ІНФОРМАЦІЙНО-ЦИФРОВА БЕЗПЕКА ЕЛЕКТРОННОЇ ТОРГІВЛІ
INFORMATION AND DIGITAL SECURITY OF E-COMMERCE

У статті досліджено питання забезпечення інформаційно-цифрової безпеки в сфері електронної торгівлі в умовах зростання кількості кіберзагроз і розширення цифрового середовища. Розглянуто основні вектори атак на електронні торгові платформи, зокрема фішинг, DDoS-атаки, злам облікових записів, витік персональних даних та фінансової інформації. Проаналізовано сучасні технології захисту, зокрема методи шифрування, багаторівневу автентифікацію, брандмауери, антивірусне програмне забезпечення та використання протоколів безпечного з'єднання. Акцент зроблено на важливості розробки комплексної стратегії безпеки, що включає як технічні, так і організаційні заходи. Окреслено перспективи гармонізації українського законодавства із міжнародними стандартами у сфері цифрової безпеки та рекомендації щодо підвищення стійкості систем електронної торгівлі до зовнішніх загроз.

Ключові слова: *інформаційна безпека, цифрова безпека, електронна торгівля, кіберзлочинність, захист даних, шифрування, кіберзагрози.*

УДК 004.056:339.138

DOI: https://doi.org/10.32782/dees.17-36

Шостак Л.В.[1]
к.е.н., доцент, доцент кафедри економіки і торгівлі,
Волинський національний університет імені Лесі Українки
Федонюк А.А.[2]
к.ф.-м.н., доцент, доцент кафедри загальної математики та методики навчання інформатики,
Волинський національний університет імені Лесі Українки
Помазун О.О.[3]
асистент кафедри інформаційних технологій та туризму,
Луцький інститут розвитку людини Університету «Україна»

Shostak Liudmyla
Lesya Ukrainka Volyn National University
Fedoniuk Anatolii
Lesya Ukrainka Volyn National University
Pomazun Olena
Lutsk Institute of Human Development of the University "Ukraine"

In the digital age, e-commerce has become an essential component of the global economy, enabling businesses and consumers to interact and transact across borders in real time. However, with this rapid development comes an increasing number of risks and vulnerabilities that threaten the stability and security of digital trade. This article presents a detailed examination of the key aspects of information and digital security in the context of e-commerce. The research focuses on the most critical cyber threats currently affecting the industry, such as phishing schemes, denial-of-service attacks, ransomware, account takeovers, and unauthorized access to sensitive user data and payment information. These threats can cause significant financial losses, reputational damage, legal consequences, and a general decline in consumer trust. The article outlines the importance of developing and implementing comprehensive cybersecurity strategies that involve not only technical tools but also organizational measures and employee training programs. Technologies such as end-to-end encryption, public key infrastructure (PKI), intrusion detection and prevention systems (IDPS), secure socket layer (SSL)/transport layer security (TLS) protocols, blockchain-based transaction monitoring, and artificial intelligence (AI)-powered anomaly detection systems are discussed as effective methods of safeguarding e-commerce platforms. In addition, the research explores regulatory and legal frameworks, including the General Data Protection Regulation (GDPR), the NIS2 Directive, and emerging Ukrainian cybersecurity standards aimed at harmonization with European Union legislation. The study also considers the role of international cooperation in combating cybercrime and improving global cyber resilience. Special attention is paid to the cybersecurity challenges faced by small and medium-sized enterprises (SMEs) due to limited resources and the lack of specialized IT staff. The authors argue for the adoption of affordable, scalable, and adaptive cybersecurity solutions that allow SMEs to remain competitive and secure in a constantly evolving threat landscape. Furthermore, the article emphasizes the need for consumer education in recognizing online threats, maintaining secure digital behavior, and using secure payment systems. In conclusion, the study provides practical recommendations for building a resilient, secure, and trustworthy digital environment that supports the sustainable development of electronic commerce.

