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. № 10.

DOI: http://doi.org/10.32702/2307-2105.2025.10.127

УДК 658

М. В. Перекицай,

аспірант,

Державний університет економіки і технологій

ORCID ID: https//orcid.org/0009-0008-8830-5381

СУЧАСНІ РИЗИКИ ТА ПОТОЧНІ ВИКЛИКИ УПРАВЛІННЯ МЕРЕЖЕВИМИ СТРУКТУРАМИ

M. Perekytsai,

PhD student, State University of Economics and Technology

CONTEMPORARY RISKS AND CURRENT CHALLENGES OF NETWORK STRUCTURES MANAGING

У статті досліджено проблему сучасних ризиків та викликів управління мережевими структурами в умовах постіндустріальної економіки, з особливим акцентом на проблематиці кібербезпеки. Завданням дослідження автор поставив проведення поглибленого аналізу ключових загроз цифрового середовища, оцінку їхнього впливу на ефективність та стабільність мережевих взаємодій, а також визначення механізмів мінімізації негативних наслідків. Автором розглянуто зростання масштабів і складності кіберзагроз, а також визначено особливості інтеграції різноманітних пристроїв, програмних рішень і хмарних сервісів, що

посилюють уразливості мережевих структур. Особливий акцент зроблено на взаємозв'язку кіберризиків із ризиками монополізації та нестабільності мережевих структур, які у взаємодії формують замкнене коло загроз для цифрової економіки. Запропоновані автором практичні рекомендації включають розбудову кіберстійкості, диверсифікацію платформ, розвиток прозорості та міжнародну координацію зусиль. Отримані результати мають як наукову, так і прикладну значущість, оскільки спрямовані на забезпечення стійкості та конкурентоспроможності мережевих структур у глобальному середовищі.

The article examines contemporary risks and current challenges in managing network structures within the post-industrial economy, with a particular focus on the issue of cybersecurity. The purpose of the study is to provide an in-depth analysis of the key threats emerging in the digital environment, to assess their impact on the efficiency and stability of network interactions, and to identify mechanisms for minimizing their negative consequences. Special attention is given to the growing complexity of networks, resulting from the integration of diverse devices, software solutions, and cloud services, which significantly expand the potential attack surface and create new vulnerabilities. The study highlights the rapid growth of cyber threats, the insufficiency of monitoring and management mechanisms, and the escalating importance of resilience in network ecosystems.

Furthermore, the article investigates the interrelation between cybersecurity risks, monopolization risks, and network instability. It is argued that cyber risks represent a primary factor amplifying the scale of threats, while monopolization and instability increase the potential damage caused by cyberattacks, thus forming a closed loop of systemic vulnerabilities. This nexus not only threatens the sustainability of digital infrastructures but also hinders competition, innovation, and trust in global digital markets.

On the basis of this analysis, the article proposes a set of practical recommendations aimed at enhancing resilience and competitiveness of network

structures. Among them are the development of multilayered cybersecurity systems, diversification of platforms and services to avoid excessive dependence on a few providers, implementation of unified regulatory standards, improvement of transparency and information sharing among participants, investment in human capital, and the establishment of international cooperation in the field of cyber defense.

The scientific significance of the research lies in advancing conceptual approaches to risk assessment and management in complex digital ecosystems, while its practical value is reflected in the applicability of the findings for different business networks. Ultimately, the article demonstrates that cybersecurity should be perceived not merely as a technical challenge but as a strategic determinant of stability, trust, and long-term competitiveness in the global post-industrial economy.

Ключові слова: *мережеві структури, управління мережевими структурами, ризики, кібербезпека, діджиталізація.*

Keywords: *network structures, network structure management, risks, cybersecurity, digitalization.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. У постіндустріальній економіці мережеві структури стають однією з ключових форм організації бізнесу та суспільних взаємодій. Вони забезпечують гнучкість, швидкість обміну інформацією та інноваційність, що робить їх конкурентною перевагою у глобалізованому світі. Водночас саме мережевий характер таких систем зумовлює підвищену вразливість до суттєвого обсягу ризиків, серед яких особливе місце посідають загрози у сфері кібербезпеки.

З огляду на зростання цифровізації та залежності від інформаційних технологій, мережеві структури є достатньо уразливими для кіберзлочинності, кібершпигунства та атак на критичну інфраструктуру.

