DOI: https://doi.org/10.37634/efp.2024.4.28
УДК 004.056.5:004.056.2:338.24:005.8.001.57

*Анатолій Анатолійович* ***ВДОВІЧЕН***
*д.е.н., професор, Чернівецький торговельно-економічний інститут ДТЕУ*
*ORCID: https://orcid.org/0000-0002-4496-6435*
*e-mail: vdovichen_anatolij@ukr.net*

*Ольга Геннадіївна* ***ВДОВІЧЕНА***
*к.е.н., доцент, Чернівецький торговельно-економічний інститут ДТЕУ*
*ORCID: https://orcid.org/0000-0003-0768-5519*
*e-mail: olgavdovichena77@gmail.com*

*Анна Олександрівна* ***КРИМСЬКА***
*к.т.н., старший викладач, Чернівецький торговельно-економічний інститут ДТЕУ*
*ORCID: https://orcid.org/0000-0001-6410-9476*
*e-mail: ryhz8998@gmail.com*

# ЦИФРОВА ЕКОНОМІКА ТА КІБЕРБЕЗПЕКА: АНАЛІЗ ЗАГРОЗ ТА СТРАТЕГІЙ ЗАХИСТУ В КОНТЕКСТІ ІНСТИТУЦІОНАЛІЗАЦІЇ

*У статті досліджено взаємозв'язок між цифровою економікою та кібербезпекою, розглянуто загрози й стратегії захисту.. Результати дослідження свідчать про різноманітність і складність атак на цифрову інфраструктуру. Доведено, що застосування проактивних заходів безпеки забезпечить зменшення ризиків і допоможе захистити конфіденційність даних.*

***Ключові слова:*** *інформаційна безпека, кібератаки, цифрові інновації, стратегії захисту даних, економічний розвиток*

## ВСТУП

Розвиток цифрової економіки зумовив революційні зміни в нашому повсякденному житті. Водночас цифрова трансформація актуалізувала нові виклики безпеці, які пов'язані з появою дедалі складніших і більш небезпечних кіберзагроз. З огляду на це питання кібербезпеки має ключове значення для державних і приватних установ, які постають перед необхідністю захищати свої конфіденційні дані, інфраструктуру та користувачів від численних кібератак [1, с. 39].

Така взаємодія між цифровою економікою й кібербезпекою порушує фундаментальні питання про те, як організації підходять до ризиків ІТ-безпеки та управляють ними в постійно змінюваних умовах. Як наслідок, актуальним вбачається здійснення глибокого аналізу загроз для ІТ-систем, а також стратегій захисту, що впроваджуються для відповіді на ці виклики, особливо в контексті інституціоналізації, де питання безпеки набувають ще більш важливого виміру [6, с. 43].

Поєднання цифрової економіки й кібербезпеки призвело до збільшення кількості міждисциплінарних досліджень, які вивчають нові загрози та стратегії захисту в контексті інституціоналізації. Така конвергенція зумовлена стрімким розвитком цифрових технологій і посиленням взаємозв'язку комп'ютерних систем у світовому масштабі [8].

Останні наукові дослідження показали різноманітність і дедалі більшу складність загроз для цифрової інфраструктури [4, с. 63]. Такі складні атаки, як сучасне шкідливе програмне забезпечення, фішингові атаки та програми-вимагачі, вказують на необхідність пошуку більш надійних стратегій захисту. Відповідно сучасні дослідження зосереджено здебільшого на виявленні векторів атак, оцінюванні ризиків і розробленні адаптивних механізмів захисту [10, с. 88].

Проте слід зазначити, що розвиток штучного інтелекту (ШІ) й машинного навчання (МН) теж викликає значний інтерес. Такі методи, як поведінковий аналіз і виявлення аномалій, стали важливими інструментами у протидії цифровим загрозам, хоча виклики залишаються, особливо стосовно інтерпретованості моделей і стійкості перед загрозою ворожих атак [15, с. 68].

