12. United Nations Development Programme (UNDP) Ukraine. (2024, February 20). *Assessment of the Impact of the War on MSMEs in Ukraine.* https://www.undp.org/ukraine/publications/assessment-wars-impact-micro-small-and-medium-enterprises-ukraine#:~:text=Micro%2C%20small%2C%20and%20medium,in%20the%20face%20of%20adversity

LARISA TERESHCHENKO. INFORMATION TECHNOLOGY AS A TOOL FOR IMPLEMENTING ECONOMIC AND MATHEMATICAL MODELS. *The article examines the role of modern information technologies as an effective tool for the implementation, optimization, and adaptation of economic-mathematical models in contemporary economic systems. Particular attention is paid to the transformation of analytical and decision-making processes under the influence of digital technologies such as cloud computing, big data analytics, artificial intelligence, and advanced simulation tools. The study emphasizes that economic-mathematical modeling increasingly relies on high-performance computing environments, integrated information systems, and digital platforms that ensure operational accuracy, scalability, and rapid processing of large datasets.*

The research reveals that the integration of information technologies significantly expands the functional capabilities of economic-mathematical models by enhancing the precision of forecasting, enabling real-time monitoring of economic processes, and supporting adaptive management under uncertainty. The article also outlines methodological approaches to constructing and validating models using software packages, specialized analytical platforms, and algorithmic modeling environments. The advantages of digital tools for solving optimization, simulation, econometric, and multi-criteria decision-making problems are systematically analyzed.

In addition, the study identifies key challenges associated with the technological implementation of economic-mathematical models, including issues of data quality, system interoperability, cybersecurity risks, and the need for highly qualified personnel. A comparative analysis of traditional and digitally enhanced modeling approaches demonstrates that the use of IT tools substantially improves computational efficiency, reduces the time needed for analytical procedures, and facilitates the transition from descriptive to predictive and prescriptive analytics.

The findings confirm that information technologies not only serve as auxiliary instruments but act as strategic enablers of innovative modeling solutions within economic research and practical management. The paper substantiates that the synergistic interaction between economic-mathematical modeling and digital technologies forms a methodological foundation for evidence-based decision-making, contributing to the stability, efficiency, and competitiveness of enterprises in conditions of market volatility and digital transformation.

Keywords: *information technologies, economic and mathematical models, digital tools, optimization, forecasting, modelling.*

УДК 33.027:338.246.8:658(477)
DOI: 10.31673/2415-8089.2025.043810

Тютюник Інна Володимирівна,
д.е.н., доцент,
Сумський державний університет
Михайлюк Олександр Степанович,
аспірант кафедри фінансових технологій і підприємництва
Сумський державний університет
Пасько Денис Віталійович,
аспірант кафедри економічної кібернетики
Сумський державний університет

НАЦІОНАЛЬНА БЕЗПЕКА В ЦИФРОВУ ЕПОХУ: СТРУКТУРНИЙ АНАЛІЗ КІБЕРРИЗИКІВ ТА ОРГАНІЗОВАНОЇ КІБЕРЗЛОЧИННОСТІ

У роботі здійснено типологізацію кіберризиків, проведено аналіз механізмів їх реалізації та оцінювання взаємодії з елементами кіберсуверенітету й кіберстійкості. Окрему увагу приділено ролі цифрових імперативів (кіберсуверенітету, кіберстійкості та кіберстримування) як взаємопов'язаних підсистем забезпечення національної безпеки. За результатами дослідження ідентифіковано основні канали впливу кіберзлочинної активності на фінансовий, інфраструктурний та оборонний сектори, сформульовано структурну модель взаємодії явних і латентних кіберзагроз та систематизовано чинники зниження національної кіберстійкості. Обґрунтовано накопичувальний характер латентних кіберризиків і їх здатність суттєво підсилювати наслідки відкритих кібератак, формуючи каскадні порушення в системі державного управління та критичної інфраструктури. Отримані результати підтверджують доцільність переходу від переважно активний підходів до превентивних моделей державної кіберполітики, орієнтованих на раннє виявлення та нейтралізацію прихованих загроз.