Key words: *information security, digital security, e-commerce, cybercrime, encryption technologies, GDPR, cybersecurity policy, phishing, artificial intelligence, SME cybersecurity, blockchain, risk mitigation.*

Постановка проблеми. Активне впровадження електронної торгівлі супроводжується значним зростанням цифрових ризиків, пов'язаних із обробкою конфіденційної інформації користувачів та проведенням онлайн-транзакцій. Умови стрімкого розвитку цифрових технологій сприяють еволюції кіберзагроз, які стають дедалі складнішими та більш витонченими. Багато сучасних систем захисту виявляються недостатньо ефективними для протидії новим видам атак і забезпечення стабільної роботи онлайн-платформ. Особливо вразливими залишаються малі та середні підприємства, які часто не мають достатніх ресурсів для впровадження повноцінних заходів кібербезпеки. У зв'язку з цим виникає необхідність у глибокому аналізі актуальних проблем цифрової безпеки в електронній торгівлі та розробці адаптивних механізмів її забезпечення.

Аналіз останніх досліджень та публікацій. Проблеми забезпечення інформаційно-цифрової безпеки електронної торгівлі досліджували вітчизняні науковці, серед яких В. Геєць, 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 інші. Однак, незважаючи на великий обсяг

[1] ORCID: https://orcid.org/0000-0001-8786-9582
[2] ORCID: https://orcid.org/0000-0003-0942-227X
[3] ORCID: https://orcid.org/0009-0003-0803-6307

досліджень у цій сфері, питання забезпечення інформаційної безпеки електронної торгівлі потребують подальшого вивчення, особливо в контексті управління ризиками та захисту даних. Зокрема, важливо вивчати різноманітні загрози, такі як комп'ютерне піратство, шахрайство, порушення прав споживачів і спам, що можуть суттєво впливати на стабільність і розвиток електронної комерції. Особливу увагу слід приділити соціально-психологічним, правовим і технічним аспектам, які безпосередньо пов'язані з цифровою безпекою. Проблеми організаційно-економічного забезпечення кібербезпеки в електронній торгівлі досі залишаються недостатньо дослідженими, що свідчить про необхідність подальших наукових досліджень у цій важливій сфері.

Постановка завдання. Завданням даного дослідження є виявлення основних загроз, що впливають на інформаційну та цифрову безпеку електронної торгівлі. Необхідно проаналізувати сучасні методи захисту даних та оцінити їх ефективність в умовах зростання кіберзагроз. Також важливо дослідити нормативно-правове забезпечення цифрової безпеки в Україні та світі. На основі отриманих результатів передбачається сформувати практичні рекомендації щодо підвищення рівня безпеки електронних торговельних платформ.

Виклад основного матеріалу дослідження. Інтенсивний розвиток цифрових технологій істотно трансформував бізнес-середовище, сприявши широкому розповсюдженню електронної торгівлі як провідної форми взаємодії між споживачами та суб'єктами господарювання. Разом із зростанням обсягів онлайн-транзакцій спостерігається й суттєве посилення кіберзагроз, які супроводжують цифрову комерцію. Недостатній рівень захищеності інформаційної інфраструктури створює передумови для витоку конфіденційних даних, здійснення шахрайських дій, погіршення іміджу підприємств і навіть призупинення ключових бізнес-процесів.

В умовах постійно зростаючої кількості кіберзагроз, бізнес змушений швидко адаптувати свої бізнес-моделі для забезпечення ефективного функціонування та захисту своїх цифрових активів [1].

За оцінками аналітиків компанії Cybersecurity Ventures [2], у 2024 році світові втрати від кіберзлочинності сягнули 20 мільярдів доларів США на добу. Особливо гостро ця проблема постала перед електронною комерцією – через її відкриту інфраструктуру та залежність від цифрових технологій вона стала легкою ціллю для хакерських атак різного типу: від фішингових схем до складних зломів IT-систем.

Найбільш поширені загрози, що становлять небезпеку для електронної торгівлі, умовно можна класифікувати наступним чином (табл. 1):

Якщо розглядати вплив загроз на електронну торгівлю за категоріями, то для e-commerce компаній – це усвідомлення загроз дозволяє формувати стратегії кіберзахисту, впроваджувати комплексні системи моніторингу та навчальні програми для