Водночас еволюція стратегій і нормативно-правових актів у сфері кібербезпеки є однією з актуальних сфер досліджень. У наукових роботах вивчається вплив стандартів і нормативно-правової бази на захист даних та управління інцидентами безпеки. Проте залишаються питання стосовно ефективності та гармонізації політик на міжнародному рівні, особливо в умовах глобалізації цифрового середовища [11, с. 536].

Зростає також інтерес до питань економічного складника кіберзлочинності. Дослідники вивчають мотиви зловмисників, основні бізнес-моделі та стратегії стримування. Проте розуміння цієї незаконної діяльності та протидія їй залишаються складним питанням, що вимагає міждисциплінарного підходу й посилення міжнародної співпраці [9, с. 51].

Зрештою наявність знань і підготовка з питань кібербезпеки є актуальною темою наукових досліджень. Науковці вивчали поведінку користувачів, корпоративні практики безпеки й ініціативи з підвищення обізнаності громадськості. Незважаючи на це, питання розуміння чинників, які впливають на впровадження належних практик безпеки, і оцінювання ефективності інформаційно-просвітницьких програм, вимагають більш грунтовної наукової уваги [2, с. 44].

**МЕТА** дослідження – поглиблений аналіз таких загроз цифровій економіці, як кібератаки, крадіжка даних та онлайн-шахрайство, а також вивчення стратегій захисту, що застосовуються інституційними та приватними особами.

## МЕТОДИ ДОСЛІДЖЕННЯ

У дослідження застосовано метод аналізу для вивчення поширених загроз та слабких місць у цифровій економіці у контексті інституціоналізації, метод син-

тезу – для поєднання різних даних і теоретичних положень з метою формування комплексного розуміння взаємозв'язку між цифровою економікою й кібербезпекою. Метод порівняння надав можливість зіставити різні стратегії захисту, з'ясувати їхні сильні та слабкі сторони стосовно нових загроз. Метод абстрагування сприяв зведенню складних концепцій і закономірностей до загальних принципів, що полегшує формулювання надійних інституціоналізованих підходів до захисту цифрових активів.

## РЕЗУЛЬТАТИ

Цифрова економіка стає невіддільною частиною світового ринку, що ґрунтовно трансформує традиційні моделі виробництва, споживання та обміну. У цифровому просторі потоки інформації та транзакцій поширюються з небувалою швидкістю, змінюючи межі наших економічних взаємодій. В основі цієї революції лежать кілька ключових аспектів, які заслуговують на увагу й аналіз.

По-перше, повсюдне забезпечення доступом до Інтернету відіграє фундаментальну роль у розвитку цифрової економіки. У всьому світі мільярди осіб користуються мережею Інтернет для швидкого поширення ідей, товарів та послуг. Цей глобальний взаємозв'язок створює віртуальний ринок без жодних кордонів, на якому підприємства можуть відносно легко вийти на потенційних клієнтів у віддалених регіонах. Як наслідок, традиційні географічні бар'єри зникають, відкриваючи шлях до глобальної економіки.

По-друге, розвиток ШІ й засобів автоматизації суттєво змінив спосіб ведення бізнесу. Складні алгоритми аналізують величезні обсяги даних для генерування цінних ідей, підвищуючи ефективність процесів та пришвидшуючи прийняття рішень. Роботи й автономні системи трансформують традиційні галузі, автоматизуючи повторювані завдання й уможливлюючи звільнити людські ресурси для діяльності з вищою доданою вартістю.

По-третє, економіка платформ стає панівною моделлю в багатьох секторах. Ці платформи часто постають у ролі посередників, полегшуючи транзакції між користувачами та збираючи важливі дані про їхню поведінку й уподобання [3, с. 108].

З огляду на сучасні тенденції можна виокремити декілька новацій.

По-перше, розвиток електронної комерції продовжує змінювати споживчі звички. Споживачі дедалі більше прагнуть зручності й персоналізації, що стимулює збільшення кількості онлайн-покупок. Компанії повинні адаптуватися до цієї реальності, інвестуючи в зручні платформи електронної комерції й зосереджуючись на клієнтському досвіді.