Ключові слова: *національна безпека, цифровізація, кіберризики, кібератаки, витік даних, латентні ризики.*

Постановка проблеми. Стрімкий розвиток цифрових технологій та їх інтеграція у більшість елементів системи державного управління створили передумови до формування принципово нових моделей функціонування національних економічних систем, механізмів забезпечення безпеки та функціонування оборонного сектору. З одного боку, впровадження цифрових технологій є дієвим інструментом підвищення ефективності управлінських рішень, налагодження взаємодії між окремими ланками економічної системи, створення умов для підвищення прозорості державних процесів та посилення інституційної спроможності країни. З іншого боку, саме цифрове середовище формує постійні ризики стабільного функціонування економіки, які проявляються як у вигляді відкритих атак на критичну інфраструктуру, так і у формі латентних загроз, що поступово накопичуються і здійснюють деструктивний вплив на стійкість держави у довгостроковій перспективі. В умовах високого рівня залежності суспільства від безперебійного функціонування інформаційних систем, дані збої і порушення їх роботи можуть спричинити масштабні наслідки.

В умовах цифрової трансформації національних економік кіберпростір перетворюється на один із ключових вимірів національної безпеки, де фінансові системи, державні інституції та критична інфраструктура стають пріоритетними цілями організованої кіберзлочинності та гібридних загроз. Суттєвої актуальності дані питання набувають в умовах збільшення частоти та масштабності кібератак, постійного удосконалення методів їх реалізації та активізації гібридних форм економічного, політичного та військового протистояння між державами. Кіберзлочинність поступово перетворюється з інструменту локального порушення інформаційної безпеки на системне та комплексне явище, що здатне блокувати роботу критичної інфраструктури, порушити функціонування державних інститутів та знижувати оборонні спроможності країни.

Незважаючи на високу актуальність питань забезпечення кібербезпеки та значний обсяг напрацювань у цій сфері, низка важливих аспектів все ще залишається недостатньо дослідженою. Зокрема, у науковій літературі відсутнє цілісне розуміння природи та форм прояву латентних ризиків на національну безпеку та ефективність наявних механізмів боротьби з ними. У цьому контексті системний аналіз структури кіберзагроз та наслідків їх впливу на національну безпеку в умовах цифрової епохи є вкрай важливим і своєчасним напрямом наукових досліджень для України.

Аналіз останніх досліджень і публікацій. Проблематика впливу фінансових кіберзлочинів на національну безпеку активно досліджується як у зарубіжній, так і у вітчизняній науковій літературі. Науковці та практики розглядають кіберпростір як повноцінну складову національної безпеки поряд із традиційними військовим, політичним, економічним та

інформаційним складовими. К. Хойрунніса, І. Амбарваті, Ю. Рахмадан та Д. Джубайді [10] розглядають кібербезпеку як невід'ємну складову загальної системи національної безпеки, а не лише як технічну підсистему захисту інформації.

У роботі [6] зазначається, що масштабні кіберзлочини у фінансовому секторі здатні провокувати значні прямі та непрямі втрати, підривати довіру до банківської системи та впливати на макрофінансові показники держави. Ці висновки узгоджуються з більш пізніми дослідженнями щодо операційних і кіберризиків у банківській сфері [3], де наголошується, що фінансові кіберінциденти можуть мати каскадний ефект і провокувати системну нестабільність.

Розвиток фінансових технологій і зростання ролі цифрових платформ у фінансовому секторі спричинили появу нового масиву досліджень. У систематичному огляді А. Алодхіані [5] встановлено, що FinTech-екосистеми стають одними з найбільш уразливих до кібератак через складність архітектури, інтеграцію численних цифрових сервісів і високий рівень автоматизації. Д. Джавагері та ін. [9] поглиблюють цей підхід, здійснюючи систематичний аналіз кіберзагроз у FinTech і показуючи, що їхній вплив виходить далеко за межі окремих фінансових організацій, трансформуючись у ризики для фінансової стабільності й довіри до цифрових фінансових інструментів.

Окремий напрям літератури присвячений взаємозв'язку між фінансовими кіберризиками та економічною безпекою держави. Фінансові злочини розглядаються як критичний фактор, що безпосередньо впливає на економічну безпеку, підриває функціонування інститутів фінансового моніторингу та може провокувати масштабні тіньові фінансові потоки. Позиція про стратегічний вплив кіберзлочинності на національну безпеку підтверджується також у роботі Л. Рибальченко та С. Охріменко [11], де підкреслено, що зростання кібератак на фінансову інфраструктуру має прямий зв'язок із ризиками дестабілізації критичних функцій держави.

