програми, програми-вимагачі (ransomware)); *фішинг та соціальна інженерія* (шахрайські електронні листи та повідомлення, що вводять в оману співробітників з метою отримання конфіденційної інформації); *атаки на відмову в обслуговуванні* (атаки, що перевантажують системи компанії, роблячи їх недоступними для користувачів); *неавторизований доступ та зломи* (неавторизований доступ до мережі або систем компанії для викрадення або зміни даних).

2. Економічні загрози: *фінансові махінації та шахрайство* (викрадення коштів, маніпуляції з фінансовими звітами, шахрайство з кредитами та платежами); *корпоративне шпигунство* (викрадення комерційної таємниці, інтелектуальної власності або конфіденційної інформації конкурентами або внутрішніми працівниками); *недобросовісна конкуренція* (використання незаконних методів для отримання переваг на ринку).

3. Фізичні загрози: *крадіжки та вандалізм* (крадіжки обладнання, сировини, продукції, а також пошкодження майна компанії); *природні катастрофи* (землетруси, повені, пожежі, урагани та інші природні явища, що можуть спричинити шкоду бізнесу); *терористичні акти та акти саботажу* (атаки,

спрямовані на знищення або пошкодження майна компанії, з метою створення паніки або завдання економічної шкоди).

4. Інформаційні загрози: *втрати даних* (втрата важливих даних через збій системи, помилки персоналу або природні катастрофи); *конфіденційність інформації* (розголошення конфіденційної інформації через помилки співробітників або зовнішні атаки).

5. Соціально-політичні загрози: *політична нестабільність* (зміни в політичній ситуації, що можуть призвести до змін у законодавстві, санкціях або економічних умовах); *трудові конфлікти* (страйки, протести та інші форми трудових конфліктів, що можуть перешкодити нормальній роботі підприємства); *репутаційні ризики* (негативні публікації, відгуки та інші фактори, що можуть вплинути на репутацію компанії).

У рамках проведеного експертного опитування було актуалізовано, визначено та оцінено 50 загроз за складовими частинами: макроекономічна, фінансова, інвестиційно-інноваційна, виробнича, зовнішньоекономічна, соціальна та продовольча безпека, які дозволяють сформувати уявлення про характер впливу війни на економічну безпеку України. Розподіл викликів і загроз економічній безпеці склав [2; 5]:

соціальна	22%
фінансова	16%
макроекономічна	14%
продовольча безпека	14%
зовнішньоекономічна	12%
інвестиційно-інноваційна	12%
виробнича	10%

Саме тому необхідно створення практичних інструментів і рекомендацій для захисту активів підприємств від загроз (табл. 1). Їх використання допоможе підприємствам створити комплексну систему захисту, яка враховує різні типи загроз і забезпечує ефективну безпеку активів.