По-друге, блокчейн стає проривною технологією, яка здатна здійснити цілу революцію в платіжних і транзакційних системах. Забезпечуючи децентралізмваний і безпечний реєстр, блокчейн дає змогу обмінюватися даними й цінностями без посередництва центрального органу влади. Ця технологія застосовується в різних сферах – від фінансових послуг до ланцюжка постачання, відкриваючи можливості для зниження витрат і підвищення прозорості.

По-третє, розвиток економіки спільного користування продовжує мати значний вплив на багато секторів. Ця спільна економіка пропонує переваги з погляду ефективності використання ресурсів і зменшення впливу на навколишнє середовище, водночас порушуючи питання регулювання та захисту працівників.

Зазначимо, що в цифровій економіці, хоча вона й відкриває багато можливостей, водночас виникає низка загроз, які можуть ставити під сумнів безперервне функціонування й безпеку цього середовища. Неможна не погодитися з думкою дослідників, які стверджують, що постійно збільшувана кількість загроз зумовлює появу серйозних викликів для бізнесу, держави й окремих осіб, які працюють у цьому комплексному віртуальному середовищі [5, с. 210].

Для того щоб зрозуміти, яких загроз зазнає цифрова економіка, доречно почати з визначення поняття «загроза». У цьому контексті загрозу пропонуємо розуміти як будь-яку дію або подію, що може спричинити шкоду, збої або втрати в цифровій економіці. Ці загрози можна поділити на кілька категорій, зокрема ІТ-безпека, онлайн-шахрайство, економічне шпигунство й кібертероризм (табл. 1).

Серед головних загроз цифровій економіці атаки шкідливих програм та витоки даних посідають перше місце. Наприклад, програми-вимагачі завдали величезних фінансових збитків багатьом компаніям, блокуючи доступ до їхніх даних і вимагаючи викуп за їх повернення. Аналогічно витоки даних, яких зазнали великі компанії та установи, ставлять під загрозу конфіденційність чутливої інформації та можуть мати руйнівний вплив на репутацію й довіру клієнтів.

Для протидії цим загрозам необхідні інституційні стратегії на кількох рівнях. На національному та міжнародному рівнях посилена співпраця між державою, бізнесом і міжнародними організаціями має важливе значення для розроблення ефективної політики та нормативно-правових актів у сфері кібербезпеки. Це передбачає створення законів і стандартів безпеки, а також обмін інформацією й передовим досвідом між учасниками процесу [14, с. 105].

На організаційному рівні компаніям необхідно інвестувати в передові технології кібербезпеки та впроваджувати заходи із запобігання, виявлення й реагування на кібератаки. До них належать навчання персоналу, моніторинг мереж, резервне копіювання даних і впровадження жорстких політик безпеки.

Зрештою, на індивідуальному рівні користувачі повинні усвідомлювати ризики, пов'язані з цифровою економікою, і дотримуватися безпечної поведінки в Інтернеті, наприклад, застосовувати надійні паролі, перевіряти джерела й регулярно оновлювати програмне забезпечення.

Безперечно, кібербезпека – важлива концепція сучасної цифрової епохи, що визначає заходи, спрямовані на захист ІТ-систем, мереж, даних та інфраструктури від кібератак та онлайн-загроз. Її значення полягає в тому, щоб гарантувати конфіденційність, цілісність і доступність інформації в умовах, коли зв'язок є універсальним, а кіберзагрози – поширеними.

У цифровій економіці кібербезпека відіграє важливу роль у забезпеченні довіри користувачів до онлайн-транзакцій, електронних платіжних систем та обміну конфіденційною інформацією. Без ефективної кібер-

