КІБЕРЗАГРОЗИ У СФЕРІ ЕЛЕКТРОННОЇ ТОРГІВЛІ: ОЦІНКА ВПЛИВУ НА ЕКОНОМІЧНУ БЕЗПЕКУ ПІДПРИЄМСТВ

CYBER THREATS IN THE FIELD OF E-COMMERCE: ASSESSING THE IMPACT ON THE ECONOMIC SECURITY OF ENTERPRISES

У статті розглянуті сучасні умови цифрової трансформації економіки, де електронна торгівля стала одним із ключових напрямів розвитку підприємництва. Проте паралельно з її стрімким зростанням зростає й рівень кіберзагроз, що ставить під загрозу економічну безпеку суб'єктів господарювання. У статті досліджено основні типи кіберзагроз, що характерні для сфери e-commerce, зокрема фішинг, DDoS-атаки, витоки персональних даних та впровадження шкідливого програмного забезпечення. Проаналізовано прямі та непрямі наслідки впливу кіберінцидентів на підприємства, включаючи фінансові втрати, репутаційні ризики та зниження довіри споживачів. Окрема увага приділена питанням оцінки загроз для малих і середніх підприємств, які найчастіше мають обмежені ресурси для організації якісного захисту. На основі аналізу міжнародного досвіду та вітчизняної практики запропоновано практичні напрями зміцнення кібербезпеки торговельних підприємств, включаючи впровадження технічних рішень, інформаційних політик, навчання персоналу та використання послуг спеціалізованих компаній. Зроблено висновки щодо необхідності формування цілісної системи кіберзахисту як важливої складової забезпечення економічної безпеки підприємств у сфері електронної торгівлі.

Ключові слова: *електронна торгівля, кіберзагрози, економічна безпека, кібербезпека, фішинг, витік даних, інформаційні ризики, цифрова трансформація, захист персональних даних, малий бізнес.*

In the contemporary digital economy, e-commerce has emerged as a pivotal sector, driving innovation and reshaping consumer behavior. However, this rapid digital transformation has concurrently escalated the prevalence and sophistication of cyber threats, posing significant risks to the economic security of enterprises. This study delves into the primary cyber threats afflicting the e-commerce landscape, including phishing attacks, distributed denial-of-service (DDoS) assaults, data breaches, and malware infiltrations. These threats not only disrupt operational continuity but also inflict substantial financial losses, erode consumer trust, and tarnish brand reputation. Particular emphasis is placed on small and medium-sized enterprises (SMEs), which, due to constrained resources and limited cybersecurity infrastructure, are disproportionately vulnerable to cyberattacks. The analysis underscores that SMEs often lack comprehensive cybersecurity strategies, rendering them susceptible to breaches that can have catastrophic financial and operational consequences. Drawing upon international case studies and best practices, the research advocates for a multifaceted approach to bolster cybersecurity resilience. Key recommendations include the adoption of advanced technological safeguards, the formulation of robust information security policies, regular employee training programs, and the engagement of specialized cybersecurity firms for threat monitoring and response. The findings accentuate the imperative for an integrated cybersecurity framework that aligns with the unique operational dynamics of e-commerce enterprises. By implementing proactive and adaptive security measures, businesses can mitigate cyber risks, safeguard sensitive data, and ensure sustained economic viability in an increasingly digital marketplace. This abstract is designed to encapsulate the core themes of your article, emphasizing the critical intersection of e-commerce growth and cybersecurity challenges, particularly for SMEs. It aligns with academic standards and is suitable for submission to journals focusing on digital economy and economic security.

Key words: *e-commerce, cyber threats, economic security, cybersecurity, phishing, data breach, information risks, digital transformation, personal data protection, small business.*

УДК 004.056.5:658.012.32:339.138
DOI: https://doi.org/10.32782/dees.17-23

Пугін О.В.[1]
аспірант,
Університет митної справи та фінансів

Puhin Oleksandr
University of Customs and Finance

Постановка проблеми. Розвиток електронної торгівлі став одним із головних векторів трансформації сучасного підприємництва в умовах цифрової економіки. Завдяки використанню інтернет-технологій підприємства отримують нові можливості для розширення ринків збуту, автоматизації бізнес-процесів та підвищення ефективності взаємодії з клієнтами. Водночас інтенсивне впровадження цифрових рішень супроводжується зростанням ризиків, пов'язаних з кіберзагрозами, які здатні завдати суттєвих економічних збитків, особливо для малого та середнього бізнесу.