У новітніх дослідженнях спостерігається зміщення фокусу в бік аналізу кіберризиків у контексті цифрової трансформації фінансових систем. О. Адекоя, Ф. Атлам та С. Лаллі [2] пропонують багатовимірну модель оцінювання впливу кібератак на цифрові фінансові сервіси, доводячи, що кіберінциденти охоплюють одночасно економічні, технологічні та соціальні аспекти. У роботі [1] розглядають роль кібербезпеки в захисті фінансів у цифрову епоху, акцентуючи на необхідності проактивної кіберполітики, посилення інституційної спроможності фінансових регуляторів і інтеграції кіберризиків у стратегії національної безпеки. Паралельно Янчюте Л. [8] аналізує виклики для фінансового сектору, пов'язані з переходом до квантово-стійкої криптографії, розглядаючи її як елемент довгострокового забезпечення фінансової та національної безпеки.

В науковому просторі також з'являються дослідження, присвячені моніторингу та систематизації кіберризиків у фінансовій сфері, де акцент робиться на потребі розроблення національної системи раннього виявлення кібератак і посилення інституційної спроможності держави протидіяти фінансовим кіберзлочинам [4]. Додатково, у глобальних аналітичних оглядах [7, 1] наголошується на тому, що фінансовий сектор стає однією з головних мішеней організованої кіберзлочинності та державних акторів, що підвищує значущість кібербезпеки для збереження державного суверенітету.

Узагальнюючи наявні дослідження, можна зробити висновок, що у більшості наукових праць фінансові кіберзлочини розглядаються як такі, що перетворилися на комплексний дестабілізуючий чинник із потенціалом створення економічних криз, підриву функціонування критичної інфраструктури та зменшення стійкості держави до гібридних загроз. При цьому в сучасній літературі все ще недостатньо представлені роботи, які б комплексно структуризували прямі та латентні фінансові кіберризики в контексті загальної системи національної безпеки.

Мета статті. Мета даного дослідження полягає у здійсненні структурного аналізу явних та латентних загроз національній безпеці в умовах цифрової трансформації та визначення їх впливу на функціонування державних інституцій, критичної інфраструктури та

обороноздатності країни.

Для досягнення поставленої мети передбачено вирішення наступних завдань:

– здійснити ідентифікацію явних та латентних кіберзагроз національній безпеці країни;

– провести аналіз структурних зв'язків між різними рівнями кіберзагроз, зокрема їх синергетичний вплив;

– дослідити напрямки трансформації механізмів функціонування державних інститутів під впливом кіберизиків.

Методи дослідження. Методологічну основу становить поєднання системного і порівняльного підходів, що дозволяє розглядати кіберризики як елементи багаторівневої системи національної безпеки. Комплексний характер виникнення кіберзагроз та масштабність їх наслідків обумовили необхідність застосування інструментів структурного, системного й функціонального аналізу. Це дозволило розглядати кіберризики не як окремі явища, а як елементи складної багаторівневої системи, що формується на перетині технологічних, економічних, інституційних та оборонних процесів.

Дослідження кіберзагроз як частини інтегрованої системи національної безпеки держави було здійснено за допомогою методу системного аналізу. Використання даного методу дозволило виокремити найбільш чутливі до кібератак структурні компоненти національної безпеки, окреслити їх функціональні характеристики та визначити прямі та синергетичні взаємозв'язки між різними видами загроз. Для систематизації кіберзагроз за критеріями відкритості, походження, механізмів реалізації та потенційних наслідків для національної безпеки було застосовано метод класифікації. Він забезпечив логічне групування загроз на явні та латентні, дозволив узагальнити особливості їхнього прояву та здійснити типологізацію ризиків, як передумови побудови концептуальної моделі протидії кіберзагрозам. За допомогою методу порівняльного аналізу було здійснено дослідження особливостей формування кіберзагроз у різних типах цифрових систем, а також ідентифіковано їх відмінності у різних секторах економіки (державне управління, фінансова сфера, енергетика, оборонний сектор).

Виклад основного матеріалу. В умовах активного розвитку цифрових технологій і їх поширення на всі сектори економіки національна безпека дедалі більше залежить від здатності держави формувати та підтримувати ключові цифрові імперативи, що забезпечують контроль над інформаційним середовищем, стійкість критичної інфраструктури та спроможність ефективно протидіяти агресії в кіберпросторі. У цьому контексті можна виділити три базові складові, що визначають сучасну модель забезпечення національної безпеки в умовах цифровізації. До таких імперативів належать кіберсуверенітет, кіберстійкість та кіберстримування, кожен з яких виконує окрему, але взаємопов'язану функцію у загальній системі національної безпеки (рис. 1).