Таблиця 1 – **Види загроз для цифрової економіки [***складено авторами на основі [5]***]**

| Назва загрози | Характеристика |
|---|---|
| ІТ-безпека | Атаки шкідливих програм, віруси, програми-вимагачі, спроби хакерських атак і витоки даних. Ці атаки можуть поставити під загрозу конфіденційність, цілісність і доступність даних, а також безпеку ІТ-систем. |
| Онлайн-шахрайство | Крадіжка персональних даних, фішингові афери, підроблені вебсайти й шахрайські транзакції. Такі дії знижують довіру споживачів до онлайн-транзакцій і можуть призвести до значних фінансових втрат для фізичних та юридичних осіб. |
| Економічне шпигунство | Крадіжка інтелектуальної власності, комерційної таємниці та конфіденційної інформації з метою отримання несправедливої конкурентної переваги. Такі дії можуть мати руйнівний вплив на бізнес, ставлячи під загрозу його здатність до інновацій і збереження конкурентоспроможності на ринку. |
| Кібертероризм | Застосування комп'ютерних технологій для здійснення терористичних атак або просування екстремістських ідеологій. Такі атаки можуть мати руйнівні наслідки для таких критично важливих об'єктів інфраструктури, як електромережі, транспортні системи й системи охорони здоров'я, ставлячи під загрозу громадську безпеку та економічну стабільність. |

безпеки бізнес ризикує зазнати фінансових втрат, витоку даних та репутаційних збитків. До того ж критичні об'єкти інфраструктури, зокрема електромережі, транспортні системи й системи охорони здоров'я, є незахищеними перед кібератаками, що може мати серйозні наслідки для громадської безпеки й економічної стабільності [12, с. 404].

Необхідно зазначити, що виклики кібербезпеці постійно еволюціонують, що відображається у складності кібератак. До основних загроз належать, зокрема, атаки шкідливих програм, витоки даних, цілеспрямовані кібератаки, онлайн-шахрайство й фішингові кампанії. Ці атаки можуть здійснюватися злочинцями, економічними шпигунами, політичними активістами або навіть національними державами, що підкреслює розмаїття суб'єктів та мотивацій у кіберпросторі.

Сучасні тенденції у сфері кібербезпеки створюють нові виклики й можливості для організацій та урядів. Активне впровадження Інтернету речей (IoT) та підключених до нього пристроїв створює нові вектори атак, оскільки ці, часто ненадійно захищені пристрої, може бути застосовано для отримання доступу до конфіденційних мереж і даних. Аналогічно розвиток ШІ та МН відкриває можливості для покращення виявлення загроз і аномалій, але водночас створює нові виклики для захисту від атак на основі ШІ [7, с. 204].

Держави та організації в усьому світі прагнуть посилити свою кібербезпеку, застосовуючи багато вимірні підходи. Це передбачає розроблення надійної політики та нормативно-правових актів у сфері кібербезпеки, інвестування в передові технології, підвищення обізнаності й навчання користувачів, а також міжнародне співробітництво для боротьби з транс кордонними кіберзагрозами.

Бізнес та державні органи все частіше інвестують в такі інноваційні рішення з кібербезпеки, як поведінковий аналіз, виявлення загроз у реальному часі, передова криптографія й захист децентралізованих мереж на основі блокчейну. Ці підходи спрямовано на передбачення загроз, швидке виявлення інцидентів та ефективне реагування для мінімізації потенційної шкоди.

Типові кіберзагрози включають атаки шкідливих програм, зокрема віруси, черв'яки, троянські програми та програми-вимагачі, спрямовані на порушення конфіденційності, цілісності й доступності даних [16, с. 13].

Ці атаки можуть призвести до величезних фінансових втрат для компаній та установ через блокування доступу до їхніх ІТ-систем і вимагання викупу за їх повернення. До того ж витік даних, наприклад крадіжка персональної та/чи фінансової інформації, матиме значний вплив на репутацію й довіру клієнтів, що, безперечно, зумовить довгострокові наслідки для економічної стійкості установи.

Значну загрозу становлять також фішингові атаки, які полягають у шахрайських спробах отримати таку конфіденційну інформацію, як облікові дані для входу в систему, паролі та номери кредитних карток. Ці атаки може бути застосовано для доступу до банківських рахунків, здійснення несанкціонованих транзакцій або крадіжки коштів, що ставить під загрозу фінансову безпеку фізичних та юридичних осіб.

