

Електронний журнал «Ефективна економіка» включено до переліку наукових фахових видань України з питань економіки (Категорія «Б», Наказ Міністерства освіти і науки України № 975 від 11.07.2019). Спеціальності – 051, 071, 072, 073, 075, 076, 292. Ефективна економіка. 2025. № 7.

DOI: <http://doi.org/10.32702/2307-2105.2025.7.5>

УДК 330.131.7

О. М. Столяренко,

д. е. н., доцент, професор кафедри фінансово-економічної безпеки

Національної академії Служби безпеки України

ORCID ID: <https://orcid.org/0000-0003-3134-3201>

С. М. Тютченко,

к. е. н., доцент, НТУ «Дніпровська політехніка»

ORCID ID: <https://orcid.org/0000-0001-8480-6519>

НАПРЯМИ ПІДВИЩЕННЯ ЦИФРОВОЇ БЕЗПЕКИ ЯК КРИТИЧНОЇ СКЛАДОВОЇ ЕКОНОМІЧНОЇ БЕЗПЕКИ

O. Stoliarenko,

*Doctor of Economic Sciences, Associate Professor, National Academy of the
Security Service of Ukraine*

S. Tiutchenko,

PhD in Economics, Associate Professor, Dnipro University of Technology

DIRECTIONS FOR IMPROVING DIGITAL SECURITY AS A CRITICAL COMPONENT OF ECONOMIC SECURITY

У статті розглянуто сутність категорії цифрової безпеки та її вплив на рівень економічної безпеки. Обґрунтовано значення та місце цифрової безпеки в системі економічної безпеки держави та суб'єктів

господарювання. Проаналізовано основні загрози у цифровому середовищі, що мають негативні економічні наслідки. Визначено ключові напрями забезпечення цифрової безпеки, включаючи нормативно-правове регулювання, технічну інфраструктуру та інформаційно-аналітичну підтримку. Обґрунтовано, що цифрова безпека виступає стратегічним чинником сталого розвитку економіки.

Цифрова безпека в сучасних умовах є однією з ключових умов належного функціонування галузей економіки. Часто це поняття розглядають в найзагальнішому сенсі – «як комплекс заходів, покликаний зменшити число ймовірних шкідливих сценаріїв чи розмір збитків, яких може зазнати підприємство у разі розголошення конфіденційної інформації. З цієї точки зору цифрова безпека — це економічний параметр, який повинен враховуватися у діяльності підприємства, а інформацію можна розглядати як певний товар або цінність, що підлягає захисту» [1] .

Цифровізація в будь-якій сфері діяльності відкриває широкі можливості для економічного зростання та фінансової стабільності, підвищення ефективності управління, зменшення операційних витрат, створення нових продуктів та ринків. Але, разом з цим, масштабне перенесення критично важливих процесів у цифрове середовище призводить до зростання локальних та глобальних кіберзагроз.

Тож, в статті досліджено сучасні актуальні думки науковців щодо визначення поняття «економічна безпека», проаналізовано наукові доробки, присвячені вивченню цифрової безпеки, як однієї з критичних складових економічної безпеки.

The article explores the essence of the category of digital security and its impact on economic security levels. It substantiates the importance and place of digital security in the national economic security system and business entities. The main threats in the digital environment that have negative economic consequences are analyzed. Key directions for ensuring digital security are

identified, including regulatory framework, technical infrastructure, and information-analytical support. It argues that digital security is a strategic factor for sustainable economic development.

In contemporary conditions, digital security is one of the key requirements for the proper functioning of economic sectors. Often viewed in the broadest sense, this concept refers to a set of measures aimed at reducing the likelihood of harmful scenarios or the magnitude of losses that enterprises may incur in case of confidential information disclosure. From this perspective, digital security is an economic parameter that should be considered in enterprise activities, with information seen as a commodity or value requiring protection.

Digitization of the economy is the process of modern economic development through the implementation of digital technologies, automation, the use of big data, artificial intelligence, cloud services, and IT technologies. This process takes place across all sectors of the economy and society. The digital transformation of the economy creates new opportunities for growth, but at the same time, it also gives rise to new threats, which can have both local and global consequences.

