ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БІЗНЕСУ УКРАЇНИ В УМОВАХ СУЧАСНИХ ЗАГРОЗ

ENSURING INFORMATION SECURITY OF UKRAINIAN BUSINESS IN THE CONDITIONS OF MODERN THREATS

У статті розглядаються сучасні виклики в забезпеченні інформаційної безпеки бізнесу України, які зумовлені зростанням кіберзагроз, економічною нестабільністю та геополітичними ризиками. Проведено аналіз інформаційної безпеки бізнесу України в умовах сучасних загроз, зокрема проаналізовано динаміку кількості кіберзлочинів в Україні. Системтизовано потенційні загрози, які постають перед інформаційною безпекою бізнесу України. Обґрунтовано необхідність інтеграції інноваційних технологій та стратегічних рішень для підвищення рівня захисту. Визначено основні вектори розвитку систем інформаційної безпеки, які враховують специфіку сучасного бізнес-середовища в Україні. Практичне значення результатів дослідження полягає у розробці рекомендацій щодо мінімізації ризиків та покращення інформаційної стійкості підприємств.
Ключові слова: *інформаційна безпека, економічні витрати, кіберзагрози, небезпека, інноваційні технології, стійкість бізнесу.*

The article examines contemporary challenges in ensuring information security for Ukrainian businesses, driven by the escalation of cyber threats, economic instability, and geopolitical risks. The necessity of integrating innovative technologies and strategic solutions to enhance protection levels is substantiated. The primary vectors for developing information security systems tailored to the specificities of Ukraine's modern business environment are identified. The practical significance of the research findings lies in the development of recommendations for minimizing risks and improving the information resilience of enterprises. Ensuring information security for businesses in Ukraine is a critical issue in the face of escalating cyber threats, economic instability, and geopolitical challenges. This research addresses the pressing need for effective strategies and technological integration to safeguard sensitive data and maintain operational stability. The objective of the study is to develop comprehensive approaches to information security, taking into account the peculiarities of Ukraine's business environment. The methodology employed in the study involves a systematic analysis of current threats, including cybercrime, infrastructural vulnerabilities, and human factors. Emphasis is placed on the application of advanced technologies such as multi-layered protection systems and artificial intelligence for anomaly detection. Additionally, the study underscores the importance of workforce education and strategic planning to mitigate risks and enhance resilience. Key findings highlight the necessity of adopting state-of-the-art cybersecurity measures, including the integration of blockchain technologies and robust response protocols. Practical recommendations are provided for businesses to improve their information security posture through targeted investments in technology and personnel training. The study also advocates for enhanced public-private partnerships and legislative advancements to create a more secure digital environment. This article contributes to the discourse on business information security by presenting actionable insights and strategies tailored to the unique challenges faced by Ukrainian enterprises. The findings are of practical value to policymakers, business leaders, and cybersecurity professionals seeking to bolster the resilience of their operations against modern threats.
Keywords: *information security, economic costs, cyber threats, danger, innovative technologies, business sustainability.*

УДК 65.012

DOI: https://doi.org/10.32782/dees.15-24

Топалов В.М.[1]
аспірант,
Луцький національний технічний університет

Topalov Volodymyr
Lutsk National Technical University

Постановка проблеми. У сучасних умовах глобалізації та цифровізації, кіберзагрози стають одним з важливих факторів ризику для бізнесу регіонів країни. Український бізнес постійно стикається з викликами в захисті конфіденційної інформації, що призводить до фінансових втрат та репутаційних збитків. Питання забезпечення інформаційної безпеки бізнесу є важливим для стабільності та конкурентоспроможності як економіки регіонів, так і національної економіки, особливо з огляду на військову агресію росії проти України [2; 3; 4]. Так, проблема забезпечення інформаційної безпеки бізнесу є пріоритетною в сучасних умовах, оскільки зростання цифровізації, широке використання хмарних технологій та інтернет-рішень значно підвищили ризики кіберзагроз. Підприємства стикаються з викликами захисту конфіденційних даних, фінансової інформації, комерційної таємниці, а також захисту репутації від можливих кібератак. Вразливість до атак хакерів, фішингових схем та витоку даних може призводити до значних фінансових втрат і підриву довіри споживачів пропонованих продуктів та послуг. У зв'язку з цим, впровадження сучасних систем кібербезпеки, розробка політик інформаційного захисту та підвищення цифрової грамотності працівників стають обов'язковими елементами сталого функціонування бізнесу.