Розподілені атаки на відмову в обслуговуванні (DDoS) є ще однією формою загрози кібербезпеці, яка може мати значний вплив на фінансові установи та їхніх клієнтів. Ці атаки мають на меті перевантажити цільові сервери шкідливим мережевим трафіком, що призводить до перебоїв в обслуговуванні й неможливості обробляти фінансові транзакції. Наслідки таких атак можуть бути руйнівними, зумовлюючи значні фінансові втрати і знижуючи довіру клієнтів до спроможності установи захистити їхні активи.

З погляду потенційного впливу на інституційні інвестиції загрози кібербезпеки викликають значні занепокоєння стосовно безпеки даних та дотримання нормативних вимог. Фінансові установи зобов'язані захищати особисту й фінансову інформацію своїх клієнтів відповідно до таких нормативних актів, як Загальний регламент про захист даних (GDPR) та Закон про захист персональних даних та електронних документів (PIPEDA). Витік даних може призвести до значних штрафів, судових позовів та шкоди репутації, що впливає на оцінку та інституційні інвестиції [13, с. 133].

У контексті інституціоналізації захист від кіберзагроз має вирішальне значення для забезпечення безпеки даних, збереження конфіденційності інформації та операційної стабільності. Будь-які установи: державні, фінансові, освітні чи комерційні відчувають постійне збільшення кількості кіберзагроз і потребують ефективних стратегій захисту для відповіді на ці виклики.

Огляд наявних стратегій кібербезпеки виявляє низку підходів і практик, спрямованих на посилення захищеності установ. До них належать: розроблення політики кібербезпеки; підвищення рівня обізнаності та навчання; упровадження контролю доступу; застосування передових технологій безпеки (табл. 2).

Таблиця 2 – **Характеристика заходів, спрямованих на підвищення захищеності [***складено авторами на основі [4, 13]***]**

| Заходи з кібербезпеки | Характеристика |
|---|---|
| Розроблення політики кібербезпеки | Наявність чіткої й деталізованої політики кібербезпеки, що визначає обов'язки, процедури та стандарти безпеки, яких слід дотримуватися для захисту систем і даних. |
| Підвищення обізнаності та навчання | Усі працівники мають розуміти ризики кібербезпеки й застосовувати безпечні практики у своїй повсякденній діяльності. Йдеться про управління паролями й виявлення фішингових електронних листів. |
| Впровадження контролю доступу | Наявність доступу до конфіденційних систем і даних лише для авторизованих користувачів. Це може включати багатофакторну автентифікацію, управління правами й моніторинг дій користувачів. |
| Використання передових технологій безпеки | Брандмауери, системи виявлення втручань, антивіруси та засоби шифрування |

У розробленні стратегій захисту для узгоджених дій з установами важливо сприяти співпраці й обміну інформацією між державними та приватними суб'єктами. Державні органи, регулятори, бізнес і некомерційні організації повинні працювати разом, щоб обмінюватися інформацією про загрози, розробляти спільні стандарти безпеки й координувати дії для запобігання кібератакам [2, с. 40].

Узгоджений підхід до кібербезпеки може також передбачати створення державно-приватних партнерств для розвитку ініціатив з підвищення обізнаності, навчання та розбудови потенціалу у сфері кібербезпеки. Такі партнерства дозволяють об'єднати ресурси й досвід різних учасників для колективного та ефективного протистояння викликам кібербезпеки.

Для вдосконалення інституційних механізмів забезпечення кібербезпеки важливо застосовувати цілісний підхід, який інтегрує кібербезпеку в усі аспекти діяльності установи. Це може передбачати інтеграцію кібербезпеки у стратегічне планування, закупівлі й розвиток систем, а також упровадження механізмів моніторингу й оцінювання для регулярного визначення ефективності стратегій кібербезпеки та їх коригування в разі потреби.

## ВИСНОВКИ

Отже, цифрова економіка – це сфера, яка швидко розвивається й характеризується постійним впровадженням інновацій. Для підприємств та керівників, які прагнуть ефективно операціонізувати свою діяльність, надзвичайно важливо мати розуміння ключових аспектів цього економічного простору та вміти орієнтуватися в сучасних тенденціях. Використання технологічного потенціалу й адаптація до ринкових змін дають змогу ефективно застосовувати можливості, що надає цифрова економіка.