Digitization in any sphere of activity opens up broad opportunities for economic growth and financial stability, enhances management efficiency, reduces operational costs, and creates new products and markets. However, the extensive migration of critical processes to the digital environment leads to an increase in local and global cyber threats.

Therefore, the article examines the most relevant scholarly perspectives on defining the concept of "economic security" and analyzes the works of scholars who have studied the components of economic security and digital security as a critical component thereof.

Ключові слова: цифрова безпека, економічна безпека, кіберзагрози, інформаційна безпека, цифрова трансформація.

Keywords: *digital security, economic security, cyber threats, information security, digital transformation.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Цифровізація економіки— це процес сучасного розвитку господарської діяльності шляхом впровадження цифрових технологій, автоматизації, використання великих даних, штучного інтелекту, хмарних сервісів ІТ-технологій. Цей процес відбувається в усіх сферах економічного та суспільного секторів. Цифрова трансформація економіки створює нові можливості для зростання, однак водночас породжує нові загрози, які можуть мати як локальні, так і глобальні наслідки. У цьому контексті цифрова безпека набуває особливого значення та виступає як ключовий елемент системи економічної безпеки, забезпечуючи збереження економічних даних та функціонування цифрової інфраструктури.

Аналіз останніх досліджень та публікацій. Багато років вітчизняні та зарубіжні науковці обґрунтовували сутність та особливості забезпечення інформаційної безпеки. Основними дослідниками були А.Колодюк, В.Копилов, М.Якушев та ін. Значні теоретичні та методологічні розробки з основних понять економічної безпеки належать науковцями О.В. Черевко, Е. Беляєву, М. Бусленко, О. Данильян.

На сучасному етапі питаннями цифрової та кібербезпеки займалися О. Пронкін, О. Глушко, В. Вдовиченко. Особливої уваги заслуговують праці з теоретичних основ цифровізації економіки науковця А. Зеленського. Основні виклики цифровізації економіки України під час війни окреслили А. Лапін, І. Грінчук, Д. Оленюк.

Історично термін «інформаційна безпека» мав вузьке технічне трактування та був пов'язаний передусім із захистом комп'ютерних систем. З розвитком цифрових технологій, глобального Інтернету, мобільних платформ та ІТ-технологій, інформаційна безпека трансформувалась у більш складну

систему цифрової безпеки, що охоплює як технологічні, так і соціальні, правові, економічні та етичні аспекти. Тож, проблема сучасна, актуальна та потребує подальших наукових досліджень.

Формулювання цілей статті (постановка завдання). Мета статті полягає в узагальненні визначення поняття цифрової безпеки як критичної складової економічної безпеки та обґрунтуванні напрямів підвищення її рівня.

Виклад основного матеріалу дослідження. Розширення інформаційного простору в економічній та суспільній сферах вимагає забезпечення високого рівня безпеки на усіх рівнях та сферах господарської діяльності. Однією із найважливіших та найкритичніших складових економічної безпеки є інформаційна безпека.

Існує багато міркувань та підходів до визначення поняття «економічна безпека». Під економічною безпекою підприємства розуміють «стан його захищеності від негативного впливу зовнішніх і внутрішніх загроз, дестабілізаційних факторів, за якого забезпечується стійка реалізація основних господарських інтересів та цілей статутної діяльності». Деякі автори термінологічно визначають економічну безпеку як здатність суб'єктів соціально-економічних відносин до захисту економічного потенціалу від внутрішніх та зовнішніх дестабілізуючих чинників. Інша група авторів розглядають економічну безпеку як стан корпоративних ресурсів, який забезпечує стабільне функціонування та розвиток, а також запобігання внутрішнім та зовнішнім загрозам. Також відсутній єдиний підхід серед науковців щодо складових економічної безпеки. Деякі автори пропонують обмежений перелік складових, деякі – навпаки використовують значно ширший перелік цих складових [2].

