DOI: https://doi.org/10.32782/2524-0072/2024-60-9

УДК 338.2

ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ ЕЛЕКТРОННОЇ ТОРГІВЛІ В УМОВАХ ВПЛИВУ СУЧАСНИХ ЗАГРОЗ

ENSURING ECONOMIC SECURITY OF E-COMMERCE ENTERPRISES IN THE FACE OF MODERN THREATS

Яремик Мирослав Іванович
кандидат економічних наук, доцент кафедри,
Українська академія друкарства
ORCID: https://orcid.org/0000-0002-5145-4323

Черненко Андрій Володимирович
аспірант,
Українська академія друкарства
ORCID: https://orcid.org/0009-0007-5099-2393

Yaremyk Myroslav
Ukrainian Academy of Printing

Chernenko Andriy
Ukrainian Academy of Printing

Метою дослідження є характеристика особливостей забезпечення економічної безпеки підприємств електронної торгівлі в умовах сучасних загроз. Доведено, що електронна комерція стала невід'ємним компонентом глобальної торгівлі та комерції, представляючи значну частину економічної діяльності у всьому світі. Виокремлено сучасні загрози в системі забезпечення економічної безпеки підприємства електронної торгівлі. Визначено, що система управління економічною безпекою повинна використовувати цілісний підхід, який включає не лише технологічні гарантії, а й організаційну стійкість та співпрацю зацікавлених сторін. Охарактеризовано дії суб'єктів економічної безпеки в контексті протидії основним загрозам. Встановлено, що ігнорування негативного впливу сучасних загроз на економічну безпеку підприємств електронної торгівлі може мати тяжкі наслідки, які загрожують їх діяльності, репутації та довгостроковій життєздатності.

Ключові слова: електронна комерція, електронна торгівля, економічна безпека, управління безпекою.

The purpose of this research is to characterize the peculiarities of ensuring the economic security of e-commerce enterprises in the context of modern threats. It is demonstrated that e-commerce has become an integral component of global trade and commerce, representing a significant portion of economic activity worldwide. Modern threats in the economic security management system of e-commerce enterprises are identified. It is determined that the economic security management system should employ a comprehensive approach, encompassing not only technological safeguards but also organizational resilience and stakeholder collaboration. The actions of economic security subjects in the context of countering major threats are described. It is established that ignoring the negative impact of modern threats on the economic security of e-commerce enterprises can have severe consequences, jeopardizing their operations, reputation, and long-term viability. Thus, ensuring the economic security of e-commerce enterprises is crucial for sustaining stability and resilience in the digital market. Consequently, the very nature of e-commerce inherently involves handling confidential financial information, including payment credentials and customer personal data. Without robust economic security measures, e-commerce enterprises are vulnerable to cyber-attacks, fraud, and data breaches, which can lead to significant financial losses, reputational damage, and loss of customer trust. In today's age of escalating cyber threats and sophisticated hacking methods, prioritizing economic security is imperative to protect both businesses and consumers from potential harm. In today's digital age, consumers are increasingly concerned about the security and privacy of their personal information while conducting online transactions. Need to understand, that if e-commerce businesses do not prioritize economic security measures and adequately protect customer data, it erodes trust and credibility, driving customers away from competitors or traditional institutions.

Keywords: e-commerce, electronic trade, economic security, security management.

Постановка проблеми. Сьогодні, електронна комерція стала невід'ємним компонентом глобальної торгівлі та комерції, представляючи значну частину економічної діяльності у всьому світі. Таким чином, будь-які збої чи загрози операціям електронної комерції можуть мати далекосяжні негативні наслідки не тільки для окремих підприємств, але й для цілої економіки. Таким чином, забезпечення економічної безпеки підприємств електронної торгівлі має вирішальне значення для підтримки стабільності та стійкості цифрового ринку. Відтак, сама природа електронної комерції за своєю суттю передбачає обробку конфіденційної фінансової інформації, включаючи платіжні реквізити та особисті дані клієнтів. Без надійних заходів економічної безпеки підприємства електронної комерції вразливі для кібератак, шахрайства та витоку даних, що може призвести до серйозних фінансових втрат, репутаційної шкоди та втрати довіри клієнтів. У сьогоднішній вік зростаючих кіберзагроз та витончених методів злому пріоритет економічної безпеки є обов'язковим для захисту як бізнесу, так і споживачів від потенційної шкоди.