Загалом загрози цифрової економіки – це складні виклики, які постійно змінюються й вимагають проактивного та скоординованого підходу з боку держав, бізнесу і приватних осіб. Посилення безпеки та стійкості цифрових систем шляхом спільних зусиль сприятиме захисту цифрової економіки та підтримці довіри до онлайн-середовища.

Безумовно, загрози кібербезпеки становлять серйозний виклик для цифрової економіки й інституційного сектору. Впровадження проактивних заходів безпеки, таких як формулювання надійних стратегій, підвищення кВаліфікації персоналу й використання передових технологій, дасть змогу зменшити ризики, пов'язані з кіберзагрозами, та забезпечити безпеку й конфіденційність даних користувачів.

***Список використаних джерел***

1. Білько С.С. Інституційне забезпечення інформаційної безпеки України. *Економіка і регіон.* 2021. № 3 (82). С. 36-41. URL: https://doi.org/10.26906/EiR.2021.3(82).2361

2. Гавриленко Н.Г., Тарасенко І. О. Сучасні тенденції цифровізації економіки: проблеми та перспективи розвитку. *Міжнародний науковий журнал «Інтернаука». Серія: Економічні науки*. 2021. № 3 (47). С. 36-46. URL: http://doi.org/10.25313/2520-2294-2021-3-7046

3. Гуржій С. В. Засади інституціонально-функціонального забезпечення кібербезпеки в сучасних умовах. *Інформація і право*. 2021. № 2 (37). С. 103-114. URL: https://doi.org/10.37750/2616-6798.2021.2(37).238344

4. Диха М.В. Причини інвестиційного шахрайства і пропозиції щодо його унеможливлення. *Економіка України.* 2023. № 7 (740). С. 57–71. URL: http://economyukr.org.ua/?page_id=723&lang=uk&aid=639

5. Кобернюк С., Карпенко В. Напрями цифровізації маркетингу аграрних підприємств. *Innovation and Sustainability*. 2023. № 1. С. 204-212. URL: https://doi.org/10.31649/ins.2023.1.204.212

6. Краус К., Краус Н., Іщенко І. Фокус пріоритетів індустрії Х. 0 та її анатомія в умовах цифровізації економічних відносин. *Innovation and Sustainability*. 2023. № 1. С. 33-50. URL: https://doi.org/10.31649/ins.2023.1.33.50

7. Куницька-Іляш М. В. Проблемно-перспективні сфери зміцнення міжнародної конкурентоспроможності та посилення структурних складових фнансової безпеки ІКТ-сектора України. *Науковий огляд: економіка та управління.* 2023. № 3 (79). С. 200-206. URL: https://doi.org/10.32782/2521-666X/2022-79-27

8. Мельниченко С. Г. Аналіз стратегічного менеджменту та його вплив на успішність організацій. *Здобутки економіки: перспективи та інновації.* 2024. № 3. URL: https://econp.com.ua/index.php/journal/article/view/19/16

9. Мялковський Д. В., Семенченко А. І. Розвиток інституційних спроможностей суб'єктів забезпечення системи безпеки та кіберзахисту України. *Розвиток системи державного управління в Україні.* 2020. № 3 (70). С. 40-54. URL: https://doi.org/10.34213/tp.20.03.05

10. Олешко А. А. Ключові імперативи державного управління цифровим розвитком. *Держава та регіони. Серія: Державне*

*управління*. 2019. № 3 (67). С. 87-91. URL: https://doi.org/10.32840/1813-3401-2019-3-16

11. Панькова О., Касперович О. Залучення ресурсів громадянського суспільства до подолання загроз коронакризи в умовах цифрових трансформацій. *Журнал європейської економіки*. 2021. № 20 (3). С. 514–547.

12. Панькова О., Касперович О., Іщенко О. Соціально відповідальне партнерство як інноваційна платформа забезпечення розвитку сфери зайнятості в умовах глобальних цифрових трансформацій. *Журнал європейської економіки*. 2020. № 19 (2). С. 392-409.