Аналіз останніх досліджень і публікацій свідчить, що цифрова трансформація бізнесу в епоху інновацій і технологічних змін створює як виклики, так і можливості. Праці Білько С. [1] присвячені дослідженню комплексного оцінювання рівня інформаційної безпеки як основи для своєчасного та обґрунтованого визначення заходів із запобігання та подолання негативних наслідків у випадку реалізації потенційних ризиків та загроз. Регіональні аспекти забезпечення інформаційної безпеки розглянуто у працях Дубницького В. та Науменка Н. [2] де відображено методологічне

[1] ORCID: https://orcid.org/0009-0006-1745-3171

забезпечення процесів формування інформаційної безпеки в сфері забезпечення економічної безпеки регіональної соціально-економічної системи, а також Ковальської Л. [4] яка провела огляд літератури поняття «інформаційна безпека», згрупувала підходи до економічної сутності інформаційної безпеки за трьома ознаками: за ознакою «захист інформації від небезпек та загроз», за ознакою «стабільний та стійкий стан системи державного управління в інформаційному просторі», за ознакою «безпечні умови існування інформаційних технологій». Забезпечення інформаційної безпеки на рівні підприємств розглянули у своїх працях Краус К., Краус Н., Штепа О. [3], які дослідили цифрову трансформацію кібербезпеки на мікрорівні в умовах воєнного стану дослідили, Кузьомко В. [5], де проведено аналіз інформаційної безпеки бізнесу в умовах цифрової трансформації економіки, Шостак Л., Помазун О. [9], які дослідили інформаційну безпеку в контексті інноваційного розвитку бізнес-моделі вітчизняних підприємств в умовах цифрової економіки. Національний рівень забезпечення інформаційної безпеки висвітлено у працях Леоненко Н. та Поступної О. [6], які дослідили сучасні виклики та загрози інформаційної безпеки України в умовах інформаційного глобалізму. У досліджені Науменко Н. [7], здійснено аналіз економічних наукових напрямків у сфері інформаційної безпеки. Наукові праці Яковенко Я., Білик М., Олійник Є. [10] демонструють успішні кейси цифрової трансформації в різних секторах економіки та стратегічні напрями та запропонували рекомендації для підприємств щодо адаптації до вимог цифрової епохи та максимізації вигод від інноваційних технологій. Проте залишається недостатньо вивченим питання інтеграції цих методів у стратегії управління інформаційною безпекою малого та середнього бізнесу.

Постановка завдання. Метою статті є розробка ефективних підходів до забезпечення інформаційної безпеки бізнесу України з урахуванням сучасних загроз та ризиків, а також формування рекомендацій для підвищення стійкості підприємств.

Виклад основного матеріалу дослідження. Забезпечення інформаційної безпеки бізнесу України є однією з умов його стабільного функціонування та розвитку. В умовах швидкої цифровізації та глобальної інтеграції бізнесу ефективне управління інформаційною безпекою потребує системного підходу, який включає розробку політик безпеки, впровадження інноваційних технологій захисту даних, постійний моніторинг загроз та навчання персоналу. Особлива увага має бути приділена адаптації національних підприємств до стандартів кіберзахисту, які відповідають міжнародним вимогам, що є запорукою конкурентоспроможності в умовах сучасного світу.