Кібератаки можуть призвести не лише до втрати даних чи фінансових збитків, а й до руйнування довіри між учасниками мережевої структури, що підриває її стійкість у цілому, а, отже, питання кібербезпеки виходить за межі технічного аспекту й стає стратегічним завданням управління.

Варто відзначити, що, окрім кіберзагроз, управління мережевими структурами супроводжується викликами, пов'язаними з ризиком монополізації ринку цифровими платформами та нестабільністю горизонтальних зв'язків у мережах. Проте саме кібербезпека виступає критичною умовою їхнього функціонування, оскільки без захищених каналів взаємодії та гарантії безпеки даних інші управлінські механізми втрачають свою ефективність. Таким чином, дослідження ризиків і викликів управління мережевими структурами, з особливим акцентом на кібербезпеку, є необхідною передумовою для формування надійних і конкурентоспроможних економічних систем у постіндустріальну добу. При цьому, дослідження ризиків управління мережевими структурами має як теоретичне, так і прикладне значення. Наукова позиція даної проблематики полягає у розробці концептуальних підходів до аналізу ризиків управління мережевими структурами в умовах постіндустріальної економіки. Особливу увагу, при цьому, варто приділяти кібербезпеці як критичному чиннику стабільності та розвитку мережевих систем, що дає можливість поглибити теоретичне розуміння вразливостей сучасних організаційних форм та шляхів їх подолання. Водночас практичний аспект полягає у можливості використання отриманих результатів для формування ефективних механізмів управління ризиками, в першу чергу, для мережевих бізнес-структур, що інтегровані у цифрові екосистеми.

Аналіз останніх досліджень і публікацій. Проблематика управління мережевими структурами є достатньо широко висвітленою як в світовій, так і вітчизняній науковій спільноті. Варто відзначити, що в своїх працях О. Стащук [4], В. Македон [9], Т. Дзядук [2], Б. Вікторов [1], О. Шведюк [5] та деякі інші так чи інакше торкаються питання існуючих ризиків та викликів в

умовах функціонування мережевого бізнесу та управління ним. Зокрема, О. Стащук піднімає вкрай актуальне питання загроз фінансово-економічній безпеці підприємств мережевих структур в умовах невизначеності. Водночас зарубіжні вчені Ш. Бензаїд, Т. Талеб та Сонг Дж.-С. [7] в свої доробках пропонують нову автономну та когнітивну систему управління безпекою, яка забезпечує детальне управління «бездотичною» безпекою на різних рівнях (тобто мережеві функції, підсекція та сегмент) та в різних адміністративних та технологічних областях різних форм бізнесу. Суттєвий інтерес також становить науковий підхід Л. Худіянто, Д. Хіндарто [8] та інших, які розглядають систему ризиків управління в бізнес-структурах крізь призму архітектури підприємства.

В той же час, враховуючи динамічний розвиток підприємницького середовища, ринків та IT-технологій, питання ризиків та викликів управління мережевими структурами в сучасному контексті не стоїть на місці та потребує подальших поглиблених наукових розвідок.

Формулювання цілей статті. Метою дослідження є проведення поглибленого аналізу сучасних ризиків та викликів, що виникають у процесі управління мережевими структурами в умовах постіндустріальної економіки, з акцентом на проблематиці кібербезпеки, що передбачає виявлення основних загроз цифрового середовища, оцінку їхнього впливу на ефективність і стабільність мережевих взаємодій, а також визначення механізмів мінімізації негативних наслідків. Дослідження має на меті розкрити взаємозв'язок між кіберризиками, ризиками монополізації та нестабільності мереж, а також сформувати практичні рекомендації для підвищення стійкості та конкурентоспроможності мережевих структур у глобалізованій економіці.

Виклад основного матеріалу дослідження. Сучасний світ бізнесу перебуває у стані постійних змін і трансформацій. Компаніям дедалі частіше доводиться працювати в умовах нестабільності ринку, зростаючої конкуренції та стрімкого розвитку технологій. У таких реаліях традиційні організаційні моделі поступово втрачають свою ефективність, адже вони не здатні

забезпечити достатню швидкість реагування на виклики та гнучкість у пристосуванні до нових обставин. Замість класичних ієрархічних структур дедалі більшої популярності набувають інноваційні, гнучкіші та адаптивні форми управління. Однією з таких альтернатив є мережева організаційна структура. Вона передбачає створення системи управління, у якій ключові підрозділи компанії функціонують із високим рівнем самостійності, тоді як координація їхньої роботи здійснюється відносно невеликим центральним офісом [6, с.48]. На відміну від традиційної ієрархії, де потоки влади й інформації рухаються зверху вниз, мережева модель робить акцент на горизонтальні зв'язки між підрозділами [5, с.23]. Такий підхід дозволяє підвищити гнучкість компанії, сприяє ефективнішій взаємодії та забезпечує здатність швидко реагувати на зміни ринкової ситуації.