Слід зазначити, що забезпечення економічної безпеки підприємств електронної торгівлі сприяє створенню сприятливого середовища для інновацій, зростання та інвестицій у цифрову економіку. Коли підприємства відчувають впевненість у безпеці своїх онлайн-транзакцій та операцій, вони з більшою ймовірністю інвестуватимуть у розширення своїх пропозицій електронної комерції, розробку нових технологій та дослідження нових ринків. Це, у свою чергу, стимулює економічне зростання, створює можливості для працевлаштування та підвищує конкурентоспроможність у глобальному масштабі. Крім того, економічна безпека тісно переплетена зі стабільністю системи постачання та логістичних мереж, які є важливими компонентами операцій електронної комерції. Знижуючи ризики, пов'язані з перебоями в ланцюжках поставок, коливаннями валютних курсів та геополітичною напруженістю, підприємства можуть забезпечити безперебійну роботу, своєчасну доставку товарів та послуг та оптимальну задоволеність клієнтів. В умовах все більш взаємопов'язаної та взаємозалежної глобальної економіки підтримка економічної безпеки має життєво важливе значення для забезпечення безперебійного потоку товарів та послуг в екосистемі електронної комерції.

Аналіз останніх досліджень і публікацій. Важливі аспекти підвищення ефективності підприємств електронної торгівлі, розкривалися в працях таких вчених В. Геєць, З. Герасимчук, Л. Гнилицька, М. Єрмошенко, Я. Жаліло, З. Живко, О. Захаров, С. Кавун, М. Копитко, І. Корчинський, О. Ляшенко, І. Мігус, С. Мельник, І. Мойсеєнко, Т. Момот, В. Мунтіян, Є. Олєйніков, І. Оттенко, В. Панченко, В. Пономаренко, В. Прохорова, Я. Пушак, І. Ревак, Є. Рудніченко, С. Урба, М. Флейчук, В. Франчук, М. Швець, Л. Шемаєва, О. Шляйфер, А. Штангрет, та ін. Однак низка теорій і концепцій щодо врахування сучасних загроз, досі залишаються не розкритими повною мірою, що й зумовило вибір даної тематики, її актуальність.

Метою дослідження є характеристика особливостей забезпечення економічної безпеки підприємств електронної торгівлі в умовах сучасних загроз.

Виклад основного матеріалу дослідження. Сьогодні у гіпердинамічному зовнішньому середовищі, для сучасної електронної комерції система управління економічною безпекою є найважливішими інструментами забезпечення життєздатності, стійкості та безпековості підприємства. Відтак, такого роду системи є незамінними механізмами, що захищають економічні інтереси бізнесу, що працює у цифровій сфері [1–3]. Сутність системи управління економічною безпекою полягає в її багатогранному підході до зниження ризиків, захисту активів та створення безпекових умов, що сприяють зростанню та процвітанню відповідно. По суті мета системи управління економічної безпекою на підприємствах електронної торгівлі різноманітна. По-перше, він спрямований на захист фінансових активів та транзакцій, забезпечуючи їхню безпеку від різних форм загроз, таких як витік даних, спроби злому та шахрайські дії. З експоненційним зростанням онлайн-транзакцій необхідність у надійних заходах кібербезпеки стає дедалі гострішою. Ефективна система управління економічною безпекою виступає як захист від цих загроз, зміцнюючи цифрову інфраструктуру платформ електронної комерції та вселяючи довіру серед споживачів [4–5].

Слід зазначити, що система управління економічною безпекою відіграє ключову роль у підтримці цілісності ланцюжків постачання в операціях електронної комерції. Впроваджуючи суворі заходи щодо моніторингу та регулювання процесів закупівель, складування

та розподілу, ці системи мінімізують ризики, пов'язані з контрафактною продукцією, невідповідністю запасів та збоями у логістиці [6-8]. При цьому вони підвищують надійність та надійність підприємств електронної комерції, тим самим підвищуючи їхню конкурентоспроможність на ринку. Важливо відзначити, що найважливішим завданням системи управління економічною безпекою є протидія сучасним загрозам, які постійно розвиваються у відповідь на технологічні досягнення та зміну динаміки ринку [9–10]. Гіпердинамічне середовище, в якому функціонують підприємства електронної торгівлі, створює безліч проблем, починаючи від витончених кібератак і до проблем дотримання нормативних вимог. Таким чином, дуже важливо, щоб системи управління економічною безпекою залишалися гнучкими, адаптивними та активними у виявленні та пом'якшенні негативного впливу сучасних загроз (табл. 1).

Однією із причин постійно змінного характеру загроз у сфері електронної комерції є швидкі темпи технологічних інновацій. Оскільки нові технології, такі як штучний інтелект, блокчейн та Інтернет речей (IoT), інтегруються до платформ електронної комерції, вони створюють нові вразливості, які можуть бути використані зловмисниками. Більше того, взаємопов'язаний характер цифрових екосистем посилює потенційний вплив порушень безпеки, що робить стратегії запобіжного управління ризиками ще більш важливими. Крім того, глобалізація електронної комерції відкрила нові кордони для використання кіберзлочинцями та незаконними організаціями. Транскордонні транзакції, міжнародні ланцюжки постачання та різноманітні нормативно-правові бази створюють складні проблеми для систем управління економічною безпекою, вимагаючи всебічного розуміння геополітичних ризиків, вимог дотримання законодавства та культурних нюансів. Нездатність усунути ці багатогранні загрози може призвести до фінансових втрат, репутаційної шкоди та юридичної відповідальності для підприємств електронної торгівлі (рис. 1).