Потенційні загрози, які постають перед інформаційною безпекою бізнесу України, включають як зовнішні, так і внутрішні фактори. Серед зовнішніх загроз важливу роль відіграють кіберзлочинці, які використовують сучасні технології для проведення атак, таких як фішинг, шкідливе програмне забезпечення та цільові атаки на корпоративні системи [6]. Водночас, внутрішні загрози, зокрема несанкціонований доступ до інформації співробітниками, випадкові помилки персоналу та недостатній рівень цифрової грамотності, також мають значний вплив. У контексті геополітичної нестабільності та зростання кількості кібератак на критичну інфраструктуру країни, бізнес стикається з підвищеним ризиком економічних втрат, порушенням конфіденційності даних та репутаційними ризиками, що вимагає від компаній системного підходу до управління інформаційними ризиками, інтеграції сучасних засобів захисту та створення культури кібербезпеки на всіх рівнях організації.

Кількість кіберзлочинів, спрямованих на український бізнес, згідно зі статистичними даними, постійно зростає, що свідчить про посилення активності кіберзловмисників та зростання вразливості корпоративного сектору. Основними цілями атак стають фінансові дані, комерційна таємниця, персональні дані споживачів та співробітників, а також інфраструктура компаній [5]. Особливе занепокоєння викликають цільові атаки, такі як викрадення баз даних, блокування доступу до систем та фішингові кампанії, які спрямовані на отримання доступу до конфіденційної інформації. Зростання кіберзагроз часто обумовлене недостатньо розвиненими системами кіберзахисту, недотриманням правил інформаційної безпеки співробітниками та відсутністю резервних стратегій реагування на інциденти, що створює суттєві економічні втрати для бізнесу, підриває довіру споживачів та ускладнює умови ведення підприємницької діяльності в Україні. Динаміка кількості кібезлочинів в Україні представлено на рис. 1.

Український бізнес стикається із значними загрозами у сфері інформаційної безпеки. Зокрема, у 2023 році кількість кібератак на підприємства зросла на 34% порівняно з 2022 роком. Аналіз показує, що понад 60% підприємств не мають належного плану реагування на такі загрози, що посилює їхню вразливість. Інфраструктурні уразливості також відіграють значну роль. За даними опитувань, 70% українських компаній використовують застаріле програмне забезпечення, яке стає головною мішенню для кіберзлочинців. Лише 15% підприємств регулярно оновлюють свої системи безпеки, що створює серйозні ризики для витоку даних та фінансових втрат.

Сучасна цифрова епоха створює безліч нових можливостей для розвитку бізнесу, державного управління та суспільства, але водночас відкриває

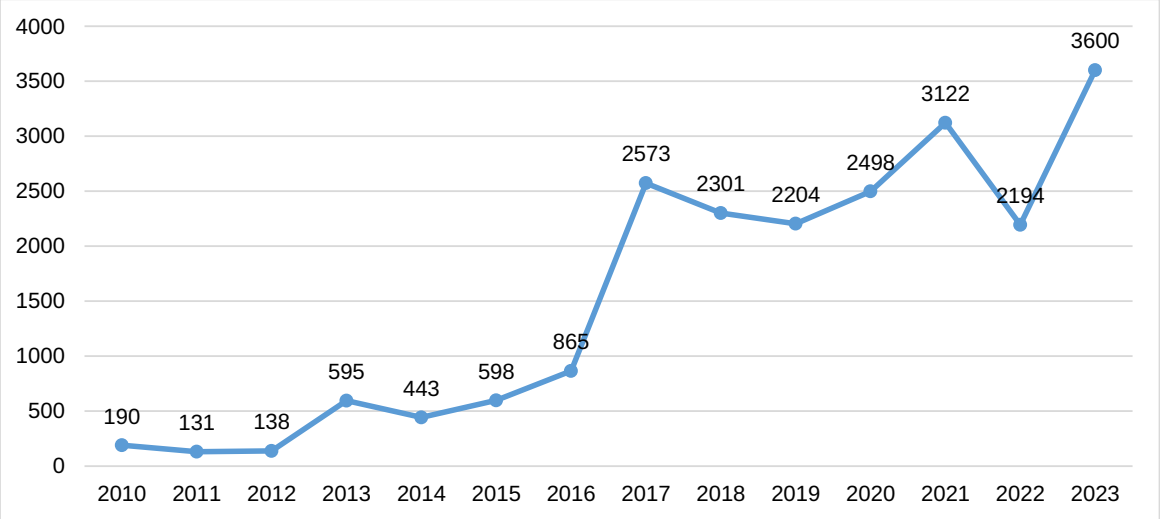

Рис. 1. Кількість кіберзлочинів в Україні у 2010–2023 роках

Джерело: сформовано авторам на основі [8]