Мережева організаційна структура є однією з найбільш сучасних моделей управління, яка активно використовується компаніями для забезпечення гнучкості, швидкого прийняття рішень та ефективної взаємодії між підрозділами. Її ключова особливість полягає у відносній самостійності підрозділів та горизонтальних зв'язках, що дозволяють швидше адаптуватися до нових умов. Проте, попри низку переваг, саме мережева модель бізнесу виявляється найбільш уразливою до зовнішніх і внутрішніх ризиків. Це пояснюється кількома факторами [6, с.50-51].

1. Висока залежність від зовнішнього середовища.

Мережеві структури функціонують у тісній взаємодії з партнерами, підрядниками, постачальниками та іншими зовнішніми учасниками ринку. Якщо один із ключових елементів мережі виявляється ненадійним або стикається з кризою, це миттєво впливає на всю систему. Наприклад, збій у роботі логістичного партнера може паралізувати діяльність компанії, навіть якщо її внутрішні підрозділи функціонують бездоганно. Така залежність робить мережеву структуру вкрай чутливою до коливань економіки, політичних рішень чи навіть локальних криз у регіоні.

2. Вразливість інформаційних потоків.

Оскільки в основі мережевої моделі лежать горизонтальні зв’язки та активний обмін даними між підрозділами, будь-який збій у комунікаціях може призвести до хаосу [3, с.98]. Якщо інформація передається із запізненням, спотворюється або потрапляє до конкурентів, це створює серйозні ризики. Крім того, мережева структура часто використовує цифрові платформи для координації дій, а отже, є більш підвладною кіберзагрозам і витокам конфіденційних даних.

3. Проблема контролю та координації.

Незважаючи на переваги автономії підрозділів, вона водночас створює ризики для цілісності компанії. Центральний офіс у мережевій структурі зазвичай невеликий, а тому має обмежені ресурси для моніторингу й контролю. У результаті можуть виникати ситуації, коли різні частини компанії рухаються у різних напрямках, приймають суперечливі рішення або вступають у конкуренцію між собою. Це послаблює єдність бізнес-моделі й підвищує ймовірність стратегічних помилок.

4. Нестабільність партнерських відносин.

Мережева структура значною мірою ґрунтується на довірі між партнерами. Але ринкові умови нестабільні: партнери можуть змінювати умови співпраці, підвищувати ціни, скорочувати постачання чи навіть переходити до конкурентів. Будь-яка така зміна створює ланцюговий ефект, що негативно впливає на всю систему. Замість стабільності, на яку розраховує бізнес, виникає невизначеність і необхідність постійно перебудовувати відносини.

5. Високий рівень конкуренції всередині ринку.

Мережеві структури зазвичай працюють у динамічних секторах економіки, де технології швидко змінюються, а конкуренти активно впроваджують нові рішення. В умовах такої конкуренції компанія, яка спирається на широку мережу партнерів, може виявитися менш маневреною, ніж більш централізовані структури. Якщо партнери не встигають адаптуватися до інновацій, це гальмує розвиток усієї компанії.

6. Психологічні та соціальні ризики.

Автономність підрозділів і горизонтальні зв'язки створюють сприятливе середовище для творчості, але водночас ускладнюють дисципліну й управління персоналом. Відсутність чіткої вертикалі влади може призводити до конфліктів між підрозділами, зниження мотивації співробітників або навіть втрати відчуття належності до єдиної компанії. У таких умовах зростає ризик кадрових проблем і зменшується лояльність працівників.

7. Ефект «доміно» у кризових ситуаціях.

Мережеві структури схильні до швидкого поширення проблем. Якщо один із елементів зазнає збою, це миттєво відбивається на інших підрозділах. Наприклад, зупинка виробництва у невеликому підрозділі може викликати затримку постачань у всій мережі, що вплине на продажі, фінанси та репутацію компанії. Таким чином, локальна проблема здатна перетворитися на системну кризу.