Зупинимось на наступному трактуванні: економічна безпека — це здатність держави, галузі чи підприємства функціонувати ефективно в умовах внутрішніх і зовнішніх загроз, зберігаючи стійкість,

конкурентоспроможність та можливість розвитку [3]. Цифрова безпека, як її підсистема, охоплює захист економічних активів, що існують у цифровому форматі: даних, систем електронного документообігу, транзакційних платформ, логістичних ланцюгів, інформаційних систем управління тощо [4].

Цифрова безпека (англ. *digital security*) є багатограним поняттям, що охоплює засоби, методи, стратегії та політики захисту даних, інформаційних систем, технологічної інфраструктури та цифрової ідентичності користувачів від несанкціонованого доступу, порушень, атак або пошкодження. Вона є ключовим елементом як національної, так і корпоративної системи безпеки в умовах цифровізації економіки, державного управління та суспільних процесів [5].

Економічна безпека включає в себе здатність економіки ефективно функціонувати в умовах зовнішніх і внутрішніх викликів. Цифрова безпека, у цьому контексті, є:

- засобом захисту активів: інтелектуальна власність, бази даних, комерційна таємниця;
- інструментом збереження довіри – як з боку споживачів, так і партнерів;
- умовою для інновацій: захист сприяє розвитку цифрових послуг, електронної комерції, фінтеху тощо.

У сучасних умовах цифрової трансформації економіки питання безпеки набуває нових вимірів. Якщо раніше домінували загрози фізичній інфраструктурі та фінансовим ресурсам, то сьогодні на перший план виходить захист інформаційного та цифрового середовища, що стало критично важливим для стабільного функціонування економіки [5].

Цифрова безпека — це комплекс заходів, спрямованих на захист інформаційних ресурсів, цифрових платформ і каналів зв'язку від несанкціонованого доступу, витоку, знищення або модифікації. Тож, цифрову безпеку прийнято розглядати як систему, яка включає такі ключові компоненти:

— кібербезпека — захист мереж, комп'ютерів, програм та даних від атак, пошкоджень або несанкціонованого доступу;

— інформаційна безпека — збереження цілісності, конфіденційності та доступності інформації;

— мережева безпека — забезпечення безпечного функціонування внутрішніх і глобальних мереж;

— захист цифрової ідентичності — контроль за автентифікацією користувачів і захист персональних даних;

— правова безпека — нормативне регулювання цифрової діяльності, включаючи захист авторських прав, дотримання стандартів, персональних даних .

Ці елементи безпосередньо впливають на стабільність економічних процесів, конкурентоспроможність бізнесу та інвестиційну привабливість країни, регіону та суб'єктів господарювання.

Вагомою складовою економічної безпеки при роботі з інформаційними технологіями є дотримання та розвиток кібербезпеки, яку визначають як «...деякий стан системи, за якого нейтралізуються загрози доступності, цілісності або конфіденційності даних, що циркулюють в інформаційних системах, в тому числі кожного суб'єкта господарювання» .

Вона є одночасно і складовою інформаційної безпеки суб'єкта господарювання, бо вимагає використання в інформаційних системах відповідного рівня сучасного захисту, постійного навчання персоналу для формування в них навичок безпечного поводження зі службовою інформацією; і безпосередньо процесом організації попередження та захисту від зовнішніх активних дій сторонніх щодо несанкціонованого отримання інформації від суб'єкта господарювання або задля пошкодження його інформаційних систем. Формування високого рівня кібербезпеки організації в сучасних умовах також потребує комплексного підходу до питання і керівництва, і відповідних фахівців, і кожного з працівників суб'єкта господарювання. Оскільки зміни та розвиток складових інформаційних

систем, інформаційних технологій проходить постійно, відповідно до них постійно змінюється законодавство та, нажаль, і прийоми й методи протиправних дій шахраїв та недоброзичливих осіб і компаній [6].