й нові виклики у сфері безпеки [1]. Одним із найактуальніших питань залишається проблема кіберзлочинності, яка набуває все більшого масштабу. Аналіз кількості кіберзлочинів в Україні у 2010–2023 роках дозволяє простежити тенденції зростання загроз у цифровому середовищі, визначити основні фактори, що сприяють їх поширенню, та оцінити ефективність заходів кіберзахисту. У 2010–2013 рр., спостерігалася відносно низька кількість таких злочинів, що свідчить про тодішню недостатню увагу до цієї проблеми або про менш активне використання цифрових технологій. Однак починаючи з 2014 року, видно різке зростання кількості кіберзлочинів, яке досягає піку у 2021 році, що, ймовірно, пов'язано зі збільшенням рівня цифровізації, впровадженням нових технологій, а також зі зміною геополітичної ситуації.

У 2022–2023 рр. спостерігається незначне зниження кількості зареєстрованих злочинів, що може свідчити про посилення заходів кібербезпеки або про зміну фокусів кіберзловмисників. Максимальні показники зафіксовані у 2021 році, що свідчить про необхідність моніторингу та адаптації до нових викликів у сфері інформаційної безпеки. Згідно з даними, загальна тенденція демонструє потребу у вдосконаленні технологічних та організаційних механізмів боротьби з кіберзлочинністю в Україні.

Аналіз динаміки кількості кіберзлочинів в Україні у 2010–2023 роках свідчить про значний ріст цифрових загроз, особливо в періоди активної цифровізації та загострення геополітичної ситуації. Найвищі показники кіберзлочинності, зафіксовані у 2021 році, підтверджують необхідність посилення комплексних заходів кібербезпеки, включаючи технологічні інновації, підвищення обізнаності населення та міжнародну співпрацю [9]. Зниження показників у 2022–2023 роках може бути позитивним сигналом про ефективність прийнятих заходів, але потребує подальшого моніторингу та вдосконалення, що підкреслює важливість системного підходу до забезпечення безпеки у цифровому середовищі.

Державна підтримка також відіграє важливу роль. Національний координаційний центр з кібербезпеки України надає рекомендації щодо захисту критичної інфраструктури. Участь у державних ініціативах, таких як навчальні семінари та обмін інформацією про загрози, сприяє підвищенню стійкості бізнесу. Ефективне управління ризиками передбачає наявність чітких планів дій у разі інцидентів. Понад 80% успішних компаній мають розроблені протоколи реагування, які включають залучення спеціалізованих команд, резервування даних та співпрацю з правоохоронними органами. Наприклад, компанії, що впровадили такі протоколи, скоротили час відновлення після атак з 72 до 24 годин.

Сучасні технології стають важливим інструментом у боротьбі з кіберзагрозами. Використання багаторівневих систем захисту, зокрема SIEM (Security Information and Event Management), дозволяє підприємствам оперативно виявляти та реагувати на інциденти. Понад 40% компаній, які впровадили SIEM-системи, відзначили зниження кількості успішних атак на 30% протягом першого року використання. Штучний інтелект також активно застосовується для аналізу аномалій у мережевій активності. Наприклад, алгоритми машинного навчання дозволяють скоротити час виявлення загроз з декількох годин до кількох хвилин, що особливо важливо для великих підприємств, де щодня генерується значний обсяг даних.

Людський фактор залишається однією з головних причин успішних кібератак. Опитування

показали, що 65% інцидентів були пов'язані з помилками працівників, зокрема переходом за шкідливими посиланнями або відкриттям заражених файлів. Регулярні тренінги та навчальні програми для персоналу дозволяють знизити ризики. Компанії, які впровадили систематичне навчання, відзначили зниження кількості інцидентів на 45% протягом двох років.