Кіберсуверенітет передбачає здатність держави самостійно контролювати свій цифровий простір, включаючи інформаційні потоки, державні електронні сервіси, конфіденційні бази даних, критичні технології та канали стратегічних комунікацій. Забезпечення кіберсуверенітету можна розглядати у чотирьох основних аспектах: технологічному, що полягає у домінуванні національних цифрових технологій у ключових сферах роботи держави (державні реєстри, оборонні інформаційні системи, телекомунікації, енергетика тощо), юридичному (визначення правил збирання, обробки та передачі даних, обмеження доступу третіх сторін та іноземних платформ до конфеденційних даних тощо), інформаційному (можливість держави контролювати та управляти інформаційною політикою компаній, що працюють на території даної країни), технологічому (мінімізація залежності від іноземних хмарних сервісів, ПЗ тощо).

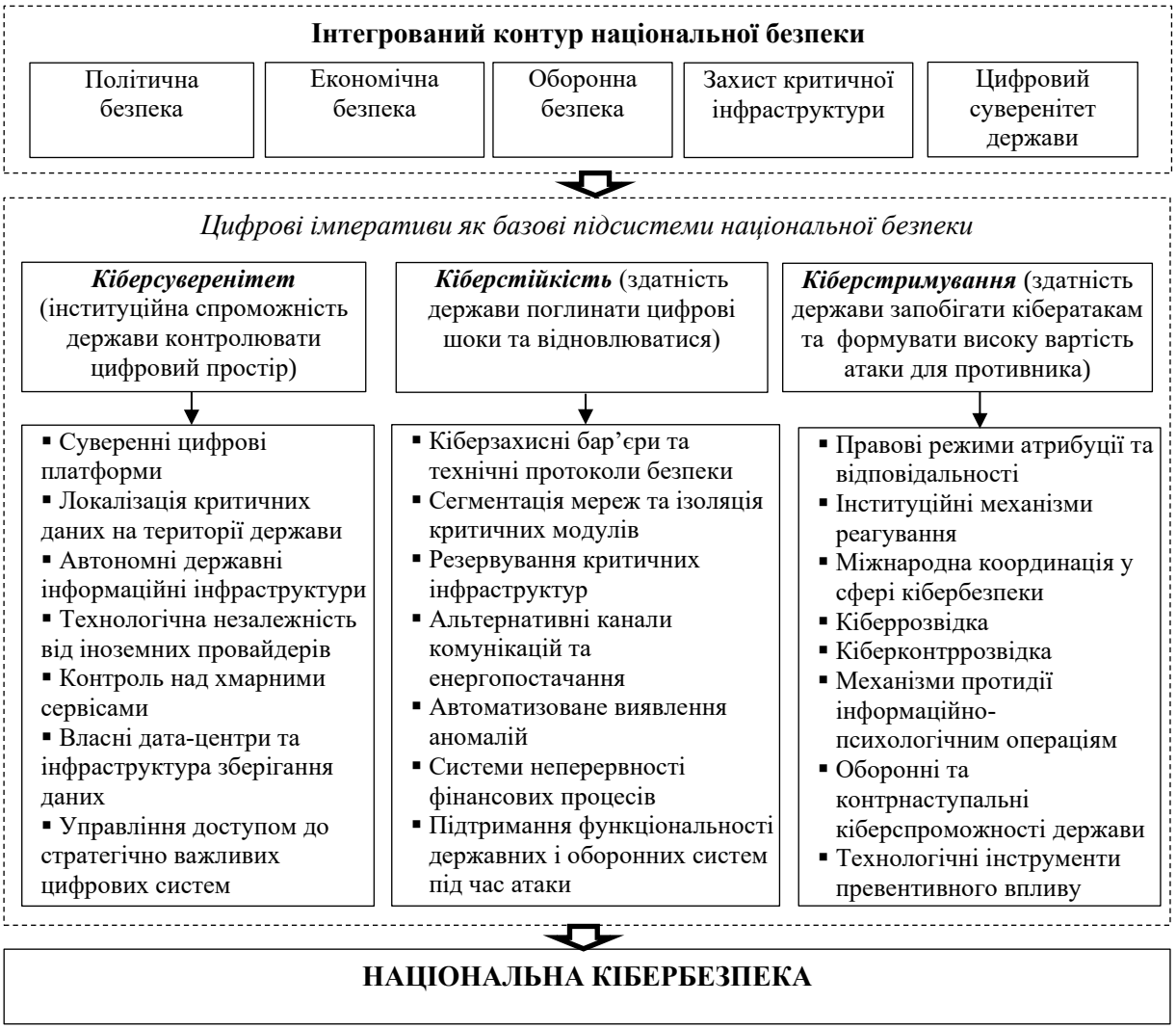

Рисунок 1. Цифрові імперативи в системі забезпечення національної безпеки

Втрата здатності країни самостійно контролювати ключові технологічні рішення призводить до появи ризиків зовнішнього втручання, шпигунства та маніпулювання цифровими даними. Це забезпечується за рахунок несанкціонованого доступу до державних інституцій, викрадення конфіденційних даних, впровадження шкідливого ПЗ, створення «точок входу» для майбутніх кібератак, порушення безперебійного управління критичними інфраструктурами.