Таблиця 1

Практичні інструменти та рекомдації для захисту активів підприємств від загроз

Кіберзагрози						
Інструменти				*Рекомендації*		
Антивірусні та антишпигунські програми	**Міжмережеві екрани** (використання фаєрволів для контролю доступу до мережі підприємства)	**Системи виявлення та запобігання вторгнень** (встановлення IDS/IPS для моніторингу та запобігання несанкціонованим доступам і атакам)	**Шифрування даних** (використання шифрування для захисту конфіденційної інформації як у зберіганні, так і при передачі)	**Навчання співробітників** (регулярне навчання співробітників щодо розпізнавання фішингових атак та безпечного використання мережі)	**Регулярне оновлення програмного забезпечення** (вчасне оновлення операційних систем та програмного забезпечення для усунення відомих вразливостей)	**Резервне копіювання даних** (регулярне створення резервних копій важливих даних та зберігання їх у захищених місцях)
Економічні загрози						
Інструменти			*Рекомендації*			
Системи моніторингу фінансових транзакцій (впровадження програм для моніторингу та аналізу фінансових операцій з метою виявлення підозрілих транзакцій)	**Контроль доступу до фінансової інформації** (використання систем контролю доступу для обмеження доступу до конфіденційної фінансової інформації)		**Аудити та перевірки** (регулярне проведення внутрішніх та зовнішніх аудитів для виявлення можливих фінансових махінацій)	**Встановлення чітких фінансових процедур** (розробка та впровадження стандартних процедур для управління фінансами та перевірки транзакцій)	**Прозорість та звітність** (забезпечення прозорості фінансових операцій та регулярне звітування перед зацікавленими сторонами)	
Інформаційні загрози						
Інструменти			*Рекомендації*			
Системи управління інформаційною безпекою (впровадження ISMS для систематичного управління інформаційною безпекою на підприємстві)	**Програмне забезпечення для захисту даних** (використання програм для захисту конфіденційної інформації та управління правами доступу)		**Розробка політики інформаційної безпеки** (створення та впровадження політики інформаційної безпеки, що регулює обробку та зберігання даних)	**Оцінка ризиків та вразливостей** (регулярна оцінка ризиків та вразливостей для визначення найбільш критичних точок та вжиття заходів щодо їх усунення)	**Регулярне тестування безпеки** (проведення регулярних тестів на проникнення та аудитів інформаційної безпеки для виявлення та усунення вразливостей)	
Соціально-політичні загрози						
Інструменти			*Рекомендації*			
Системи раннього попередження (впровадження систем для моніторингу соціально-політичних змін та раннього попередження про можливі загрози)	**Плани безперервності бізнесу** (розробка планів безперервності бізнесу для забезпечення стійкості до соціально-політичних змін)		**Відстеження політичної ситуації** (постійний моніторинг політичної ситуації в країні та регіоні для швидкого реагування на можливі зміни)	**Взаємодія з державними органами** (налагодження співпраці з правоохоронними органами та іншими державними структурами для отримання актуальної інформації та підтримки)	**Підготовка до кризових ситуацій** (проведення тренувань та симуляцій кризових ситуацій для підготовки співробітників та управління до можливих загроз)	

Кожен інструмент та рекомендація спрямовані на підвищення стійкості та захисту бізнесу від можливих негативних впливів.

Висновки. Безпека бізнесу вимагає комплексного підходу, який включає фізичну, інформаційну та фінансову безпеку. Ефективна стратегія повинна враховувати всі можливі загрози і вразливості, що можуть виникнути в бізнес-процесах.

Регулярний аудит систем безпеки дозволяє виявляти та усувати потенційні загрози до їх реалізації. Це включає перевірку інформаційних систем, оцінку фізичних бар'єрів і моніторинг фінансових транзакцій.

Використання сучасних технологій, таких як шифрування даних, системи виявлення вторгнень та біометричні засоби ідентифікації, суттєво підвищує рівень захищеності бізнесу від зовнішніх і внутрішніх загроз.

Освічені працівники, які знають основні принципи безпеки і вміють діяти в надзвичайних ситуаціях, є важливою складовою захисту бізнесу. Постійне навчання та підвищення кваліфікації персоналу з питань безпеки допомагає знизити ризик людських помилок [6].

Наявність детально розробленого плану реагування на інциденти (Incident Response Plan) дозволяє швидко та ефективно реагувати на будь-які загрози, мінімізуючи потенційні збитки та відновлюючи нормальну роботу бізнесу.

Дотримання законодавства та нормативних вимог щодо безпеки бізнесу є обов'язковим. Це включає захист персональних даних, дотримання стандартів кібербезпеки та відповідальність за захист інформації клієнтів і партнерів.

Співпраця з професійними охоронними компаніями та консультантами з безпеки дозволяє отримати експертну допомогу та використовувати найкращі практики у сфері захисту бізнесу.

Формування корпоративної культури, де безпека є однією з основних цінностей, сприяє активному залученню всіх співробітників у процес забезпечення безпеки. Це допомагає створити атмосферу відповідальності та обізнаності щодо потенційних загроз.

Впровадження цих стратегій і тактик сприятиме створенню надійної системи захисту, яка зможе адаптуватися до змінюваних умов та ефективно протидіяти новим загрозам, забезпечуючи стабільність та безперервність бізнес-процесів.