Таким чином, система управління економічною безпекою повинна використовувати цілісний підхід, який включає не лише технологічні гарантії, а й організаційну стійкість та співпрацю зацікавлених сторін. Програми навчання

Таблиця 1

Основні сучасні загрози в системі забезпечення економічної безпеки підприємства електронної торгівлі

№	Загрози	Характеристика
1	Постійні кібератаки від країни-агресора	З огляду на значну залежність електронної торгівлі від інформаційних технологій, кібератаки можуть спричинити серйозні шкоди як економічні, так і репутаційні. Агресивні дії країни-агресора можуть бути спрямовані на порушення роботи платформи електронної торгівлі, крадіжку конфіденційної інформації або виток даних про клієнтів
2	Зниження кадрового потенціалу	Брак кваліфікованих кадрів у галузі інформаційної безпеки може призвести до неефективності заходів забезпечення економічної безпеки. Недостатня кількість кваліфікованих спеціалістів може ускладнити виявлення, аналіз та вирішення проблем безпеки
3	Неефективне інформаційно-аналітичне забезпечення	Недостатня якість інформаційного та аналітичного забезпечення може обмежити можливості підприємства в області виявлення та протидії потенційним загрозам. Недостовірна чи застаріла інформація може призвести до неправильних рішень з питань безпеки
4	Воєнний стан	Сьогодні, підприємства електронної торгівлі можуть стати об'єктом нападів, що може призвести до обмежень у веденні бізнесу, перерв у постачанні товарів та послуг, а також фінансових втрат
5	Масова міграція населення	Масова міграція населення (як внутрішня, так й зовнішня) може викликати різні економічні та соціальні виклики, які можуть вплинути на ефективність функціонування електронної торгівлі. Зокрема, зміни в демографічній структурі та розподілі ресурсів можуть викликати нестабільність на ринку праці, збільшення соціальної напруги та зміни в споживчому попиті