Не менш важливою складовою формування національної безпеки країни в умовах активного розвитку кіберзлочинності є забезпечення є кіберстійкості, під якою розуміють здатність державних і недержавних інституцій протидіяти кібератакам, адаптуватися до нових загроз і швидко відновлюватися після них з мінімальними втратами. Її забезпечення передбачає формування технологічних бар'єрів (аутентифікація, шифрування тощо), що сприяють захищеності інформаційних систем, здатність служб безпеки швидко реагувати на кіберінциденти, постійну модернізацію процедур, технологій та програм підготовки кадрів відповідно до існуючих типів загроз, забезпечення безперервного виконання критичних функцій навіть у періоди масштабних кібератак, швидке повернення системи до поточного режиму роботи після припинення кібератаки та зникнення кіберзагрози. Забезпечення високого рівня кіберстійкості національної економіки зменшує ризик деструктивного впливу кібератак на систему державного управління, економічний розвиток та обороноздатність країни.

До найбільш типових ризиків, що загрожують порушенню кіберстійкості країни належать:

масштабні DDoS-атаки, що паралізують роботу цифрових сервісів, здійснення атак на системи критичної інфраструктури, маніпулювання даними, атаку на системи логістики, зв'язку та управління в секторі оборони тощо. Це суттєво знижує здатність держави до забезпечення стабільного функціонування ключових елементів системи не лише у періоди криз чи конфліктів, а і у періоди стабільності.

Здатність держави запобігати кібератакам та агресії за рахунок поєднання правових, технологічних, організаційних, дипломатичних та військових інструментів забезпечує кіберстримування. На відміну від кіберстійкості, яка передбачає реалізацію заходів спрямованих на протидію наслідків вже здійснених атакам, кіберстримування фокусується на їх попередженні. Реалізація даного аспекту забезпечення національної безпеки можлива за рахунок визначення чітких норм кримінальної відповідальності, контролю цифрових платформ та регулювання кіберпростору, встановлення потужних систем кіберзахисту, які роблять атаку економічно чи технічно недоцільною, спроможність держави здійснити кібератаку або застосувати інші інструменти національної оборони у відповідь на вчинені дії, розвиток міжнародної співпраці, участь у кіберкоаліціях, обмін інформацією про загрози, демонстрація технологічної переваги та спроможності ефективно реагувати на агресію.

Фактично розвиток кіберстримування сприяє формуванню «цифрового бар'єру», який знижує мотивацію противника до здійснення кібератак.

Однак постійне удосконалення та ускладнення способів здійснення кібератак, активне використання анонімних платформ і криптовалют для їх фінансування, залучення приватних хакерських груп державами-агресорами, а також нанесення репутаційних втрат державі через маніпуляції та дезінформацію значно знижують ефективність дій держави в напрямку стримування кіберзлочинності в системі управління національною економікою. Внаслідок цього цифрові загрози здійснюють безпосередній вплив не лише на державні інституції, але й на економічних суб'єктів, фінансовий сектор і ключові соціальні системи.

Всю сукупність загроз, що формуються в цифровому середовищі можна поділити на явні та латентні (рисунок 2).