Тож головним в забезпеченні економічної безпеки суб'єкта господарювання в сучасних умовах цифровізації та глобальної економіки можна вважати забезпечення безпеки інформації, каналів її зв'язку та здатність прогнозувати подальший розвиток науки, техніки, технології та законодавчої бази. Досягти одночасно потрібного рівня цифровізації практичної діяльності та економічної безпеки організації можливо за наступних умов:

- забезпечення постійного розвитку всього персоналу організації з питань інформаційної безпеки, для чого знайомити їх не тільки з правилами загальної безпечної роботи та поведінки, але й з практичними прикладами найновітніших шахрайських дій та схем, з прийомами та методами запобігання та нейтралізації негативних наслідків;

- формування та жорсткий контроль за дотриманням правил безпеки роботи з інформацією та інформаційними носіями;

- навчання відповідних працівників роботі з новаційними пропозиціями ринку інформаційних технологій;

- формування правил найменування документів, їх каталогізації та збереження з жорстким контролем дотримання цих вимог всіма робітниками організації;

- посилення попереднього вивчення осіб, що мають або будуть мати доступ до конфіденційної інформації;

- розвиток кібербезпеки в організації;

- раціональне оновлення інформаційних систем, технологій, обладнання, що буде відповідати прогнозам прибутковості діяльності організації та ін [6].

У національній системі безпеки цифрова компонента поступово займає центральне місце у стратегіях економічної безпеки, що зафіксовано, зокрема, у Національній стратегії кібербезпеки України [7].

Національна стратегія кібербезпеки України на 2021-2025 роки була затверджена Указом Президента від 26 серпня 2021 року. Вона визначає пріоритети, цілі та завдання забезпечення кібербезпеки країни. Згідно з цим документом, забезпечення кібербезпеки є одним з пріоритетів у системі національної безпеки України. Щорічно затверджується комплекс заходів із забезпечення кібербезпеки з індикаторами їх виконання. У березні Кабмін затвердив план заходів на 2025-й рік, який є завершальним у «Стратегії кібербезпеки України», розробленій фахівцями Держспецзв'язку на 2021-2025 роки.

Згідно з документом, протягом року повинна відбутись низка заходів для посилення кібербезпеки України у напрямках:

- нормативно-правового забезпечення діяльності у сфері кібербезпеки;
- розвитку організаційно-технологічної складової національної системи кібербезпеки;
- налагодження більш тісного співробітництва з міжнародними партнерами України;
- впровадження ризикоорієнтованого підходу в частині заходів із забезпечення кібербезпеки об'єктів критичної інфраструктури та державних органів;
- подальшого розвитку системи підготовки кадрів у сфері кібербезпеки.

На реалізацію заходів, передбачених «Стратегією кібербезпеки», у Державному бюджеті на 2025 рік передбачено 468,8 млн грн для різних виконавців. В межах реалізації «Стратегії кібербезпеки України» виконані наступні завдання:

— розроблено Порядок реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі;

— розроблено та затверджено Базові заходи із кіберзахисту, «Методичні рекомендації щодо здійснення базових заходів кіберзахисту» та «Методичні рекомендації щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі»;

— проведено багато навчань із кіберзахисту для держслужбовців та для приватного сектору;

— зроблено значний внесок у розвиток кадрового потенціалу у сфері кіберзахисту [8].

Згідно з дослідженнями компанії McKinsey, лише в 2023 році глобальні економічні збитки від кібератак сягнули понад \$10 трлн. В Україні, згідно з аналітичними матеріалами CERT-UA, щороку фіксується понад 200 інцидентів, що прямо впливають на бізнес-операції компаній .

Типові економічні втрати:

- прямі фінансові збитки від крадіжки коштів;
- витрати на відновлення інфраструктури;
- зниження ринкової капіталізації компаній після інцидентів;
- відтік інвесторів і клієнтів через втрату довіри [9].

До основних загроз цифровій безпеці в економічному контексті належать:

- кібершахрайство та атаки на банківську систему;
- витік конфіденційної інформації компаній;
- атаки на інфраструктуру промислових об'єктів;
- маніпуляції з даними в електронній торгівлі;
- шантаж через криптовіруси (ransomware);
- збої в системах управління ланцюгами постачання.

Ці загрози можуть призвести до фінансових втрат, репутаційного збитку, порушення конкурентних переваг та дестабілізації ринку. За статистичними даними загрози мають наступний розподіл: кіберзлочинність

– 35% ; витік даних – 25%; DDoS-атаки – 15%; інсайдерські загрози – 10%; промислове шпionaж – 10%; інші – 5%.