Кібератаки на інтернет-магазини, витоки персональних даних, злом платіжних систем, фішингові кампанії – усе це є реальними викликами, які щодня загрожують діяльності підприємств у сфері e-commerce. Недостатня обізнаність власників бізнесу щодо сучасних методів захисту, обмежені ресурси на впровадження систем кібербезпеки, а також відсутність ефективної стратегії управління інформаційними ризиками створюють додаткові загрози для економічної безпеки суб'єктів господарювання.

Актуальність проблеми зумовлює необхідність системного аналізу кіберзагроз у сфері електронної торгівлі, оцінки їх впливу на економічну стійкість підприємств та розроблення практичних підходів до їх запобігання.

Аналіз останніх досліджень та публікацій. Питання кібербезпеки в умовах цифрової

[1] ORCID: https://orcid.org/0009-0004-8780-2985

економіки останнім часом набули значної уваги як серед українських, так і зарубіжних науковців. У працях Кравченко І.І. [1] та Пархоменка С.М. [2] акцентовано увагу на структуризації загроз інформаційній безпеці підприємств та необхідності формування системного підходу до захисту електронних даних. Дослідження Швиданенка О.А. [3] та Микитенко В.В. [4] зосереджені на оцінці економічних наслідків від кібератак для підприємств малого та середнього бізнесу, зокрема в умовах обмежених фінансових ресурсів.

Зарубіжні автори, такі як Гордон Л. і Лоеб М. [8], та Андерсон Р. [9] розглядають проблему з точки зору оцінювання вартості ризику та інвестицій у кіберзахист, пропонуючи моделі управління інформаційними ризиками. У звітах міжнародних організацій, зокрема ENISA, OECD та IBM Security, міститься актуальна статистика щодо типів кіберінцидентів, а також рекомендації з побудови ефективної системи кіберзахисту.

Водночас, незважаючи на велику кількість наукових публікацій, проблема оцінки впливу кіберзагроз саме на економічну безпеку підприємств електронної торгівлі залишається недостатньо дослідженою. Особливо відчутною є потреба у комплексному підході, що поєднує фінансову, інформаційну та репутаційну складові ризиків.

Постановка завдання. Метою дослідження є виявлення та систематизація основних кіберзагроз у сфері електронної торгівлі, а також оцінка їхнього впливу на економічну безпеку підприємств з урахуванням фінансових, інформаційних та організаційних чинників. Особлива увага приділяється формуванню практичних рекомендацій щодо підвищення рівня кіберзахисту суб'єктів господарювання в умовах цифрової трансформації.

Виклад основного матеріалу дослідження. У сучасних умовах цифровізації електронна торгівля стала важливою складовою економіки, суттєво змінюючи традиційні моделі ведення бізнесу. Вона відкриває нові можливості для підприємств різних масштабів - від локальних виробників до транснаціональних корпорацій – частині розширення ринків збуту, зниження транзакційних витрат, підвищення гнучкості взаємодії з клієнтами. E-commerce сприяє розвитку інноваційних форм підприємництва, активізує цифрові сервіси та є потужним каталізатором зростання малого та середнього бізнесу.

Однак разом із цим розвитком суттєво зростають і ризики, пов'язані з кіберзлочинністю. Згідно з міжнародними дослідженнями, кількість кібератак у сфері електронної комерції щорічно збільшується, а їх наслідки можуть бути катастрофічними для підприємств: від втрати конфіденційної інформації до фінансових збитків і повного блокування діяльності. Особливо вразливими є підприємства малого та середнього бізнесу, які часто не мають належного рівня технічного та організаційного захисту.

У зв'язку з цим актуальним є дослідження проблеми кіберзагроз саме в контексті економічної безпеки підприємств, які здійснюють свою діяльність у сфері електронної торгівлі. Пошук ефективних механізмів протидії цим загрозам є важливим як для стабільності окремих бізнес-структур, так і для цифрової економіки загалом.

