УДК 342.947
DOI https://doi.org/10.32782/1813-3401.2025.3.15

О. О. Тимошенко
кандидат економічних наук,
доцент кафедри інформаційної та фінансової безпеки Інституту безпеки,
ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом»
ORCID ID: 0009-0001-8227-8772

О. В. Турський
аспірант
ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом»,
ORCID ID: 0009-0009-2092-778X

О. Ф. Черток
викладач кафедри національної безпеки,
ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом»
ORCID ID: 0009-0001-8227-8772

ДЕРЖАВНЕ УПРАВЛІННЯ БЕЗПЕКОЮ ФІНАНСОВИХ УСТАНОВ У СИСТЕМІ ЕКОНОМІЧНОЇ БЕЗПЕКИ: СУЧАСНІ ВИКЛИКИ ТА МЕХАНІЗМИ РЕАГУВАННЯ

Стаття присвячена дослідженню державного управління безпекою фінансових установ як функціонального елементу системи економічної безпеки, що набуває критичної ваги в умовах воєнних ризиків, цифровізації та структурних трансформацій фінансового ринку. Акцентовано на ролі держави у формуванні стійкості банківського й небанківського секторів, забезпеченні довіри до фінансової системи та мінімізації системних наслідків кризових явищ для макрофінансової стабільності.

Проаналізовано сучасні виклики безпеці фінансових установ, пов'язані з кібератаками, шахрайством і соціальною інженерією, відмиванням коштів, операційними збоями, ризиками безперервності діяльності та інформаційною асиметрією в цифрових каналах. Проаналізовано управлінські інструменти державного впливу у сфері нагляду й регулювання, комплаєнсу, ризик-орієнтованого контролю, реагування на інциденти та координації між регуляторами, правоохоронними органами і суб'єктами фінансового сектору.

Досліджено необхідність переходу від переважно реактивних практик до проактивної моделі державного управління безпекою, заснованої на прогнозуванні, сценарному аналізі та інтегрованому ризик-менеджменті. Запропоновано підхід до формування механізмів реагування через поєднання нормативно-правових, організаційних, технологічних та інформаційно-аналітичних заходів, включно з розвитком стандартів кіберстійкості, посиленням процедур KYC/AML, удосконаленням обміну даними, аудиту й тестування стійкості, а також підвищенням культури безпеки персоналу.

Виявлено, що ефективність державного управління безпекою фінансових установ визначається здатністю забезпечити узгодженість регуляторних вимог, своєчасність реагування на загрози, доказовість управлінських рішень та баланс між інноваціями і контролем ризиків.

Ключові слова: *державне управління, економічна безпека, фінансові установи, фінансова безпека, кібербезпека, комплаєнс, ризик-орієнтований нагляд, безперервність діяльності, протидія шахрайству, AML/CFT.*

Постановка проблеми. Проблема зумовлена тим, що фінансові установи в Україні функціонують у середовищі багатоаспектних ризиків, де воєнні загрози, кібератаки, зростання шахрайства, тиск на платоспроможність позичальників, перебої інфраструктури та прискорена

цифровізація одночасно підвищують імовірність операційних збоїв та системних наслідків для економіки. За цих умов безпека банківського й небанківського секторів перестає бути суто внутрішньою функцією комплаєнсу або IT-захисту й трансформується у складову економічної безпеки держави, що безпосередньо впливає на довіру до фінансової системи, стійкість грошово-кредитного середовища, інвестиційний клімат і спроможність держави фінансувати критичні потреби.

Водночас існує розрив між швидкістю еволюції загроз і адаптацією механізмів державного управління: нормативно-правові та організаційні інструменти не завжди узгоджені між собою, міжвідомча взаємодія часто має фрагментарний характер, а моделі нагляду й контролю нерідко зберігають реактивну логіку, коли основні дії здійснюються після інциденту або кризи. Додатковим ускладненням виступає недостатня інтеграція ризик-орієнтованих підходів, процедур раннього попередження та аналітики даних у системі регулювання, що обмежує можливості прогнозування й своєчасного запобігання загрозам.