Рис.1. Загрози цифровій безпеці економіки

Тож сучасне підприємство стикається з наступними труднощами в питаннях інформаційної економічної безпеки: необхідністю здійснювати сучасну диджиталізацію (постійно слідкувати за розвитком інформаційних технологій, відповідно до умов обирати та використовувати оптимальні для організації саме в її умовах способи приведення інформації в цифрову форму), яку визначають більш широко як «... заснований на можливостях сучасної ІТ-індустрії процес застосування підприємствами сучасних інформаційно-комунікаційних технологій для досягнення своєї мети, зорієнтований на трансформацію існуючих бізнес-процесів шляхом їх диджиталізації»; необхідністю здійснювати законодавчо визначений обмін інформацією з державними органами та зовнішнім середовищем на принципово новому інформаційному рівні; забезпечувати збереження та конфіденційність інформації, комерційну таємницю та її прозорість.

Цифровізація має декілька прямих загроз для інформації організації. Частина з них стосується людського чинника, частина – технічної складової процесу. Наступною проблемою є питання збереження або знищення

інформації. Промислове шпигунство призводить до передачі секретної інформації конкурентам.

Другу глобальну групу ризиків для економічної безпеки підприємства в процесі впровадження новітніх інформаційних технологій створює техніко-технологічна складова. В першу чергу необхідним є забезпечення організації відповідною технікою, яка на даний час має суттєву вартість та швидко застаріває. Тому кожен суб'єкт господарювання змушений здійснювати прогностичні розрахунки щодо доцільності впровадження сучасних інформаційних технологій в діяльність, їх окупність. При цьому зрозуміло, що їх відсутність для більшості партнерів є сигналом в недостатній платоспроможності суб'єкта, в консерватизмі або низькому рівні підготовки керівництва та персоналу тощо, що, звісно, негативно впливає на імідж. Так само досить високу ціну має зовнішнє програмне забезпечення, ліцензійні програми тощо. Тож економічна безпека підприємства потребує високого професіоналізму в створенні планів перспективного розвитку, в здійсненні економічного обґрунтування щодо впровадження тих чи інших інформаційних технологій, програм, обладнання [6].

Динаміку витрат на кібербезпеку в бізнесі за 2020-2025 роки представлено на рис.2.

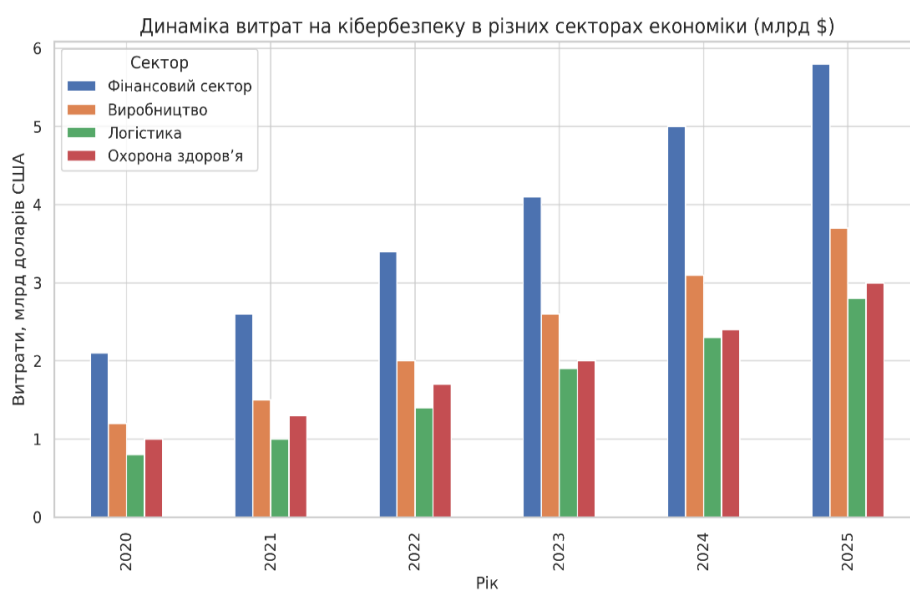


Рис.2. Динаміка витрат на кібербезпеку в бізнесі (2020–2025)

Тож, згідно графіку, прослідковується загальна тенденція до збільшення витрат суб'єктів господарювання на заходи цифрової безпеки, що в кінцевому рахунку позитивно вплине на рівень економічної безпеки в цілому.