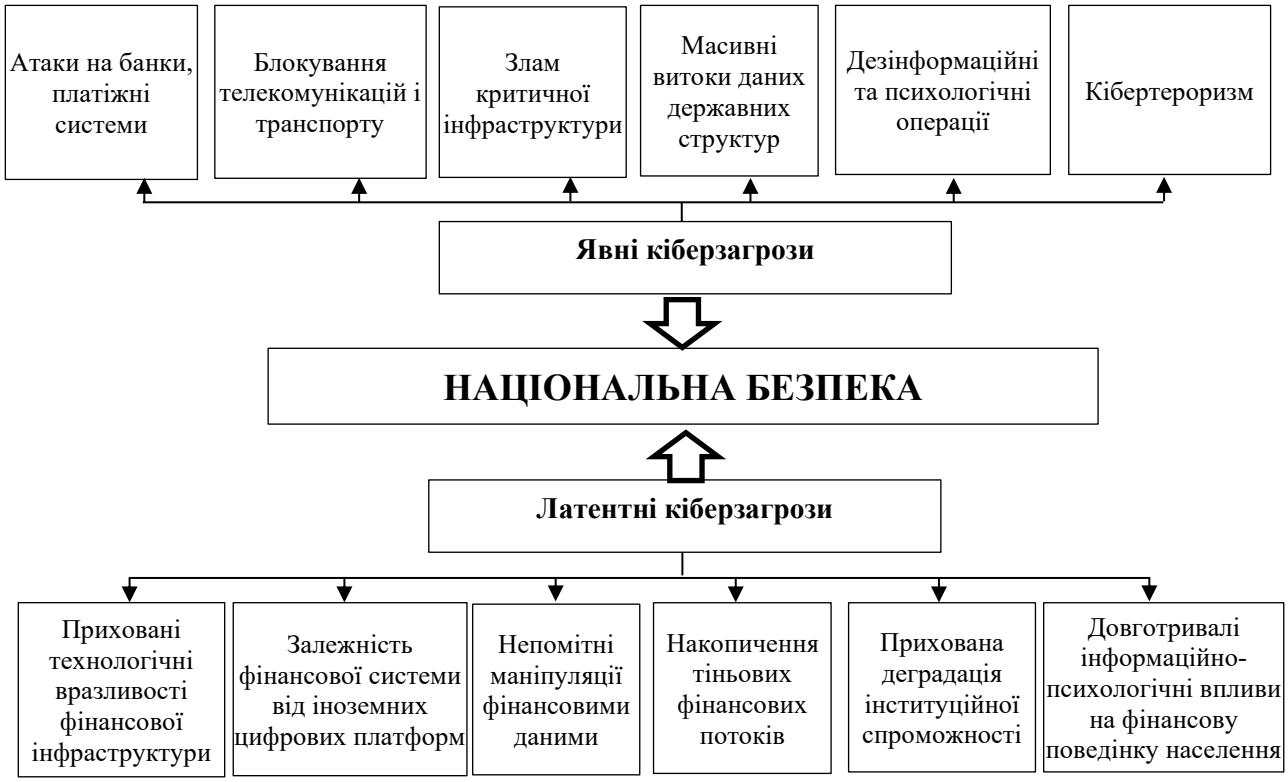

Рисунок 1. Структурна взаємодія явних і латентних кіберзагроз у системі національної безпеки

Явні кіберзагрози характеризуються відкритим, швидким та однозначним проявом, оскільки реалізуються у формі миттєвих атак, інцидентів чи спроб несанкціонованого втручання. Такі дії легко фіксуються технічними засобами, часто супроводжуються прямими матеріальними наслідками та здатні одразу порушувати роботу державних інститутів, фінансової інфраструктури або критично важливих об'єктів.

На відміну від явних загроз, латентні характеризуються прихованим накопиченням і тривалим періодом непомітної присутності в системі, коли шкідлива активність маскується під легітимні процеси та проявляється із запізненням. Дана категорія ризиків належать APT-кампанії, компрометація ланцюгів постачання, повільна ексфільтрація даних, інсайдерські впливи, приховані маніпуляції даними та підготовка до саботажу критичної інфраструктури. Такі загрози складніше виявляти та вимірювати, однак саме вони формують довгострокові системні ризики для стійкості фінансової й цифрової інфраструктури.

Явні та латентні кіберзагрози безпосередньо інтегровані в систему національної безпеки, оскільки впливають на ефективність управління державою, функціонування її критичної інфраструктури та суспільну довіру до публічних інститутів. Явні атаки такі як злом державних реєстрів, порушення роботи платіжних систем тощо мають швидкий і публічний ефект: вони здатні блокувати надання публічних послуг, зупиняти логістику та фінансові транзакції, провокувати соціальну напругу й підривати легітимність управлінських рішень. У кризових умовах такі інциденти набувають характеру гібридних операцій, коли кібервплив використовується як інструмент тиску на державу, а збитки виходять за межі IT-систем і трансформуються в економічні втрати, перебої в оборонному забезпеченні та зниження стійкості систем життєзабезпечення.

Латентні загрози створюють не менш критичні, але більш системні ризики для національної безпеки, оскільки вони спрямовані на довготривале зниження спроможностей держави. Прихований характер такого впливу дозволяє противнику накопичувати доступ до мереж, збирати чутливу інформацію про оборонні закупівлі, фінансові потоки, персональні дані та ключові контури управління.