Висновки. Забезпечення інформаційної безпеки вимагає комплексного підходу, що поєднує використання сучасних технологій, навчання персоналу, впровадження чітких протоколів реагування та співпрацю з державними структурами. Інструменти, такі як SIEM-системи та штучний інтелект, демонструють високу ефективність у виявленні та нейтралізації загроз, значно скорочуючи кількість успішних атак. Водночас, людський фактор залишається критичним аспектом, що потребує постійної уваги через регулярні тренінги. Державна підтримка та координація з бізнесом підвищують загальну кіберстійкість країни. Таким чином, інтеграція технологій, навчання та ефективне управління ризиками є ключовими елементами забезпечення інформаційної безпеки та стійкості бізнесу.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Білько С. Інформаційна та економічна безпека: оцінювання рівня та взаємозв'язку. *Науковий вісник Полісся*. 2022. Вип. 1 (24). С. 58–77. DOI: https://doi.org/10.25140/2410-9576-2022-1(24)-58-77 (дата звернення: 10.10.2024).
2. Дубницький В.І., Науменко Н.Ю. Методологічне забезпечення формування інформаційної безпеки в сфері економічної безпеки регіону. *Вісник економічної науки України*. 2019. № 1. URL: http://dspace.nbuv.gov.ua/handle/123456789/151638 (дата звернення: 15.11.2024).
3. 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.
4. Ковальська Л., Топалов В., Топалов Р. Інформаційна безпека регіону: підходи до розгляду та економічна сутність. *Економічний форум*. 2023. Вип. 13 (2). С. 18–24.
5. Кузьомко В. Інформаційна безпека бізнесу в умовах цифрової трансформації економіки. *Інноваційне підприємництво: стан та перспективи розвитку*: збірник матеріалів VI Всеукраїнська науково-практична конференція (м. Київ, 29–30 березня 2021 р.). Київ : КНЕУ. 2021. С. 26–28.
6. Леоненко Н.А., Поступна О.В. Інформаційна безпека України: механізми, сучасні виклики та загрози в умовах інформаційного глобалізму. *Вісник Національного університету цивільного захисту України. Серія: Державне управління*. 2022. № 2 (17). URL: http://repositsc.nuczu.edu.ua/handle/123456789/16883 (дата звернення: 10.10.2024).
7. Науменко Н.Ю. Аналіз економічних наукових напрямків у сфері інформаційної безпеки. *Електронне наукове фахове видання з економічних наук «Modern Economics»*. 2019. № 16. С. 115–120. URL: http://dspace.mnau.edu.ua/jspui/bitstream/123456789/6290/1/naumenko.pdf (дата звернення: 10.11.2024).
8. Офіційний сайт Департаменту кіберполіції Національної поліції України. URL: https://cyberpolice.gov.ua/news/policziya-rozpochala-kryminalne-provadzhennya-za-faktom-kiberatak-na-sajty-derzhavnyx-organiv-1549/ (дата звернення: 25.11.2024).
9. Шостак Л., Помазун О. Інформаційна безпека в контексті інноваційного розвитку бізнес-моделі вітчизняних підприємств в умовах цифрової економіки. *Цифрова економіка та економічна безпека*. 2024. Вип. 5 (14). С. 160–165. DOI: https://doi.org/10.32782/dees.14-25 (дата звернення: 15.10.2024).
10. Яковенко Я.Ю., Білик М.Ю., Олійник Є.В. Цифрова трансформація бізнес-структур: стратегічні орієнтири в епоху інновацій та технологічних змін. *Економічний простір*. 2024. № 190. С. 355–360. DOI: https://doi.org/10.32782/2224-6282/190-63 (дата звернення: 10.11.2024).