Отже, мережева організаційна структура є сучасною і прогресивною моделлю управління, яка має значний потенціал у динамічному бізнес-середовищі. Вона забезпечує швидкість прийняття рішень, гнучкість і високу адаптивність. Проте саме ці характеристики роблять її найбільш чутливою до ризиків та зовнішнього впливу.

В даному контексті слід відзначити, що останнє десятиліття характеризується різким зростанням кількості кібератак, що пояснюється як удосконаленням інструментів злочинців, так і збільшенням обсягів даних та інтеграцією бізнес-процесів у цифрове середовище. Сучасні мережеві структури часто використовують: IoT-пристрої (розумні датчики, обладнання, персональні гаджети), які мають низький рівень захисту; хмарні сервіси, де зберігаються критично важливі дані та застосунки; різноманітні програмні рішення, що інтегруються між собою, але створюють численні точки доступу для кібератак. Збільшення кількості цих елементів призводить до зростання кількості вразливостей. Зокрема, сучасні атаки стають дедалі складнішими:

використовуються методи соціальної інженерії, штучний інтелект для обходу захисту, комбіновані атаки на кілька рівнів одночасно. Це формує нову реальність, в якій управління мережевими структурами без належної уваги до кібербезпеки стає фактично неможливим.

Слід відзначити, що мережеві структури за своєю природою багаторівневі та динамічні. Включення нових учасників (компаній, платформ, індивідуальних користувачів), а також інтеграція інфраструктур різного рівня (локальні мережі підприємств, національні та глобальні платформи) значно ускладнює їх управління. До ключових факторів, що посилюють ризики, належать:

- гетерогенність учасників мережі (різний рівень цифрової зрілості та безпеки);
- відсутність єдиних стандартів кіберзахисту;
- недостатня прозорість у функціонуванні платформ, що може приховувати критичні вразливості [7, с.167].

Таким чином, чим складніша структура мережі, тим більше точок потенційного проникнення для кібератак і тим важче забезпечити ефективний моніторинг усіх процесів.

В свою чергу, своєчасний моніторинг мережевої структури є критичним чинником управління ризиками. Виявлення аномалій у роботі систем, підозрілої активності чи несанкціонованих доступів дозволяє знизити масштаби наслідків атак. Проте проблема полягає у величезному обсязі даних і необхідності їх обробки в реальному часі. Застосування систем штучного інтелекту та машинного навчання частково вирішує ці виклики, однак вимагає значних ресурсів і високої кваліфікації персоналу. Більше того, надмірна залежність від автоматизованих систем може створювати нові ризики, пов’язані з їхнім збоєм або маніпуляцією.

В таблиці 1 надамо узагальнене бачення впливу основних кіберризиків у контексті управління мережевими структурами.

Таблиця 1. Вплив ризиків на ефективність і стабільність мережевої структури

Тип загрози	Характеристика	Потенційний вплив на ефективність	Потенційний вплив на стабільність
Збільшення кількості кіберзагроз	Різноманітні атаки на дані, сервіси та користувачів	Зниження продуктивності, зростання витрат на відновлення	Порушення довіри, ризик колапсу мережевих зв'язків
Зростання складності мереж	Інтеграція різних пристроїв, сервісів і програм	Ускладнення управління, збільшення помилок	Нестабільність мережевих взаємодій, підвищення вразливості
Недостатній моніторинг	Відсутність оперативного реагування на атаки	Затримки в усуненні проблем, втрати ресурсів	Розповсюдження збоїв по всій мережі

*складено автором на основі [7, 9]

Виходячи з вищевикладеного, відзначимо, що для підвищення рівня стійкості мережевих структур у цифровому середовищі доцільно застосовувати комплексний підхід, що включає:

1) Впровадження багаторівневих систем кіберзахисту – використання комбінації технологій (фільтри, шифрування, багатофакторна автентифікація).

2) Розвиток систем моніторингу та аналітики в реальному часі – застосування інструментів штучного інтелекту для виявлення аномалій.

3) Стандартизація та регламентація безпеки – створення єдиних протоколів і стандартів у межах мережевих структур.

4) Навчання та підвищення кваліфікації персоналу – людський фактор залишається ключовою слабкою ланкою в системі захисту.

5) Розвиток культури довіри та прозорості – прозора політика обміну інформацією та колективна відповідальність за безпеку.