Таблиця 1

Класифікація загроз для електронної торгівлі

Тип загрози	Механізм дії	Практичні наслідки	Приклад	Рекомендації щодо захисту
Фішинг	Надсилання підроблених повідомлень, що імітують надійні джерела для викрадення логінів, паролів, карток	Крадіжка облікових даних, доступ до акаунтів користувачів, витік фінансової інформації	Атака на eBay у 2020 році – скомпрометовано понад 145 млн акаунтів	Навчання персоналу та користувачів, фільтрація пошти, двофакторна автентифікація
DDoS-атаки	Надмірне навантаження на сервер шляхом масових запитів, що паралізує його роботу	Тимчасова недоступність сайту, фінансові втрати через втрату клієнтів, шкода репутації	Атаки на Amazon та Shopify у 2021 р.	Використання CDN, анти-DDoS сервісів, балансувальників навантаження
SQL-ін'єкції	Вставлення зловмисного SQL-коду у поля форм вводу для доступу до баз даних	Викрадення даних користувачів, змінення або знищення записів у БД, порушення конфіденційності	Уразливості у Magento у 2022 році використовувались для зламу магазинів	Використання параметризованих запитів, перевірка введених даних, оновлення CMS
Міжсайтове скриптування (XSS)	Вбудовування шкідливого JavaScript у вебсторінки, які відкривають інші користувачі	Захоплення сеансів, крадіжка cookies, переадресація на фейкові сайти	Атака через рекламні банери на e-commerce сайтах у 2020 році.	Валідація та ескейпінг введених даних, впровадження Content Security Policy
Шкідливе ПЗ (Malware)	Впровадження троянів, кейлогерів, вірусів з метою шпигунства або викрадення даних	Неконтрольований доступ до систем, фінансові втрати, саботаж роботи інфраструктури	Уразливості в POS-системах Target у 2013 р. – викрадено 40 млн к	Захист endpoint-пристроїв, антивіруси, регулярні аудити безпеки

Джерело: сформовано авторами

персоналу. В свою чергу для клієнтів саме інформування користувачів про ризики сприяє безпечній поведінці в мережі Інтернет (перевірка сайтів, унікальність паролів тощо). Щодо розробників, то загрози можна попередити, шляхом створення безпечного коду з врахуванням OWASP-рекомендацій та регулярним оновленням інфраструктури.

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 [3]. Ігнорування або неефективне управління складними і динамічними кіберзагрозами у сфері електронної комерції може мати багатошарові наслідки для суб'єктів господарювання. Зокрема, це включає значні фінансові збитки внаслідок простою систем, витоку конфіденційних даних або втрати клієнтської бази, суттєве погіршення ділової репутації в цифровому середовищі, а також імовірність притягнення до відповідальності згідно з чинним законодавством у межах кібербезпеки, захисту персональних даних і споживчих прав. У сукупності ці фактори можуть не лише ускладнити операційну діяльність компанії, а й поставити під загрозу її довгострокову конкурентоспроможність на ринку.

Одним із основних елементів захисту електронної комерції, на думку авторів, є технологічні рішення з використанням сучасних технічних засобів (табл. 2).

Організаційні заходи становлять фундаментальну складову системи забезпечення цифрової безпеки суб'єктів господарювання, особливо в умовах зростаючої ролі електронної комерції. Ефективне управління інформаційними ризиками потребує цілісного підходу до формування організаційної культури кіберзахисту на всіх рівнях корпоративної структури. Одним із ключових напрямів у цьому контексті виступає підвищення обізнаності працівників щодо принципів кібергігієни, що значною мірою сприяє мінімізації інцидентів, пов'язаних із людським чинником.

Також надзвичайно важливою є реалізація системи контрольованого доступу до цифрових ресурсів підприємства шляхом чіткого розмежування повноважень користувачів відповідно до їхніх функціональних обов'язків. Невід'ємним компонентом ефективної політики безпеки є розробка та впровадження внутрішніх нормативно-регламентуючих документів (Security Policies), які визначають правила експлуатації інформаційної інфраструктури, порядок поводження з даними та процедури реагування на кіберінциденти.

Крім того, важливу роль у забезпеченні стійкості інформаційної системи до збоїв та атак відіграє регулярне резервне копіювання критично важливої інформації (Backups), що дозволяє оперативно відновити дані у випадку їх втрати або пошкодження. Завершальним елементом організаційної складової кіберзахисту виступає проведення періодичного аудиту інформаційної безпеки та тестування на проникнення (Pentesting), які дають змогу своєчасно виявити вразливості та оцінити загальний рівень захищеності системи. У сукупності зазначені заходи формують цілісну організаційну інфраструктуру кібербезпеки, що є необхідною умовою стабільного функціонування підприємств у цифровому середовищі.