Проблема також полягає у необхідності балансування державної політики між посиленням регуляторних вимог і підтримкою інновацій, фінансової інклюзії та конкурентоспроможності ринку. Надмірне регуляторне навантаження може гальмувати розвиток цифрових сервісів і фінтеху, тоді як недостатність контролю підвищує вразливість до шахрайських схем, відмивання коштів, витоків даних і порушень безперервності діяльності. У результаті актуалізується потреба в науково обґрунтованому визначенні сучасних викликів, оцінці дієвості наявних механізмів реагування та формуванні цілісної моделі державного управління безпекою фінансових установ як системного інструмента забезпечення економічної безпеки.

Аналіз останніх досліджень і публікацій. Аналіз останніх досліджень і публікацій свідчить, що проблематика державного управління безпекою фінансових установ та її роль у системі економічної безпеки розкривається в працях О. І. Барановського, Ю. М. Харазішвілі, З. С. Варналія, В. М. Гейця, А. І. Даниленка, В. І. Мунтіяна, І. О. Лютого.

Водночас попри наявність значного теоретичного доробку залишаються дискусійними питання інтеграції ризик-орієнтованого нагляду, кіберстійкості, комплаєнсу та міжвідомчої координації у цілісну модель державного реагування на сучасні загрози фінансовому сектору, що зумовлює потребу подальших досліджень, спрямованих на уточнення механізмів управління стійкістю, доказовості управлінських рішень і підвищення результативності інструментів державної політики у сфері економічної безпеки.

Метою дослідження є обґрунтування сучасних викликів безпеці фінансових установ та визначення дієвих механізмів державного управління і реагування на загрози в системі економічної безпеки.

Виклад основного матеріалу. Безпека фінансових установ у сучасній економіці є не автономною функцією окремого банку чи страховика, а елементом національної стійкості, від якого залежить здатність держави підтримувати платіжну дисципліну, фінансувати критичні видатки, зберігати довіру вкладників і забезпечувати безперервність обігу грошей у легальному секторі. Умови воєнного стану, енергетичні та логістичні розриви, міграційні переміщення, зростання частки дистанційних фінансових сервісів і посилення гібридних загроз фактично змінюють саму природу ризиків, адже інцидент у сфері інформаційних технологій або порушення процесів обслуговування клієнтів можуть масштабуватися до ефекту доміно на ринку. У цих координатах державне управління безпекою фінансових установ має виходити з логіки системного ризику, коли першочерговим є не лише нагляд за виконанням нормативів, а й здатність регулятора організувати превентивну взаємодію між учасниками ринку, створити режими раннього попередження та забезпечити кризову керованість у разі шоків. Важливо, що законодавча рамка банківської діяльності прямо фіксує орієнтири на захист інтересів вкладників, стійкість і стабільність банківської системи [1], а отже питання безпеки набуває публічного змісту як умова реалізації загальносуспільного інтересу, а не лише корпоративної ефективності. У межах економічної безпеки це означає, що держава повинна забезпечувати такі управлінські режими, за яких приватні рішення фінансових установ не створюють неприйнятних зовнішніх ефектів для економіки, а стандарти управління ризиками стають обов'язковою інфраструктурою довіри.

Ключовим викликом для системи управління безпекою фінансових установ є трансформація загроз у цифровому вимірі, коли більшість критичних бізнес-процесів залежить

від інформаційно-телекомунікаційної інфраструктури, а обслуговування клієнтів масово відбувається через мобільні застосунки, віддалену ідентифікацію та інтегровані платіжні сервіси. Це підвищує вартість будь-якого збою, бо навіть короткочасна недоступність сервісів здатна спричинити панічні реакції, каскадні затримки платежів, втрати ліквідності та репутаційні втрати. Державна політика кібербезпеки формує базові правила та інституційну архітектуру реагування, визначаючи рамки координації, ролі суб'єктів і загальні принципи захисту життєво важливих інтересів у кіберпросторі [2]. Водночас практика доводить, що формальних норм недостатньо, якщо вони не підкріплені операційними механізмами контролю зрілості кіберзахисту, регулярним тестуванням стійкості та вимогами до корпоративного управління ризиками. Саме тому державне управління має бути побудоване як цикл: ідентифікація загроз і вразливостей, визначення регуляторних очікувань, контроль виконання, інцидент-менеджмент і відновлення, а також корекція правил на основі уроків інцидентів. Для фінансових установ такий підхід є критичним, бо цифрова конкуренція створює спокусу прискорювати вихід продуктів на ринок, інколи жертвуючи безпекою, і лише державний нагляд може утримувати баланс між інноваційністю та прийнятним рівнем ризику.