Особливо небезпечними є латентні маніпуляції даними та інфраструктурою (підміна записів у реєстрах, спотворення фінансової звітності, непомітне втручання в системи управління), адже вони підривають довіру до управлінських рішень, ускладнюють юридичні процедури врегулювання питань і можуть проявитися в момент максимальної вразливості – під час пікових навантажень, воєнних загострень або відновлення економіки. Таким чином, явні загрози формують ключовий сегмент ризику, тоді як латентні мають накопичувальний ефект, а їх поєднання визначає реальний рівень кіберстійкості держави як складової національної безпеки.

Висновки. Отримані результати підтверджують, що в умовах цифрової трансформації національна безпека дедалі більше визначається не лише здатністю держави реагувати на кібератаки, а й спроможністю передбачати та нейтралізувати приховані механізми кіберзлочинної активності. Запропонований структурний поділ кіберзагроз на явні та латентні дає змогу перейти від фрагментарного розуміння інцидентів до системного їх бачення. Явні атаки формують критичні порушення в критичних сервісах, тоді як латентні загрози здійснюють накопичувальний вплив на ключові сегменти державного управління, фінансову інфраструктуру й довіру до інститутів. Це узгоджується з сучасним науковим дискурсом, у якому кіберпростір розглядається як повноцінний вимір національної безпеки, а фінансовий сектор – як одна з центральних цілей організованої кіберзлочинності та державних акторів.

У цьому контексті критично важливим є врахування синергетичного зв'язку між явними та латентними загрозами. У межах запропонованого підходу латентні ризики не просто функціонують паралельно з явними атаками, а посилюють їхні економічні, інституційні та репутаційні наслідки. Саме тому оцінювання національної кіберстійкості виключно на основі зареєстрованих інцидентів або прямих фінансових втрат призводить до систематичного заниження реального рівня вразливості. У більшості випадків фактичні збитки проявляються

з часовим лагом і мають непрямий характер, зокрема через підрив довіри, порушення інституційної спроможності та накопичення структурних дисбалансів. Відповідно, пріоритетом державної кіберполітики має стати зменшення кумулятивного впливу та нівелювання латентних загроз, а також підвищення чутливості систем раннього виявлення і превентивного реагування.

Результати також розкривають, що три цифрові імперативи забезпечення кібербезпеки (кіберсуверенітет, кіберстійкість і кіберстримування) функціонують як взаємопов'язані елементи єдиної системи національної безпеки, але мають різну ефективність щодо типів загроз. Кіберстійкість критично важлива для мінімізації наслідків явних атак і швидкого відновлення; кіберсуверенітет визначає контроль над даними, інфраструктурою та технологічною залежністю; кіберстримування знижує мотивацію атакувальника, проте його дієвість обмежується складністю атрибуції, транснаціональністю організованих груп і використанням анонімних платформ та фінансових інструментів.

Таким чином, перспективи подальших досліджень полягають у кількісній оцінці латентних загроз, зокрема через розроблення індикаторів раннього попередження (аномалії доступів, поведінкові патерни, ризики ланцюгів постачання), побудову сценарних профілів атак для фінансового та інфраструктурного секторів, а також із формалізацією механізмів взаємодії у вигляді причинно-наслідкових або мережевих моделей.

Дослідження виконано в рамках держбюджетної НДР «Моделювання механізмів протидії організованій та транснаціональній кіберзлочинності у воєнний та післявоєнний часи» (№ д/р 0124U000550), фінансування – Міністерство освіти і науки України.