Серед актуальних засобів забезпечення безпеки в електронному бізнесі одним із найбільш універсальних та ефективних інструментів, що активно використовується в межах інформаційної безпеки, зокрема в інфраструктурному компоненті телекомунікаційних систем, є електронний цифровий підпис (ЕЦП), або цифровий сертифікат. Його застосування гарантує автентичність, цілісність

Таблиця 2

Характеристика сучасних методів захисту інформаційних систем в електронній торгівлі: переваги та обмеження

Методи захисту	Переваги	Недоліки
SSL/TLS шифрування	Захищена передача даних між клієнтом і сервером	Не гарантує захисту даних після доставки
Двофакторна автентифікація (2FA)	Зниження ризику несанкціонованого доступу	Можлива вразливість до фішингу
Firewall	Базовий захист мережі від зовнішніх вторгнень	Обмежена здатність виявлення складних загроз
IDS/IPS	Виявлення спроб зламу в реальному часі	Висока вартість та складність налаштування
Штучний інтелект та машинне навчання	Автоматичне виявлення аномалій у трафіку та поведінці	Потребує великих обсягів даних для навчання
Хмарні сервіси безпеки	Централізований захист і масштабованість	Залежність від сторонніх постачальників

Джерело: сформовано авторами

і юридичну значимість електронних документів, що є критично важливим у процесах дистанційної взаємодії між суб'єктами бізнесу.

Це стосується більшою мірою електронного документообігу у відкритій (загально доступній) інфраструктурі телекомунікації з, так званими, відкритими ключами (PKI, Public Key Infrastructure). Нині інфраструктура PKI визначається низкою технічних стандартів, що склалися переважно об'єктивно з урахуванням масштабів поширення певної техніки та технологій: глобальних міжнародних (ISO – International Organization for Standardization; RFC – Request for Comments), регіонально-міжнародних, зокрема – європейських (ETSI – European Telecommunications Standards Institute) та ін. [4, с. 74].

Особливо вразливими до загроз у сфері інформаційно-цифрової безпеки є малі т середні підприємства, які часто не мають достатніх ресурсів для створення повноцінної системи кіберзахисту.

Слід зазначити, що малі та середні підприємства з низьким або нестабільним грошовим потоком стають особливо вразливими до криз, оскільки їм важко вийти на беззбитковість [5, с. 34]. Це робить їх потенційно привабливими цілями для хакерів. Рекомендовано використовувати хмарні рішення безпеки з підпискою за моделлю SaaS (Security-as-a-Service), а також автоматизовані сервіси моніторингу, доступні навіть для компаній з обмеженим бюджетом. Наприклад, український інтернет-магазин електроніки «X-Shop» у 2022 році запровадив базовий набір заходів – SSL-сертифікат, 2FA, систему резервного копіювання та щомісячний аудит вразливостей, що дозволило зменшити кількість інцидентів на 70%.

Автор Нікіфорова А. [6, с.69] пропонує використовувати AFS, як інтегроване рішення для захисту веб-застосунків інтернет-банкінгу та їхніх користувачів від кіберзагроз. Воно забезпечує виявлення фінансового шкідливого ПЗ, фішингу, спроб захоплення облікових записів, шахрайських операцій, атак на веб-застосунки та інших підозрілих дій, а також фіксує активність користувачів в онлайн-середовищі.

Зростання віртуальної онлайн-торгівлі невід'ємно пов'язане з загалом реальною офлайн-логістикою. В останні декілька років логістичні провайдери все частіше виділяють Інтернет-магазини в окремий клієнтський сегмент, масово з'являються спеціалізовані компанії, які обслуговують Інтернет-магазини та компанії, що займаються продажами через сайти [7]. У контексті електронної торгівлі логістизація означає не лише оптимізацію фізичних потоків товарів, а й глибоку інтеграцію логістичного підходу до управління цифровими процесами, що охоплюють аналіз, проєктування та синтез логістичних ланцюгів у віртуальному середовищі. Такий підхід дозволяє забезпечити безперервність та ефективність обміну інформацією між усіма учасниками електронної комерції – від постачальника до кінцевого споживача.