Поняття кібербезпеки охоплює комплекс заходів, спрямованих на захист інформаційних систем, мереж та цифрових активів підприємства від зовнішніх і внутрішніх загроз. У контексті електронної торгівлі кібербезпека набуває особливої ваги, оскільки підприємства щоденно обробляють великі обсяги чутливої інформації – персональні дані клієнтів, фінансову документацію, бази товарів, дані про транзакції тощо.

Економічна безпека підприємства – це стан захищеності його ресурсів, каналів надходження доходів і конкурентоспроможності від внутрішніх та зовнішніх загроз, у тому числі кібернетичного характеру. У сфері e-commerce кіберзагрози прямо впливають на економічну стабільність, прибутковість і ринкову репутацію бізнесу.

Класифікація основних кіберзагроз у сфері електронної торгівлі включає:

1. Фішинг – поширення фальшивих електронних листів чи сайтів з метою отримання конфіденційної інформації.

2. DDoS-атаки – перевантаження сервера запитами, що призводить до зупинки роботи сайту.

3. Зловмисне ПЗ (malware) – шкідливі програми, що можуть красти або знищувати дані.

4. Витік персональних і фінансових даних – часто спричинений як зовнішніми атаками, так і внутрішніми порушеннями.

5. Атаки на платіжні системи – підміна реквізитів, перехоплення платіжної інформації.

6. Соціальна інженерія – маніпулювання співробітниками підприємства з метою отримання доступу до систем.

У таблиці 1 представлені основні кіберзагрози у сфері електронної торгівлі, їх частоти виникнення, потенційних наслідків та рівня ризику.

У науковій та бізнес-літературі підкреслюється, що ефективна система кіберзахисту має базуватися на поєднанні технічних рішень (фаєрволи, антивіруси, шифрування), процедур управління ризиками, а також організаційних заходів, включаючи навчання персоналу та постійний моніторинг загроз.

Таким чином, формування стратегії кібербезпеки для торговельних підприємств є важливим чинником збереження їх економічної стабільності в умовах цифрової економіки.

Кіберзагрози у сфері електронної торгівлі мають прямий і опосередкований вплив на економічну

Таблиця 1

Порівняльна характеристика основних кіберзагроз у сфері електронної торгівлі

Тип загрози	Частота виникнення	Потенційні наслідки	Рівень ризику
Фішинг	Висока	Витік даних клієнтів, фінансові втрати	Високий
DDoS-атаки	Середня	Простої веб-сайту, втрата продажів	Середній
Зловмисне ПЗ (Malware)	Висока	Пошкодження систем, крадіжка інформації	Високий
Атаки на платіжні системи	Низька	Компрометація фінансових транзакцій	Високий
Витік персональних даних	Середня	Штрафи, втрата довіри клієнтів	Високий

Джерело: систематизовано автором за даними [5; 6]

безпеку підприємств. Збитки від таких інцидентів можуть охоплювати фінансові втрати, зниження довіри споживачів, витрати на відновлення інфраструктури, штрафи за порушення вимог захисту персональних даних тощо.

За даними компанії IBM Security [5], середня вартість одного витоку даних у сфері роздрібної торгівлі становила 3,28 млн доларів США, а в 2022 році ця цифра була меншою – 3,02 млн доларів, що свідчить про загострення проблеми. Основні витрати припадають на втрату прибутку (45%), репутаційні ризики (28%) та юридичні компенсації (18%).

В Україні, згідно зі статистичними даними [7], протягом 2022–2023 років спостерігалося зростання кількості зафіксованих кіберінцидентів на 67%, при цьому близько 22% атак були спрямовані на онлайн-сервіси комерційного призначення – інтернет-магазини, платіжні шлюзи та CRM-системи.

Прикладом може слугувати атака на український маркетплейс Prom.ua, яка відбулася у 2022 році. Внаслідок DDoS-атаки сайт був недоступний понад 8 годин, що призвело до втрати замовлень, зниження позицій у пошукових системах і необхідності компенсації продавцям.

Зарубіжні кейси також є показовими. У 2021 році компанія Shopify повідомила про витік персональних даних понад 100 тис. клієнтів внаслідок зловмисних дій двох співробітників служби підтримки. Після інциденту компанія понесла витрати на аудит безпеки та юридичні витрати на суму понад 2 млн доларів США.