REFERENCES:

1. Bilko S. (2022) Informatsiina ta ekonomichna bezpeka: otsiniuvannia rivnia ta vzaiemozviazku. [Information and economic security: assessing the level and relationship]. *Naukovyi visnyk Polissia,* vol. 1 (24), pp. 58–77. DOI: https://doi.org/10.25140/2410-9576-2022-1(24)-58-77 (accessed October 10, 2024).
2. Dubnytskyi V., Naumenko N. (2019) Metodolohichne zabezpechennia formuvannia informatsiinoi bezpeky v sferi ekonomichnoi bezpeky rehionu. [Methodological support for the formation of information security in the field of economic security of the region]. *Visnyk ekonomichnoi nauky Ukrainy*, vol. 1. Available at: http://dspace.nbuv.gov.ua/handle/123456789/151638 (accessed November 15, 2024).
3. Kraus K., Kraus N., Shtepa O. (2022) Tsyfrova transformatsiia kiberbezpeky na mikrorivni v umovakh voiennoho stanu. [Methodological support for the formation of information security in the field of economic security of the region]. *Innovation and Sustainability*, vol. 3, pp. 26–37.
4. Kovalska L., Topalov V., Topalov R. (2023) Informatsiina bezpeka rehionu: pidkhody do rozghliadu ta ekonomichna sutnist. [Information security of the region: approaches to consideration and economic essence]. *Ekonomichnyi forum*, vol. 13(2), pp. 18–24.
5. Kuzomko V. (2021) Informatsiina bezpeka biznesu v umovakh tsyfrovoi transformatsii ekonomiky. [Business information security in the context of digital transformation of the economy]. *Innovatsiine pidpryiemnytstvo: stan ta perspektyvy rozvytku*: zbirnyk materialiv VI Vseukrainska naukovo-praktychna konferentsiia, (m. Kyiv, 29–30 bereznia 2021). Kyiv: KNEU, pp. 26–28. (in Ukrainian).

6. Leonenko N., Postupna O. (2022) Informatsiina bezpeka Ukrainy: mekhanizmy, suchasni vyklyky ta zahrozy v umovakh informatsiinoho hlobalizmu. [Information security of Ukraine: mechanisms, modern challenges and threats in the conditions of information globalism]. *Visnyk Natsionalnoho universytetu tsyvilnoho zakhystu Ukrainy. Seria: Derzhavne upravlinnia*, vol. 2 (17). Available at: http://repositsc.nuczu.edu.ua/handle/123456789/16883 (accessed October 10, 2024).

7. Naumenko N. (2019) Analiz ekonomichnykh naukovykh napriamkiv u sferi informatsiinoi bezpeky. [Analysis of economic scientific directions in the field of information security]. *Elektronne naukove fakhove vydannia z ekonomichnykh nauk «Modern Economics»*, vol. 16, pp. 115–120. Available at: http://dspace.mnau.edu.ua/jspui/bitstream/123456789/6290/1/naumenko.pdf (accessed November 10, 2024).

8. Ofitsiinyi sait Departamentu kiberpolitsii Natsionalnoi politsii Ukrainy. [Official website of the Cyber Police Department of the National Police of Ukraine]. Available at: https://cyberpolice.gov.ua/news/policziya-rozpochala-kryminalne-provadzhennya-za-faktom-kiberatak-na-sajty-derzhavnyx-organiv-1549/ (accessed November 25, 2024).

9. Shostak L., Pomazun O. (2024) Informatsiina bezpeka v konteksti innovatsiinoho rozvytku biznes-modeli vitchyznianykh pidpryiemstv v umovakh tsyfrovoi ekonomiky. [Information security in the context of innovative development of the business model of domestic enterprises in the digital economy]. *Tsyfrova ekonomika ta ekonomichna bezpeka*, vol. 5 (14), pp. 160–165. DOI: https://doi.org/10.32782/dees.14-25 (accessed October 15, 2024).

10. Yakovenko Y., Bilyk M., Oliinyk Y. (2024) Tsyfrova transformatsiia biznes-struktur: stratehichni oriientyry v epokhu innovatsii ta tekhnolohichnykh zmin. [Digital transformation of business structures: strategic guidelines in the era of innovation and technological change]. *Ekonomichnyi prostir*, vol. 190, pp. 355–360. DOI: https://doi.org/10.32782/2224-6282/190-63 (accessed November 10, 2024).