References

1. Adejumo, A. P. & Ogburie, C. P. (2025). The role of cybersecurity in safeguarding finance in a digital era. World Journal of Advanced Research and Reviews, 25(03), 1542-1556. https://doi.org/10.30574/wjarr.2025.25.3.0909
2. Adekoya, O. A., Atlam, H. F., & Lallie, H. S. (2025). Quantifying the Multidimensional Impact of Cyber Attacks in Digital Financial Services: A Systematic Literature Review. *Sensors*, *25*(14), 4345. https://doi.org/10.3390/s25144345
3. Aldasoro, I., Gambacorta, L., Giudici, P., Leach T. (2022). The drivers of cyber risk, *Journal of Financial Stability*, 60, 100989. https://doi.org/10.1016/j.jfs.2022.100989.
4. Al-Kasassbeh, F.Y., Ghazleh, A. M. (2023). International and National Efforts to Protect Cyber Security: Jordan Case Study. *International Journal of Cyber Criminology*, 17(2), 350-363.
5. Alodhiani, A. (2023). Financial Technology (Fintech) and Cybersecurity: A Systematic Literature Review. *Arab Journal for Humanities and Social Science*, 10(8), 22-31. https://doi.org/10.59735/arabjhs.vi20.55
6. Antonescu, M., Birău, R. (2015). Financial and non-financial implications of cybercrimes in emerging countries. *Procedia Economics and Finance*, 23, 145-152.
7. Çifci, H. & Ergüner Özkoç, E. (2025). Analysis of National Cybersecurity Strategies of G20: objectives, latent themes, latest trends and comparisons. *Data & Policy*. 7. https://doi.org/10.1017/dap.2024.99
8. Jančiūtė, L. (2025). Cybersecurity in the financial sector and the quantum-safe cryptography transition: in search of a precautionary approach in the EU Digital Operational Resilience Act framework. *International Cybersecurity Law Review*, 6, 145-154 (2025). https://doi.org/10.1365/s43439-025-00135-7
9. Javaheri, D., Fahmideh, M., Chizari, H., Lalbakhsh, P. & Junbeom, H. (2023). Cybersecurity threats in FinTech: A systematic review. *Expert Systems with Applications, 241(1), 122697.* https://doi.org/10.1016/j.eswa.2023.122697
10. Khoirunnisa, K., Ambarwati, I., Rahmadan, Y., Jubaidi, D. (2025). Cyber Warfare and National Security. *China Quarterly of International Strategic Studies*, 11(01), p. 1-20. https://doi.org/10.1142/S2377740025500010

11. Rybalchenko, L., Ohrimenco, S. (2024). The impact of cybersecurity and crime on national security. *Philosophy, Economics and Law Review*, 4(2), 62-72. https://doi.org/10.63341/2786-491X-2024-2-62

INNA TIUTIUNYK, OLEKSANDR MYKHAILIUK, DENYS PASKO. NATIONAL SECURITY IN THE DIGITAL AGE: A STRUCTURAL ANALYSIS OF CYBER RISKS AND ORGANIZED CYBERCRIME. *In the context of the digital transformation of national economies, cyberspace is becoming one of the key dimensions of national security, where financial systems, state institutions and critical infrastructure are becoming priority targets of organized cybercrime and hybrid threats. The increasing complexity, stealth and transnational nature of cyberattacks necessitates the transformation of traditional approaches to security assessment, which are mostly focused on recording individual incidents and do not take into account the cumulative impact of latent forms of cyber influence. The aim of the study is to carry out a structural analysis of explicit and latent cyber threats and assess their impact on the functioning of the financial system, critical infrastructure and state institutions. The methodological basis is a combination of systemic and comparative approaches, which allows us to consider cyber risks as elements of a multi-level system of national security. The paper typifies cyber risks, analyzes the mechanisms of their implementation and evaluates their interaction with elements of cyber sovereignty and cyber resilience. Special attention is paid to the role of digital imperatives (cyber sovereignty, cyber resilience and cyber deterrence) as interconnected subsystems of ensuring national security. According to the results of the study, the main channels of influence of cybercriminal activity on the financial, infrastructure and defense sectors are identified, a structural model of the interaction of explicit and latent cyber threats is formulated and the factors of reducing national cyber resilience are systematized. The cumulative nature of latent cyber risks and their ability to significantly enhance the consequences of open cyber attacks, forming cascading violations in the system of public administration and critical infrastructure are substantiated. The results obtained confirm the feasibility of transitioning from predominantly proactive approaches to preventive models of state cyber policy, focused on early detection and neutralization of hidden threats.*

Keywords: *national security, cyber risks, cyber-attacks, data leakage, intelligent systems.*

УДК 005+004]:339.5
DOI: 10.31673/2415-8089.2025.043809

Фомішина Віра Миколаївна,
доктор економічних наук, професор
Херсонський національний технічний університет
Гужавіна Іна Василівна,
к.е.н., доцент
Державний університет
інформаційно-комунікаційних технологій
Огородник Руслан Петрович,
старший викладач
Херсонський національний технічний університет

СУТНІСТЬ І ОСОБЛИВОСТІ МЕНЕДЖМЕНТУ В ЗОВНІШНЬОТОРГОВЕЛЬНИХ ОПЕРАЦІЯХ

У статті представлено комплексне дослідження сутності менеджменту в зовнішньоторговельних операціях та визначено ключові особливості управління міжнародною комерційною діяльністю в умовах зростаючої глобальної взаємодії та цифрової трансформації бізнес-середовища. Актуальність теми обумовлена зростанням ролі зовнішньоекономічної діяльності для підприємств різних галузей та необхідністю підвищення