Фінансові наслідки для МСП можуть бути ще серйознішими. За даними Ponemon Institute, понад 60% малих підприємств, які зазнали серйозної кібератаки, припиняють діяльність протягом 6 місяців після інциденту. Причиною цього є не лише прямі збитки, а й втрата довіри споживачів і партнерів.

Графік на рисунку 1 наочно демонструє тенденцію зростання як середньої вартості витоку даних, так і витрат на кібербезпеку, підкреслюючи необхідність стратегічного управління ризиками у сфері електронної торгівлі.

Таким чином, аналіз статистики і практичних прикладів свідчить про високий рівень ризиків для електронної торгівлі. Без відповідного рівня захисту підприємства наражаються на серйозні економічні втрати, які можуть поставити під загрозу їхнє подальше функціонування.

Один із базових, але водночас найефективніших напрямів протидії кіберзагрозам полягає у впровадженні технологічних рішень, здатних забезпечити стабільну та безпечну роботу цифрової інфраструктури підприємства. Саме технічні інструменти є першою лінією оборони в боротьбі з несанкціонованим доступом, шкідливим програмним забезпеченням та витоками конфіденційної інформації. Нижче розглянуто ключові технології, які доцільно застосовувати у сфері електронної торгівлі:

1. SSL-сертифікати: Забезпечення шифрування трафіку між клієнтом і сервером. Сайти без SSL втрачають до 30% довіри користувачів (дані HubSpot).

2. Двофакторна автентифікація (2FA): За даними Google, увімкнення 2FA блокує понад 96% фішингових атак.

3. Антивірусне та антималварне ПЗ: Рішення класу EDR (Endpoint Detection and Response) дають змогу виявляти складні загрози в режимі реального часу.

Окрім технічного захисту, надзвичайно важливим елементом кіберзахищеності є чітко сформована внутрішня політика інформаційної безпеки підприємства. Вона охоплює організаційні правила, регламенти доступу, процедури реагування на інциденти та принципи поводження з даними. Наявність такої політики дозволяє мінімізувати людський фактор, структурувати процеси управління ризиками та забезпечити відповідність законодавчим вимогам у сфері захисту інформації. Основні складові ефективної політики розглянуто нижче:

1. Розробка регламентів доступу до інформації та контроль за правами користувачів.

2. Ведення журналів подій (логування) та регулярне оновлення програмного забезпечення.

3. Встановлення резервного копіювання критичних даних (backups), яке згідно з даними Datto, дозволяє скоротити втрати підприємства на 48% у разі інциденту.