Список використаних джерел:

1. Вдовічен А. А., Вдовічена О. Г., Кримська А. О. Цифрова економіка та кібербезпека: аналіз загроз та стратегій захисту в контексті інституціоналізації. *Економіка. Фінанси. Право.* 2024. № 4. С. 135–140.

2. Новікова О. Ф., Покотиленко Р. В. Економічна безпека: концептуальні визначення та механізми забезпечення : монографія. Донецьк: НАН України, Ін-т економіки промисловості, 2006. 408 с.

3. Актуальні виклики та загрози економічній безпеці України в умовах воєнного стану. *НІСД (Національний інститут стратегічних досліджень) : офіційний сайт.* 2023. 31.05. URL: https://niss.gov.ua/publikatsiyi/analitychni-dopovidi/aktualni-vyklyky-ta-zahrozy-ekonomichniy-bezpetsi-ukrayiny-v

4. Найбільші кібератаки проти України з 2014 року. Інфографіка (б д.). *Новини України та Світу. Головні і останні новини. NV.* URL: https://nv.ua/ukr/ukraine/events/najbilshi-kiberataki-proti-ukrajini-z-2014-roku-infografika-1438924.html

5. Королюк Ю., Вдовічен А.Перспективи блокчейн-трансформації економіки України. *Фінансово-економічні, соціальні та правові аспекти розвитку регіонів: загрози та виклики :* матеріали Міжнар. наук.-практ. конф. (24 трав. 2024 р., м. Чернівці). Чернівці : Технодрук, 2024. С. 304–307.

6. Limba T., Plėta T., Agafonov K.& Damkus M. Cyber security management model forcriticalinfrastructure. *Entrepreneurship and Sustainability Issues.* 2017. 4(4):559–573. DOI: https://doi.org/10.9770/jesi.2017.4.4(12)

References:

1. Vdovichen, A.A., Vdovichena, O.G., Krymska, A.O. (2024). Digital economy and cyber security: analysis of threats and protection strategies in the context of institutionalization. *Ekonomika. Finansy. Pravo [Economy. Finances. Right],* no. 4, pp. 135–140 (in Ukr.).

2. Novikova, O.F., Pokotylenko, R.V. (2006). Economic security: conceptual definitions and mechanisms of provision. NAS of Ukraine, Institute of Industrial Economics, Donetsk, 408 p. (in Ukr.).

3. Actual challenges and threats to the economic security of Ukraine in the conditions of martial law (2023, 31.05). *NISD (National Institute for Strategic Studies).* URL: https://niss.gov.ua/publikatsiyi/analitychni-dopovidi/aktualni-vyklyky-ta-zahrozy-ekonomichniy-bezpetsi-ukrayiny-v (in Ukr.).

4. The largest cyber attacks against Ukraine since 2014. Infographics (b d.). *Novyny Ukrainy ta Svitu. Holovni i ostanni novyny. NV [News of Ukraine and the world. Main and latest news. NV].* URL: https://nv.ua/ukr/ukraine/events/najbilshi-kiberataki-proti-ukrajini-z-2014-roku-infografika-1438924.html (in Ukr.).

5. Koroliuk, Yu., Vdovichen, A. (2024). Prospects of blockchain transformation of the economy of Ukraine. *Finansovo-ekonomichni, sotsialni ta pravovi aspekty rozvytku rehioniv: zahrozy ta vyklyky. Materialy Mizhnar. nauk.-prakt. konf.* [Financial, economic, social and legal aspects of the development of regions: threats and challenges. Mat. of the International. science and practice conf.] (May 24, 2024, Chernivtsi). Technoprint, Chernivtsi, pp. 304–307 (in Ukr.).

6. Limba, T., Plėta, T., Agafonov, K.,& Damkus, M. (2017). Cyber security management model forcriticalinfrastructure. *Entrepreneurship and Sustainability Issues,* 4(4),559–573. DOI: https://doi.org/10.9770/jesi.2017.4.4(12)