У цьому контексті цифрова безпека постає не просто як технічне питання кіберзахисту, а як стратегічна компонента економічної безпеки, що забезпечує:

- Фінансову стабільність — захист банківських систем, біржових платформ і криптовалютних ресурсів від шахрайства й атак;
- Операційну безперервність — запобігання зупинкам підприємств через DDoS-атаки або інфікування програм;
- Збереження комерційної інформації — запобігання витокам критичних даних, що мають стратегічне значення;
- Репутаційну безпеку — підтримку довіри клієнтів, партнерів та інвесторів до цифрових послуг;
- Надійність функціонування цифрової інфраструктури підприємств і держави ;
- Захист критичних економічних даних, без яких неможливе прийняття ефективних управлінських рішень [10].

До шляхів підвищення цифрової безпеки в економічному секторі можна віднести наступні:

- на інституційному рівні: формування державної політики у сфері цифрової безпеки; координація міжвідомчих структур (СБУ, Кіберполіція, НКЦК); впровадження міжнародних стандартів ISO/IEC 27001, NIST, GDPR;
- на корпоративному рівні: проведення аудиту інформаційної безпеки; розробка стратегій кіберзахисту; створення внутрішніх служб кібербезпеки;
- на освітньо-науковому рівні: підготовка фахівців з цифрової безпеки; проведення наукових досліджень з оцінки цифрових ризиків; розвиток цифрової грамотності серед населення.

Таким чином, відсутність належного рівня цифрової безпеки на будь-якому рівні може стати критичною загрозою для успішного економічного розвитку, конкурентоспроможності та національного суверенітету.

Висновки та перспективи подальших досліджень. Цифрова безпека є критично важливою складовою економічної безпеки. В процесі цифровізації всіх сфер економіки потреба в системному підході до забезпечення цифрового захисту тільки зростатиме. Для забезпечення стійкості економічного розвитку необхідне інтегрування цифрової безпеки у стратегії національного, регіонального та корпоративного рівнів. Пріоритетом має стати не лише технологічна модернізація, а й формування культури безпеки у суспільстві.

Цифрова трансформація економіки створює нові можливості для зростання, однак водночас породжує нові загрози, які можуть мати як локальні, так і глобальні наслідки. У цьому контексті цифрова безпека набуває особливого значення як ключовий елемент системи економічної безпеки, забезпечуючи стабільність фінансових потоків, функціонування цифрової інфраструктури та захист критичних економічних даних.

Розвиток цифрових технологій суттєво трансформує підходи до забезпечення безпеки. Незалежно від політичного устрою, одним із ключових завдань сучасної держави залишається гарантування економічної безпеки громадян, підприємств усіх форм власності, регіонів та суверенітету країни. У зв'язку з цим зростає значущість дослідження впливу цифровізації на економічну безпеку різних суб'єктів господарювання та регіонів України, що, своєю чергою, потребує розробки та впровадження новітніх підходів до визначення, оцінки та управління безпекою.

Література

1. Кузєв І. О., Феденко К. П. Основні поняття безпеки інформаційно-комунікаційних технологій. *Матеріали V Міжнародної науково-практичної Інтернет-конференції «ІННОВАЦІЇ: теорія і практика»*. Кропивницький : Академія Прикладних наук. 2024. С. 34-35.

URL:

<https://apn.biz.ua/storage/web/files/222aea5d7034ef6fb798bbc7330fe96d.pdf>

2. Verkhoglyadova N., Kononova I. International Partnership and Cooperation of Ukraine in Wartime . Collective monograph ed. by D. Nascimento, G. Starchenko. University of Coimbra. Portugal – Chernihiv : REICST, 2022. P. 382-396. URL: <https://reicst.com.ua/asp/article/view/monograph-02-2022-05-02>

3. Лук'яненко Д. Г., Панкрухін О. М. Система економічної безпеки держави: структура та управління. Київ : КНЕУ. 2021.