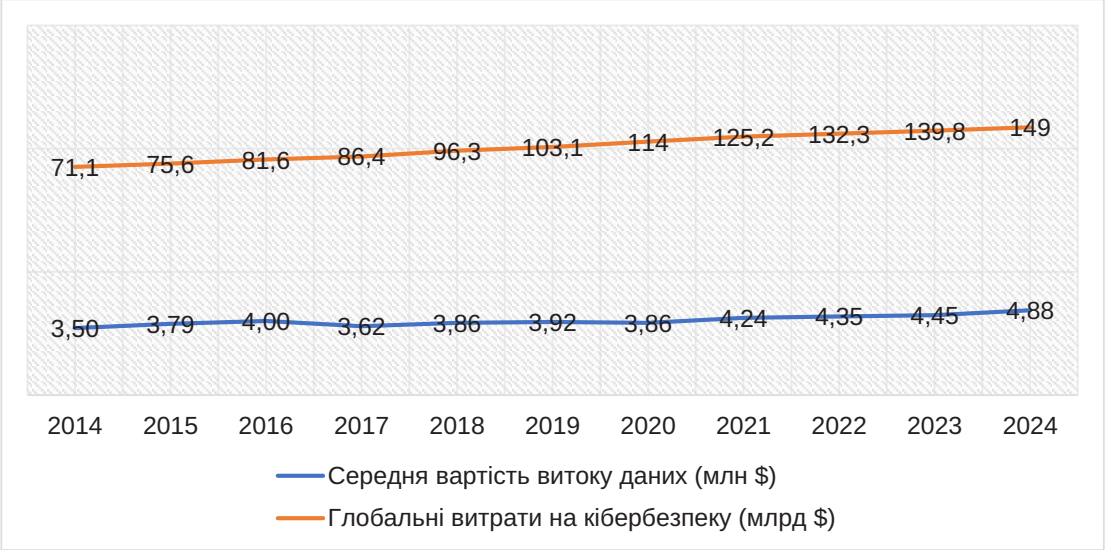

Рис. 1. Динаміка середньої вартості витоку даних та глобальних витрат на кібербезпеку (2014–2024)

Джерело: систематизовано автором за даними [5; 7]

У сфері кібербезпеки людський фактор залишається одним із найвразливіших елементів захисту. Згідно з даними IBM Security [5], понад 90% кіберінцидентів пов'язані з помилками співробітників, такими як відкриття фішингових листів або використання слабких паролів.

Організація тренінгів з цифрової гігієни та моделювання фішингових атак. Наприклад, після впровадження навчальних програм у рамках програми KnowBe4, рівень кліків по фішингових листах знижується з 37% до 4% вже через три місяці.

У сучасному цифровому середовищі підприємства, особливо малі та середні, стикаються з обмеженими ресурсами для забезпечення належного рівня кібербезпеки. Аутсорсинг функцій безпеки та впровадження хмарних технологій стають ефективними рішеннями, що дозволяють отримати доступ до професійних послуг, зменшити витрати та підвищити гнучкість IT-інфраструктури.

Малі та середні підприємства можуть делегувати завдання із захисту даних аутсорсинговим компаніям, які мають відповідну експертизу. Це особливо ефективно для компаній, які не мають власного IT-відділу.

Використання хмарних платформ з вбудованими рішеннями безпеки, таких як Shopify, Wix або Bitrix24, дозволяє зменшити витрати на інфраструктуру на 20–40%, одночасно підвищивши загальний рівень захисту.

У динамічному середовищі електронної торгівлі, де кіберзагрози постійно еволюціонують, регулярна оцінка ризиків є критично важливою для забезпечення економічної безпеки підприємств. Цей процес дозволяє своєчасно виявляти вразливості, адаптувати стратегії захисту та ефективно розподіляти ресурси на найбільш критичні напрями.

Проведення аудиту безпеки та тестування на проникнення (penetration testing). За даними IBM, компанії, які проводять такі перевірки хоча б раз на рік, зменшують втрати від інцидентів на 50%.

Висновки. У сучасному цифровому середовищі кіберзагрози становлять серйозну загрозу для економічної безпеки підприємств, особливо в сфері електронної торгівлі. Згідно з дослідженнями, успішні кібератаки можуть призвести до значних фінансових втрат, включаючи витрати на відновлення даних, юридичні зобов'язання та регуляторні штрафи, а також до операційних збоїв, що мають негайний і довгостроковий вплив на доходи.

Для ефективного протистояння цим загрозам необхідне стратегічне управління ризиками, яке включає постійне виявлення, аналіз, оцінку та реагування на кіберзагрози. Цей підхід допомагає організаціям забезпечити захист даних, відповідність нормативним вимогам та безперервність бізнес-процесів.

Особливої уваги потребують малі та середні підприємства (МСП), які часто мають обмежені ресурси для впровадження комплексних заходів кібербезпеки. Для забезпечення базового рівня цифрового захисту МСП рекомендується:

– Навчати співробітників основам кібербезпеки, включаючи розпізнавання фішингових атак та безпечне поводження з паролями.

– Використовувати сучасне антивірусне програмне забезпечення та регулярно оновлювати всі системи та додатки.

– Забезпечити резервне копіювання даних та використовувати хмарні сервіси з вбудованими механізмами безпеки.

– Розробити політику інформаційної безпеки, що включає контроль доступу та реагування на інциденти.

Застосування стратегічного управління кіберризиками дозволяє малим і середнім підприємствам не лише зменшити ймовірність кібератак, але й забезпечити безперервність бізнес-процесів, зміцнити довіру клієнтів і партнерів, а також відповідати нормативним вимогам у сфері інформаційної безпеки.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Кравченко О.О. Управління фінансовою безпекою економічних суб'єктів: теоретикоприкладні аспекти: колективна монографія. *Видавництво Іванченка І. С.* 2024. С. 336.