13. Поляков О.М. Активізація міжнародної співпраці у сфері забезпечення кібербезпеки: шляхи удосконалення в реаліях сьогодення. *Інформація і право*. 2021. № 2(37). С. 129-138. URL: https://doi.org/10.37750/2616-6798.2021.2(37).238348

14. Храпкіна В. В. Інституціональні аспекти цифрової трансформації та розвитку цифрової економіки України. *Цифрова економіка та економічна безпека*. 2024. № 1(10). С. 103-107. URL: https://doi.org/10.32782/dees.10-19

15. Чорна О.А. Нормативне забезпечення та інститути трансформації підприємств до цифрової економіки. *Управління економікою: теорія та практика*. 2022. С. 51-82. URL: https://doi.org/10.37405/2221-1187.2022.51-82

16. Bannikov V. Systematization of approaches to the understanding and implementation of lean manufacturing. *Наукові праці Міжрегіональної Академії управління персоналом. Економічні науки.* 2022. Вип.4 (67). С. 9-15. URL: https://doi.org/10.32689/2523-4536/67-2

***References***

1. Bilko S.S. Institutional support of information security in Ukraine. *Economy and Region.* 2021. № 3 (82). pp. 36-41. URL: https://doi.org/10.26906/EiR.2021.3(82).2361 (in Ukrainian).

2. Havrylenko N. H., Tarasenko I. O. Modern trends of digitalization of the economy: problems and development prospects. *International Scientific Journal «Internauka». Series: Economic Sciences.* 2021. № 3 (47). pp. 36-46. URL: http://doi.org/10.25313/2520-2294-2021-3-7046 (in Ukrainian).

3. Gurzhiy S.V. Principles of institutional-functional support for cybersecurity in modern conditions. *Information and Law.* 2021. № 2 (37). pp. 103-114. URL: https://doi.org/10.37750/2616-6798.2021.2(37).238344 (in Ukrainian).

4. Dykha M.V. Causes of investment fraud and proposals for its prevention. *Economy of Ukraine.* 2023. № 7 (740). pp. 57-71. URL: http://economyukr.org.ua/?page_id=723&lang=uk&aid=639 (in Ukrainian).

5. Kobernyuk S., Karpenko V. Directions of digitalization of marketing of agrarian enterprises. *Innovation and Sustainability.* 2023. № 1. pp. 204-212. URL: https://doi.org/10.31649/ins.2023.1.204.212 (in Ukrainian).

6. Kraus K., Kraus N., Ishchenko I. Focus on priorities of X industry and its anatomy in the conditions of digitization of economic relations. *Innovation and Sustainability.* 2023. № 1. pp. 33-50. URL: https://doi.org/10.31649/ins.2023.1.33.50 (in Ukrainian).

7. Kunitska-Ilyash M. V. Problematic and prospective areas of strengthening international competitiveness and enhancing structural components of financial security of the ICT sector of Ukraine. *Scientific Review: Economics and Management.* 2023. № 3 (79). pp. 200-206. URL: https://doi.org/10.32782/2521-666X/2022-79-27 (in Ukrainian).

8. Melnychenko S.H. Analysis of strategic management and its impact on organizational success. *Achievements of Economics: Perspectives and Innovations.* 2024. № 3. URL: https://econp.com.ua/index.php/journal/article/view/19/16 (in Ukrainian).

9. Mialkovskyi D.V., Semenchenko A.I. Development of institutional capacities of entities ensuring security and cyber defense system of Ukraine. *Development of the system of public administration in Ukraine.* 2020. № 3 (70). pp. 40-54. URL: https://doi.org/10.34213/tp.20.03.05 (in Ukrainian).

10. Oleshko A. A. Key imperatives of state management of digital development. *State and Regions. Series: Public Administration*. 2019. № 3 (67). pp. 87-91. URL: https://doi.org/10.32840/1813-3401-2019-3-16 (in Ukrainian).

11. Pankova O., Kasperovich O. Involvement of civil society resources in overcoming the threats of the corona crisis in the conditions of digital transformations. *Journal of European Economy.* 2021. № 20 (3). pp. 514-547 (in Ukrainian).