4. Пронкін О. М. Інформаційна безпека в умовах цифрової економіки. *Економіка і держава*. 2022. № 10. С. 42-47.

5. Пронкін О. М. Теоретичні аспекти інформаційної та цифрової безпеки. *Економіка і держава*. 2022. № 8. С. 35-40.

6. Кір'ян О., Кононенко Я., Торяник Д. Інформаційна складова економічної безпеки організації . *Цифрова економіка та економічна безпека*. 2022. № 3(03). С. 79–84. URL: <http://dees.iei.od.ua/index.php/journal/article/view/114>

7. Про затвердження плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України : розпорядження Кабінету Міністрів України від 15.03.2025 р. № 204-р. URL: <https://zakon.rada.gov.ua/laws/show/204-2025-%D1%80#Text>

8. Горбік В. Про «Стратегію кібербезпеки» [Електронний ресурс]. URL: <https://dev.ua/news/strategii-kiberbezpeky-2025>

9. Cybersecurity Ventures. Cybercrime Report 2022 [Електронний ресурс]. URL: <https://cybersecurityventures.com>

10. Вдовиченко В. І. Кіберінфраструктура економіки: загрози та способи захисту. *Науковий вісник НАН України*. 2023. № 2.

References

1. Kuzev, I.O. and Fedenko, K.P. (2024), “Basic concepts of information and communication technology security”, *Materialy V Mizhnarodnoi naukovo-praktychnoi Internet-konferentsii "Innovatsii: teoriia i praktyka"* [Materials of the V International Scientific and Practical Internet Conference "INNOVATIONS:

Theory and Practice"], Akademiia Prykladnykh Nauk, Kropyvnytskyi, Ukraine, pp. 34-35, available at: <https://apn.biz.ua/storage/web/files/222aea5d7034ef6fb798bbc7330fe96d.pdf> (Accessed 25 June 2025).

2. Verkhoglyadova, N. and Kononova, I. (2022), International partnership and cooperation of Ukraine in wartime, University of Coimbra, REICST, Portugal, pp. 382-396, available at: <https://reicst.com.ua/asp/article/view/monograph-02-2022-05-02> (Accessed 25 June 2025).

3. Lukianenko, D.H. and Pankrukhin, O.M. (2021), *Systema ekonomichnoi bezpeky derzhavy: struktura ta upravlinnia* [The system of economic security of the state: structure and management], KNEU, Kyiv, Ukraine.

4. Pronkin, O.M. (2022), "Information security in the digital economy", *Ekonomika i derzhava*, vol. 10, pp. 42-47.

5. Pronkin, O.M. (2022), "Theoretical aspects of information and digital security", *Ekonomika i derzhava*, vol. 8, pp. 35-40.

6. Kirian, O. Kononenko, Ya. and Toryanyk, D. (2022), "Information component of economic security of the organization", *Tsyfrova ekonomika ta ekonomichna bezpeka*, vol. 3(03), pp. 79-84, available at: <http://dees.iei.od.ua/index.php/journal/article/view/114> (Accessed 25 June 2025).

7. Cabinet of Ministers of Ukraine (2025), Resolution "On approval of the action plan for 2025 for the implementation of the Cybersecurity Strategy of Ukraine", available at: <https://zakon.rada.gov.ua/laws/show/204-2025-%D1%80#Text> (Accessed 25 June 2025).

8. Horbik, V. (2025), "On the "Cybersecurity Strategy"", available at: <https://dev.ua/news/strategii-kiberbezpeky-2025> (Accessed 25 June 2025).

9. Cybersecurity Ventures. (2022), "Cybercrime Report 2022", , available at: <https://cybersecurityventures.com> (Accessed 25 June 2025).

10. Vdovychenko, V.I. (2023), "Cyber infrastructure of the economy: threats and methods of protection", *Naukovyi visnyk NAN Ukrainy*, vol. 2.

Стаття надійшла до редакції 01.07.2025 р.