Розвиток інформаційно-комунікаційних технологій створило нові особливі умови для інтенсивності торгівлі. Зростання кількості Інтернет-магазинів, поряд із класичними торговими точками, є важливим чинником до змін і логістичної діяльності підприємств, що провадять Інтернет-торгівлю. Саме такий вид комерції прискорює процеси товарно-грошового обігу, що реалізовується з використанням Інтернет-технологій. Логістична діяльність в даному контексті повністю спирається на електронні ресурси, починаючи з пошуку постачальників, закінчуючи формуванням транспортних маршрутів та використання складських операційних систем [8]. Окремі автори [9] ввважають, що в умовах цифровізації логістичних систем особливої актуальності набуває питання інформаційної та кібербезпеки, адже вразливості на будь-якому етапі логістичного ланцюга можуть призвести до несанкціонованого доступу до комерційних даних, порушення конфіденційності замовлень або зловживання транзакційною інформацією.

Саме тому сучасна логістика в e-commerce повинна включати механізми захисту інформаційних потоків, систем контролю доступу, шифрування даних, а також використання сертифікованих платформ для відстеження й обробки замовлень. У результаті логістизація електронного бізнесу трансформується у стратегічний напрям, що поєднує ефективність управління ресурсами з комплексною цифровою безпекою.

Паралельно не варто ігнорувати й безпеку даних, що надходять із зовнішніх джерел, викликає стурбованість щодо їх надійності та достовірності, оскільки традиційно вони вважаються такими, якщо підтверджуються даними з трьох або більше незалежних джерел [10, с. 106]. Проблематика трансформації інформації з об'єкта споживання у повноцінний товар, а також соціально-економічні наслідки цього процесу потребують ґрунтовного наукового аналізу в умовах стрімкого розвитку цифрової економіки.

Сучасні тенденції в електронній торгівлі демонструють, що інформація набуває комерційної цінності, стаючи стратегічним активом, який необхідно захищати від зовнішніх і внутрішніх загроз. У зв'язку з цим зростає роль інформаційно-цифрової безпеки, що повинна забезпечувати цілісність, доступність і конфіденційність цифрових активів на всіх етапах їх обігу. Водночас цифрова трансформація економіки відбувається не ізольовано в межах окремих держав, а є глобальним процесом, що вимагає скоординованих підходів до кібербезпеки на міжнародному рівні. Це зумовлює необхідність формування комплексної політики захисту даних у цифровому торговельному просторі.

Висновки. Забезпечення цифрової безпеки електронної торгівлі потребує комплексного підходу, що включає технічні, організаційні та нормативно-правові механізми. Успішне впровадження таких рішень дозволяє мінімізувати ризики, зберігати конфіденційність користувачів і підвищувати рівень довіри до цифрового середовища. Особливу увагу слід приділити адаптації новітніх технологій та законодавчих вимог, зокрема для МСП, які є найбільш вразливою категорією суб'єктів цифрової економіки.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Шостак Л., Федонюк А., Помазун О. Кібербезпека в системі формування бізнес-моделі підприємства в умовах цифрової економіки. *Економіка та суспільство*. 2024. Вип. 64. DOI: https://doi.org/10.32782/2524-0072/2024-64-37
2. Кіберзагрози для бізнесу: основні ризики та поради для захисту. URL : https://speka.media/kiberzagrozi-dlya-biznesu-osnovni-riziki-ta-poradi-dlya-zaxistu-vrxz52
3. Яремик М., Черненко А. Забезпечення економічної безпеки підприємств електронної торгівлі в умовах впливу сучасних загроз. *Економіка та суспільство*. 2024. Вип. 60. DOI: https://doi.org/10.32782/2524-0072/2024-60-9
4. Цимбалюк І.В. Безпека електронної торгівлі (організаційно-правовий аспект). *Правова інформатика.* 2012. Вип. 3(35). С. 70–77. URL: https://ippi.org.ua/sites/default/files/12tivopa.pdf
5. Романюк П. Основні проблеми електронної комерції в умовах цифрової трансформації бізнесу. *Цифрова економіка та економічна безпека*. 2023. Вип. 4 (04). С. 32–37. https://doi.org/10.32782/dees.4-6
6. Нікіфорова Л. Використання інноваційних інформаційних технологій в електронній комерції та цифровій економіці. *Innovation and Sustainability*, 2022. Вип. 1. С. 65–71. DOI: https://doi.org/10.31649/ins.2022.1.65.71
7. Ilchenko N., Freiuk O. Logistic activity e-commerce B2C. Innovative Scientific Researches: European Development Trends and Regional Aspect. 2020. P. 86–107. DOI: https://doi.org/10.30525/978-9934-588-38-9-28
8. Шостак Л., Милько І., Павлова С. Електронна торгівля та Інтернет-технології в логістиці. *Економіка та суспільство*. 2023. Вип. 55. DOI: https://doi.org/10.32782/2524-0072/2023-55-97
9. Шостак Л.В., Мохнюк А.М. Розвиток Інтернет-бізнесу як важливого елементу комунікацій в логістиці. *Інфраструктура ринку*. 2021. Вип. 60. С. 123–128. DOI: https://doi.org/10.32843/infrastruct60-23
10. Ткаченко С. Перспективи розвитку цифрової економіки у глобальному просторі. *Економічні горизонти*. 2023. Вип. 2(24). С. 101–109. DOI: https://doi.org/10.31499/2616-5236.2(24).2023.281234