Джерело: власні дослідження

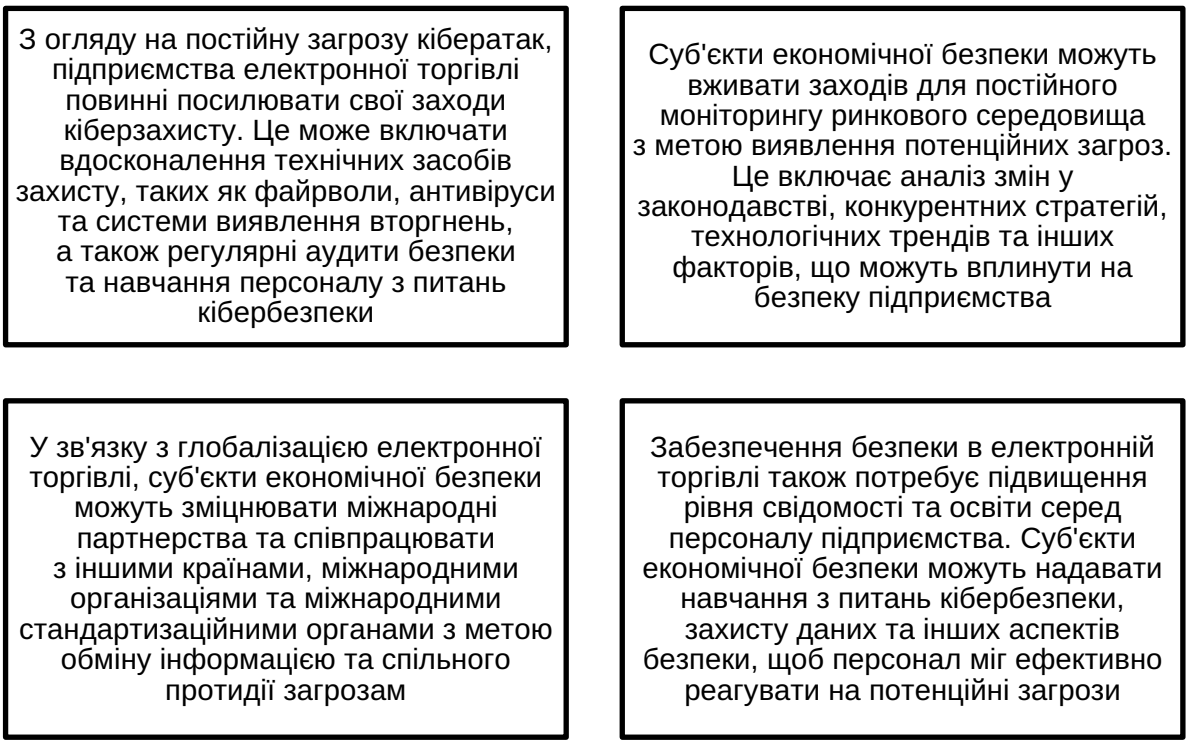

Рис. 1. Основні дії суб’єктів економічної безпеки в контексті протидії сучасним загроз

Джерело: власні дослідження

співробітників, протоколи реагування на інциденти та стратегії управління кризами є невід'ємними компонентами надійної системи економічної безпеки, що надає персоналу на всіх рівнях можливість діяти рішуче перед негативним впливом сучасних загроз.

Висновки. Підсумовуючи, слід зазначити, що ігнорування негативного впливу сучасних загроз на економічну безпеку підприємств електронної торгівлі може мати тяжкі наслідки, які загрожують їх діяльності, репутації та довгостроковій життєздатності. Відтак, ігнорування сучасних загроз робить підприємства електронної торгівлі вразливими для різних кібератак, таких як витік даних, атаки з використанням програм-вимагачів та фішингові атаки. Слід зазначити, що ігнорування впливу сучасних загроз на економічну безпеку може підірвати довіру споживачів до платформ електронної комерції. У сьогоднішню цифрову епоху споживачі все більше переймаються безпекою та конфіденційністю своєї особистої інформації під час проведення онлайн-транзакцій. Якщо підприємства електронної торгівлі не приділяють пріоритетної уваги заходам економічної безпеки та адекватно захищають дані клієнтів, це підриває довіру та авторитет, відштовхуючи клієнтів до конкурентів чи традиційних закладів. В результаті підприємства електронної торгівлі можуть зіткнутися зі зниженням продажів, лояльності клієнтів та частки ринку, що зрештою погіршує їх перспективи зростання та конкурентні переваги на ринку.

REFERENCES:

1. Toska, A., Fetai, B. (2023). The impact of e-commerce on the economic growth of the Western Balkan countries: A panel data analysis. *International Journal of Sustainable Development and Planning,* vol. 18, no. 3, pp. 935–941. [in English]

2. Bondarenko, A. F., Zakharkina, L. S., Syhyda, L. O., Saher, L. Y. (2020). The economic and marketing attractiveness of countries: Measurement and positioning in terms of economic security. *International Journal of Sustainable Development and Planning*, vol. 15, no. 4, pp. 439–449. [in English]

3. Marmullaku, B., Fetai, B., Arifi, A. (2020). Education and its impact in economic growth in lower middle income countries. *Journal Global Policy and Governance*, vol. 9(1), pp.79–91. [in English]

4. Bilan, Y., Lyeonov, S., Lyulyov, O., Pimonenko, T. (2019). Brand management and macroeconomic stability of the country. *Polish Journal of Management Studies*, vol. 19(2), pp. 61–74. [in English]

5. Aldaas, A. (2021). A study on electronic payments and economic growth. Global evidences. *Accounting*, vol. 7(2), pp. 409–414. [in English]

6. Kolisnychenko, T., Sefikhanova, K., Kapral, O., Karpenko, V., Sylkin, O. (2023). Development of an algorithm for Internet marketing strategy implementation: A case study in the EU hotel and restaurant sector. *Ingénierie des Systèmes d'Information*, vol. 28, no. 6, pp. 1549–1556. [in English]

7. Fátima, F., Gonçalves, A., Sandrina, T. (2021). Information technology adoption on digital marketing: A literature review. *Informatics*, vol. 8(4), p. 74. [in English]

8. Oyewole, O. S., Gambo, J., Abba, M., Onuh, M. E. (2013). Electronic payment system and economic growth: A review of transition to cashless economy in Nigeria. *International Journal of Scientific Engineering and Technology*, vol. 2(9), pp. 913–918. [in English]

9. Gadde, S., Rao, G. S., Veesam, V. S., Yarlagadda, M., Patibandla, R. S. M. L. (2023). Secure data sharing in cloud computing: A comprehensive survey of two-factor authentication and cryptographic solutions. *Ingénierie des Systèmes d'Information*, vol. 28, no. 6, pp. 1467–1477 [in English]

10. Karine, H. A. J. I. (2021). E-commerce development in rural and remote areas of BRICS countries. *Journal of Integrative Agriculture*, vol. 20(4), pp. 979–997. [in English]