Застосування цих механізмів дозволяє знизити ризики втрати даних, забезпечити стійкість до зовнішніх атак і сформувати конкурентоспроможні мережеві структури.

Окремо слід зазначити, що кіберризики, ризики монополізації та нестабільності мереж тісно переплетені та взаємно підсилюють один одного. Так, кіберризики створюють основу для уразливості мережевих структур: витік даних чи атака на критичну інфраструктуру може порушити функціонування всієї системи. Це знижує довіру між учасниками мережі та формує передумови для дестабілізації. В свою чергу, монополізація цифрових платформ поглиблює вплив кіберризиків: концентрація даних і сервісів у руках кількох гравців робить їх надзвичайно привабливою ціллю для атак. Крім того, залежність від одного чи кількох провайдерів знижує варіативність рішень і гальмує розвиток конкурентного середовища. Водночас, нестабільність мережевих зв'язків (через відсутність прозорих правил, слабку координацію чи відтік учасників) у поєднанні з кіберзагрозами посилює ризик колапсу мережевої взаємодії. У нестабільних мережах навіть незначна атака або збій можуть спричинити лавиноподібні наслідки. На рис.1 наведемо «трикутник ризиків».

Рис.1. «Трикутник ризиків» управління мережевою структурою

*побудовано автором

Наведений рисунок відображає взаємозв'язок між трьома ключовими групами ризиків: кіберзагрозами, монополізацією та нестабільністю мережевих зв'язків. Усі вони взаємно підсилюють один одного, створюючи

загрозу функціонуванню мережевих структур. Стійкість можлива лише за умови комплексного управління всіма трьома типами ризиків одночасно.

Таким чином, кіберзагрози виступають первинним фактором, що підсилює монополізаційні ризики та провокує нестабільність, а монополізація та нестабільність, у свою чергу, збільшують масштаб і глибину наслідків кібератак. Це створює замкнене коло, розірвати яке можливо лише завдяки комплексним управлінським рішенням. Відповідно, управління мережевими структурами вимагає не лише розуміння природи ризиків, а й формування комплексної системи практичних заходів, спрямованих на їх мінімізацію. Особлива вага в цих заходах, при цьому, має бути відведена питанню кібербезпеки, яке виступає первинним фактором ризику та здатне підсилювати як тенденції до монополізації, так і загальну нестабільність мережевих взаємодій. Нижче запропонуємо ключові напрями підвищення стійкості й конкурентоспроможності мережевих структур у сучасних умовах.

1. Розбудова кіберстійкості як основа управління мережевими структурами.

Кіберстійкість — це здатність системи не лише захищатися від атак, а й швидко відновлюватися після інцидентів. Багаторівневий захист: застосування комбінації технологій (міжмережеві екрани, системи виявлення вторгнень, шифрування, багатофакторна автентифікація) забезпечує додаткові бар’єри для зловмисників.

Регулярне тестування вразливостей: проведення penetration testing та аудитів безпеки допомагає виявляти слабкі місця ще до того, як ними скористаються хакери.

Прогнозування загроз за допомогою ШІ: сучасні алгоритми здатні аналізувати мільйони подій у мережі й виділяти потенційно небезпечні сценарії, що знижує час реагування.

Таким чином, кіберстійкість є не стільки технічною опцією, скільки обов’язковою складовою стратегічного управління мережевими структурами.

2. Диверсифікація платформ і сервісів.

Залежність від одного постачальника послуг чи платформи створює ризики монополізації та підвищує привабливість такої системи для кібератак.

Використання мультихмарних рішень: розподіл даних та застосунків між кількома хмарними сервісами знижує ризик втрат у разі атаки чи збою.

Впровадження відкритих стандартів: сумісність сервісів і платформ забезпечує гнучкість та можливість швидко змінювати постачальника без суттєвих витрат.

Підтримка конкуренції: диверсифікація учасників ринку створює здорове конкурентне середовище, що стимулює інновації та знижує рівень монополізації.

3. Посилення регуляторних механізмів.

На глобальному рівні зростає потреба у встановленні прозорих правил гри на цифрових ринках:

– Антимонопольна політика: обмеження домінування великих цифрових платформ та підтримка малих і середніх гравців.

– Міжнародні стандарти кібербезпеки: гармонізація вимог щодо захисту даних і безпеки інфраструктур.