REFERENCES:

1. TShostak L., Fedoniuk A., Pomazun O. (2024). Kiberbezpeka v systemi formuvannia biznes-modeli pidpryiemstva v umovakh tsyfrovoi ekonomiky [Cybersecurity in the system of forming an enterprise business model in the digital economy]. *Ekonomika ta suspilstvo,* vol. 64. DOI: https://doi.org/10.32782/2524-0072/2024-64-37
2. Kiberzahrozy dlia biznesu: osnovni ryzyky ta porady dlia zakhystu [Cyber threats to business: key risks and protection tips]. Available at: https://speka.media/kiberzagrozi-dlya-biznesu-osnovni-riziki-ta-poradi-dlya-zaxistu-vrxz52
3. Yaremyk M., Chernenko A. (2024). Zabezpechennia ekonomichnoi bezpeky pidpryiemstv elektronnoi torhivli v umovakh vplyvu suchasnykh zahroz [Ensuring the economic security of e-commerce enterprises under the influence of modern threats]. *Ekonomika ta suspilstvo*, vol. 60. DOI: https://doi.org/10.32782/2524-0072/2024-60-9
4. Tsymbaliuk I.V. (2012). Bezpeka elektronnoi torhivli (orhanizatsiino-pravovyi aspekt) [E-commerce security (organizational and legal aspect)]. P*ravova informatyka*, vol. 3(35), pp. 70–77. Available at: https://ippi.org.ua/sites/default/files/12tivopa.pdf
5. Romaniuk P. (2023). Osnovni problemy elektronnoi komertsii v umovakh tsyfrovoi transformatsii biznesu [Main problems of e-commerce in the context of digital business transformation]. *Tsyfrova ekonomika ta ekonomichna bezpeka*, vol. 4 (04), pp. 32–37. DOI: https://doi.org/10.32782/dees.4-6
6. Nikiforova L. (2022). Vykorystannia innovatsiinykh informatsiinykh tekhnolohii v elektronnii komertsii ta tsyfrovii ekonomitsi [Use of innovative information technologies in e-commerce and digital economy]. *Innovation and Sustainability*, vol. (1), pp. 65–71. DOI: https://doi.org/10.31649/ins.2022.1.65.71
7. Ilchenko N., Freiuk O. (2020) Logistic activity e-commerce B2C. Innovative Scientific Researches: European Development Trends and Regional Aspect, pp. 86–107. DOI: https://doi.org/10.30525/978-9934-588-38-9-28
8. Shostak L., Mylko I., Pavlova S. (2023). Elektronna torhivlia ta Internet-tekhnolohii v lohistytsi [E-commerce and Internet technologies in logistics]. *Ekonomika ta suspilstvo*. vol. 55. DOI: https://doi.org/10.32782/2524-0072/2023-55-97
9. Shostak L.V., Mokhniuk A.M. (2021). Rozvytok Internet-biznesu yak vazhlyvoho elementu komunikatsii v lohistytsi [Development of Internet business as an important element of communications in logistics]. *Infrastruktura rynku*, vol. 60, pp. 123–128. DOI: https://doi.org/10.32843/infrastruct60-23
10. Tkachenko S. (2023). Perspektyvy rozvytku tsyfrovoi ekonomiky u hlobalnomu prostori [Prospects for the development of the digital economy in the global space]. *Ekonomichni horyzonty*, vol. (2(24), pp. 101–109. DOI: https://doi.org/10.31499/2616-5236.2(24).2023.281234