12. Pankova O., Kasperovich O., Ishchenko O. Socially responsible partnership as an innovative platform for ensuring the development of the employment sphere in the conditions of global digital transformations. *Journal of European Economy.* 2020. № 19 (2). pp. 392-409 (in Ukrainian).

13. Poliakov O.M. Activation of international cooperation in the field of cybersecurity: ways of improvement in today's realities. *Information and Law. 2021*. № 2 (37). pp. 129-138. URL: https://doi.org/10.37750/2616-6798.2021.2(37).238348 (in Ukrainian).

14. Khrapkina V.V. Institutional aspects of digital transformation and development of the digital economy of Ukraine. *Digital Economy and Economic Security.* 2024. № 1 (10). pp. 103-107. URL: https://doi.org/10.32782/dees.10-19\ (in Ukrainian).

15. Chorna O.A. Regulatory support and institutes of enterprise transformation for the digital economy. *Management of Economy: Theory and Practice.* 2022. pp. 51-82. URL: https://doi.org/10.37405/2221-1187.2022.51-82 (in Ukrainian).

16. Bannikov V. Systematization of approaches to the understanding and implementation of lean manufacturing. *Scientific Works of the Interregional Academy of Personnel Management. Economic Sciences.* 2022. Vol. 4(67). pp. 9-15. URL: https://doi.org/10.32689/2523-4536/67-2

***Anatolii VDOVICHEN***
*Doctor of Economics, Professor, Chernivtsi trade and economic institute of State University Of Trade And Economics*
*ORCID: https://orcid.org/0000-0002-4496-6435*
*e-mail: vdovichen_anatolij@ukr.net*

***Olha VDOVICHENA***
*PhD in Economics, Associate Professor, Chernivtsi trade and economic institute of State University Of Trade And Economics*
*ORCID: https://orcid.org/0000-0003-0768-5519*
*e-mail: olgavdovichena77@gmail.com*

***Anna KRYMSKA***
*PhD in Engineering, Senior Lecturer, Chernivtsi trade and economic institute of State University Of Trade And Economics*
*ORCID: https://orcid.org/0000-0001-6410-9476*
*e-mail: ryhz8998@gmail.com*

# DIGITAL ECONOMY AND CYBERSECURITY: ANALYSIS OF THREATS AND DEFENSE STRATEGIES IN THE CONTEXT OF INSTITUTIONALIZATION

***Introduction.*** *This paper explores the relationship between the digital economy and cybersecurity, discussing threats to these domains and necessary defense strategies in the context of increasing institutionalization of activities on the Internet. It also emphasizes the importance of this issue in an interconnected world where transactions and communications predominantly occur on digital platforms, becoming increasingly international.*

***The purpose of the paper is*** *to provide an in-depth analysis of various threats to the digital economy, such as cyberattacks, data theft, and online fraud, as well as to study protection strategies employed by institutional and private entities.*

***Results.*** *The research findings indicate a significant diversity and growing complexity of attacks on digital infrastructure, especially with the emergence of new methods such as phishing, ransomware, and distributed denial-of-service (DDoS) attacks. The study also identifies major gaps in existing defense systems, particularly in user awareness, network security, and vulnerability management. Based on the analysis conducted, several important points have been noted, emphasizing the critical importance of a comprehensive approach to cybersecurity, which entails close cooperation between the government, businesses, international organizations, and civil society. Additionally, there is an emphasis on the need for continuous investment in research and development of innovative security technologies, as well as in training and increasing awareness among end-users.*

***Conclusions.*** *Overall, the threats to the digital economy are complex challenges that are constantly evolving and require a proactive and coordinated approach from governments, businesses, and individuals. By working together to enhance the security and resilience of digital systems, we can better protect the digital economy and preserve trust in the online environment. Ultimately, cybersecurity threats pose a serious challenge to the digital economy and the institutional sector. By taking proactive security measures such as implementing robust security policies, training personnel, and utilizing state-of-the-art technologies, financial institutions can mitigate risks associated with cyber threats and safeguard the security and confidentiality of their clients' data.*

***Keywords:*** *information security, cyberattacks, digital innovations, data protection strategies, economic development*