– Державна підтримка кіберзахисту: інвестиції у критичну цифрову інфраструктуру, розвиток центрів реагування на кіберінциденти.

– Регуляція має бути збалансованою: з одного боку — запобігати монополізації, а з іншого — не обмежувати інновації.

4. Прозорість і довіра у взаємодії.

У мережевих структурах довіра є основою стабільності. Кібератаки найчастіше підривають саме цей фундамент.

– Обмін інформацією про інциденти: створення механізмів колективного попередження й реагування дозволяє швидко локалізувати загрози.

– Прозора політика безпеки: компанії, які відкрито інформують партнерів і клієнтів про застосовані заходи кіберзахисту, формують стійкіші зв’язки.

– Колективна відповідальність: усі учасники мережі мають дотримуватися єдиних стандартів, оскільки слабка ланка може стати точкою входу для атаки.

5. Гнучкі моделі управління.

Жорсткі ієрархічні структури у цифровому середовищі часто виявляються менш ефективними.

– Децентралізація управління: використання блокчейн-технологій та смарт-контрактів дозволяє підвищити прозорість і безпеку операцій.

– Самоорганізація учасників: мережі, що здатні до автономного регулювання взаємодій, краще протидіють зовнішнім загрозам.

– Адаптивність: системи управління мають оперативно реагувати на зміни середовища та змінювати алгоритми взаємодії у разі виявлення ризиків.

6. Інвестиції у людський капітал.

Попри стрімкий розвиток технологій, саме люди залишаються центральною ланкою в системі безпеки.

– Цифрова грамотність: навчання співробітників базовим правилам кібергігієни (складні паролі, захист пристроїв, перевірка листів).

– Професійна підготовка фахівців: створення спеціалізованих освітніх програм для менеджерів із кібербезпеки.

– Формування корпоративної культури безпеки: співробітники повинні сприймати захист даних не як обтяження, а як частину бізнес-процесу.

7. Створення міжнародних партнерств.

Кіберзагрози не мають кордонів, тому локальні зусилля обмежені.

– Глобальна координація: міжнародні угоди та альянси у сфері кіберзахисту забезпечують оперативний обмін інформацією.

– Спільні проєкти: розробка міжнародних платформ для моніторингу й аналізу атак.

– Гармонізація регуляції: узгодження підходів до захисту даних, що спрощує інтеграцію мереж у глобальному масштабі.

8. Системний підхід до інтеграції заходів.

Важливо розглядати наведені рекомендації не як окремі кроки, а як взаємопов'язану систему.

– Кіберстійкість неможлива без інвестицій у людський капітал.

– Диверсифікація платформ має сенс лише у поєднанні з регуляторними механізмами.

– Прозорість і довіра не можуть бути досягнуті без гнучких моделей управління та децентралізації.

У результаті формується комплексна екосистема, де ризики кібербезпеки, монополізації та нестабільності взаємно врівноважуються за рахунок багаторівневих механізмів протидії.

Висновки та перспективи подальших розвідок у даному напрямі. Підводячи підсумки, слід зазначити, що управління мережевими структурами у постіндустріальній економіці супроводжується низкою ризиків, серед яких провідне місце займають кіберзагрози. Зростання складності мережевих систем, інтеграція різних пристроїв, програмного забезпечення та хмарних сервісів формують середовище з численними вразливостями. Недостатній рівень моніторингу та контролю може призвести до значних фінансових і репутаційних втрат, а також підриву довіри між учасниками мережевої структури.

Відзначимо, що кіберризики перебувають у тісному взаємозв'язку з ризиками монополізації та нестабільності. Концентрація даних і сервісів у руках кількох великих платформ робить їх привабливою ціллю для атак і водночас знижує варіативність управлінських рішень. Нестабільність горизонтальних зв'язків у мережах, посилена зовнішніми загрозами, здатна спричиняти лавиноподібні наслідки та навіть колапс мережевих взаємодій.

В свою чергу, з метою підвищення стійкості та конкурентоспроможності мережевих структур необхідне застосування

комплексного підходу, що поєднує технологічні, організаційні та соціальні заходи. Серед них — розбудова кіберстійкості, диверсифікація платформ і сервісів, впровадження єдиних стандартів безпеки, розвиток прозорості й довіри у взаємодії, інвестиції у людський капітал, а також міжнародна координація зусиль у сфері кіберзахисту.