2. Пархоменко С.М. Цифрова трансформація будівельної галузі в Україні: публічно-управлінський контекст. *Державне управління: удосконалення та розвиток.* 2024. № 2. URL: https://www.nayka.com.ua/index.php/dy/issue/view/124

3. Швиданенко О.А., Кузьомко В.М., Норіцина Н.І. Економічна безпека бізнесу : навч. посіб. Київ : КНЕУ. 2011. С. 511.

4. Микитенко В.В., Гребенюк О.В. Захист інформаційно-економічної безпеки підприємства в умовах глобалізації. *Вісник НАН України*. 2005. № 3. С. 41–47.

5. IBM Security. *IBM*. URL: https://www.ibm.com

6. Fitzgerald A., Gutierrez R. Cybersecurity Risk Assessment: A Comprehensive Guide to Identifying and Mitigating Cyber Risks. *SECUREFRAME*. URL: https://secureframe.com/blog/cybersecurity-risk-assessment

7. Borgeaud A. Spending on cybersecurity worldwide from 2017 to 2024. *STATISTA.* URL: https://www.statista.com/statistics/991304/worldwide-cybersecurity-spending/

8. Gordon L.A., Loeb M.P. The Economics of Information Security Investment. *ACM Transactions on Information and System Security*. 2022. № 5(4). P. 438-457.

9. Anderson R. Why Information Security is Hard – An Economic Perspective. *Proceedings of the 17th Annual Computer Security Applications Conference.* 2001.

10. 2024 Data Breach Investigations Report. *Verizon*. URL: https://www.verizon.com/business/resources/T242/infographics/2024-dbir-retail-snapshot.pdf

REFERENCES:

1. Kravchenko O.O. (2024) Upravlinnia finansovoiu bezpekoiu ekonomichnykh subiektiv: teoretykoprykladni aspekty: kolektyvna monohrafiia [Managing the financial security of economic entities: theoretical and applied aspects: collective monograph]. Vydavnytstvo Ivanchenka I. S, pp. 336.

2. Parkhomenko S.M. (2024) Tsyfrova transformatsiia budivelnoi haluzi v Ukraini: publichno-upravlinskyi kontekst [Digital transformation of the construction industry in Ukraine: public-management context]. *Derzhavne upravlinnia: udoskonalennia ta rozvytok*, no. 2. Available at: https://www.nayka.com.ua/index.php/dy/issue/view/124

3. Shvydanenko O.A., Kuzomko V.M., Noritsyna N.I. (2011) Ekonomichna bezpeka biznesu : navch. Posib [Economic security of business: a textbook]. Kyiv: KNEU, pp. 511.

4. Mikitenko V.V., Grebenyuk O.V. (2005) Zakhyst informatsiino-ekonomichnoi bezpeky pidpryiemstva v umovakh hlobalizatsii [Protection of information and economic security of the enterprise in conditions of globalization]. *Visnyk NAN Ukrainy,* no. 3, pp. 41-47.

5. IBM Security. *IBM*. Available at: https://www.ibm.com

6. Fitzgerald A., Gutierrez R. Cybersecurity Risk Assessment: A Comprehensive Guide to Identifying and Mitigating Cyber Risks. *SECUREFRAME.* Available at: https://secureframe.com/blog/cybersecurity-risk-assessment

7. Borgeaud A. Spending on cybersecurity worldwide from 2017 to 2024. *STATISTA.* Available at: https://www.statista.com/statistics/991304/worldwide-cybersecurity-spending/.

8. Gordon L.A., Loeb M.P. (2022) The Economics of Information Security Investment. *ACM Transactions on Information and System Security*, no. 5(4), pp. 438-457.

9. Anderson R. Why Information Security is Hard – An Economic Perspective. *Proceedings of the 17th Annual Computer Security Applications Conference.* 2001.

10. 2024 Data Breach Investigations Report. *Verizon*. Available at: https://www.verizon.com/business/resources/T242/infographics/2024-dbir-retail-snapshot.pdf