Таким чином, кібербезпека постає не лише як технічний аспект, а як ключовий стратегічний чинник, що визначає стабільність, довіру та конкурентні переваги мережевих структур у глобальній економіці.

В контексті проведеного дослідження, подальші наукові розвідки у сфері управління мережевими структурами доцільно спрямувати на такі дослідницькі напрямки, як формування адаптивних механізмів управління ризиками, здатних швидко реагувати на зміну середовища та ескалацію загроз, а також вивчення міжнародного досвіду координації у сфері кіберзахисту та можливостей створення глобальних стандартів безпеки для мережевого бізнесу.

Література

1. Вікторов Б. В. Типи мережевих підприємств у міжнародному бізнесі. Вчені записки Університету «КРОК». 2020. № 2(58). С. 26-39.

2. Дзядук Т. В. Мережева економіка як елемент формування сучасної світової господарської системи. Економіка та держава. 2008. № 7. С. 25-27.

3. Кавун О. О. Підприємницькі мережі у роздрібній торгівлі України: сутність, класифікація і перспективи формування. Актуальні проблеми економіки. 2010. № 5 (107). С. 97-98.

4. Стащук О. В. Загрози фінансово-економічній безпеці підприємств мережевих структур в умовах невизначеності. Підприємництво і торгівля. 2023. № 39. С. 260-265. https://doi.org/10.32782/2522-1256-2023-39-33

5. Шведюк О. Визначення мережевої структури як сучасної форми координації економічної діяльності. Актуальні проблеми економіки. 2010. № 5 (107). С. 22-29.

6. Arifiyanto J. Company Forms in Digital Economy Era. Neoclassical Legal Review: Journal of Law and Contemporary Issues. 2023. № 2(1). P. 47-52.

7. Benzaid Ch., Taleb T., Song J.-S. AI-Based Autonomic and Scalable Security Management Architecture for Secure Network Slicing in B5G. IEEE Network. 2022. Vol. 36. No. 6. Pp. 165-174.

8. Judijanto L., Hindarto D., Wahjono S. I., Djunarto B. Edge of Enterprise Architecture in Addressing Cyber Security Threats and Business Risks. International Journal Software Engineering and Computer Science (IJSECS). 2023. Vol. 3 (3). P. 386-396.

9. Makedon V. Management of the Development of Network Structures of Industrial Companies in the Conditions of the Digital Economy. European Journal of Management Issues. 2024. №32(3). С. 195-205.

References

1. Viktorov, B.V. (2020), “Types of network enterprises in international business”, Vcheni zapysky Universytetu «KROK», vol. 2 (58), pp. 26-39.

2. Dziaduk, T.V. (2008), “Network economy as an element of the formation of the modern world economic system”, Ekonomika ta derzhava, vol. 7, pp. 25-27.

3. Kavun, O.O. (2010), “Business networks in retail trade in Ukraine: essence, classification and prospects for formation”, Aktual'ni problemy ekonomiky, vol. 5 (107), pp. 97-98.

4. Staschuk, O.V. (2023), “Threats to the financial and economic security of enterprises of network structures in conditions of uncertainty”, Pidpryiemnytstvo i torhivlia, vol. 39, pp. 260-265. https://doi.org/10.32782/2522-1256-2023-39-33

5. Shvediuk, O. (2010), “Definition of the network structure as a modern form of coordination of economic activity”, Aktual'ni problemy ekonomiky, vol. 5 (107), pp. 22-29.

6. Arifiyanto, J. (2023), “Company Forms in Digital Economy Era”, eoclassical Legal Review: Journal of Law and Contemporary Issues, vol. 2 (1), pp. 47-52.

7. Benzaid, Sh. Taleb, T. and Song, J.-S. (2022), “AI-Based Autonomic and Scalable Security Management Architecture for Secure Network Slicing in B5G”, IEEE Network, vol. 36, no. 6, pp. 165-174.

8. Judijanto, L. Hindarto, D. Wahjono, S.I. and Djunarto, B. (2023), “Edge of Enterprise Architecture in Addressing Cyber Security Threats and Business Risks”, International Journal Software Engineering and Computer Science (IJSECS), vol. 3 (3), pp. 386-396.

9. Makedon, V. (2024), “Management of the Development of Network Structures of Industrial Companies in the Conditions of the Digital Economy”, European Journal of Management Issues, vol. 32 (3), pp. 195-205.

Стаття надійшла до редакції 24.09.2025 р.