Окремий контур проблематики утворює залежність фінансового сектору від критичної інфраструктури, насамперед енергетики, зв'язку, дата-центрів, хмарних платформ, платіжних систем і каналів міжбанківського обміну даними. Для державного управління це означає необхідність інтегрувати фінансову безпеку в національну систему захисту критичної інфраструктури, адже фінансові установи водночас і споживають критичні послуги, і самі виступають критично важливим сектором для економіки. Українське законодавство про критичну інфраструктуру визначає правові й організаційні засади формування системи її захисту [3], що дозволяє розглядати безпеку фінансових установ як частину ширшого державного завдання зі збереження керованості країни в умовах кризових подій. На практиці це має втілюватися через вимоги до безперервності діяльності, резервування каналів зв'язку, географічного рознесення критичних компонентів, процедур аварійного відновлення, а також через узгоджені протоколи взаємодії з операторами критичної інфраструктури. Додатково виникає питання сумісності стандартів: фінансовий нагляд може вимагати одних рівнів резервування, а профільні органи з питань інфраструктури інших, і без державної координації установи отримують суперечливі імперативи. Тому управлінський ефект досягається тоді, коли держава задає єдині мінімальні стандарти стійкості та забезпечує міжвідомчий механізм їх узгодження, включно з обміном даними про інциденти та спільним плануванням кризових сценаріїв.

Управлінська спроможність держави значною мірою проявляється в якості регуляторних актів і здатності регулятора перетворювати загальні норми на конкретні вимоги до організації процесів безпеки. Показовим у цьому сенсі є посилення вимог до інформаційної безпеки та кіберзахисту надавачів фінансових послуг у небанківському сегменті, де регулятор закріплює обов'язок учасників ринку привести діяльність у відповідність до нових вимог протягом перехідного періоду [4]. Така логіка є управлінськи виправданою, оскільки небанківський сектор часто включає платіжні компанії, фінансові компанії та інші установи з високою технологічною інтенсивністю, але неоднорідною зрілістю систем захисту. Державний підхід має поєднувати жорсткість у визначенні мінімальних стандартів і гнучкість у процедурі впровадження, щоб уникати одночасно і формалізму, і зупинки ринку. Важливим компонентом є вимога до управління ризиками через політики, регламенти доступу, навчання персоналу, інвентаризацію активів, управління уразливостями та реагування на інциденти, бо саме ці елементи найчастіше стають слабкою ланкою в організаціях, що швидко масштабуються. У контексті економічної безпеки це підсилює здатність держави локалізувати ризики на рівні окремої установи, не допускаючи їх переходу в системну кризу, і формує однакове поле довіри для клієнтів, незалежно від того, чи взаємодіють вони з банком чи небанківським надавачем послуг.

Поряд із нормативним регулюванням принципове значення має інституційна підтримка фінансового сектору в режимі оперативного реагування на кібератаки та обміну інформацією. Тут прикладом є діяльність профільного кіберцентру та команди реагування на інциденти в банківській системі, які мають на меті захист інформаційних ресурсів регулятора та допомогу банкам і небанківським установам у впровадженні заходів кібербезпеки [5]. З позиції

державного управління це створює «нервову систему» фінансової безпеки, коли інформація про інциденти не залишається всередині організації, а потрапляє в координоване середовище, де можливі швидке попередження інших учасників, типізація атак, формування рекомендацій і відпрацювання спільних сценаріїв.

Європейська регуляторна еволюція додатково демонструє перехід від розрізнених вимог до цілісної концепції цифрової операційної стійкості фінансового сектору. Регламент ЄС про цифрову операційну стійкість для фінансового сектору встановлює рамку, в якій управління ІКТ-ризиками, інцидент-репортинг, тестування цифрової стійкості та контроль за ризиками третіх сторін інтегруються в єдину систему регуляторних обов'язків [6]. Для українського контексту це важливо не лише як орієнтир євроінтеграційного зближення, а й як управлінська модель: державі доцільно вибудовувати механізми, що охоплюють повний ланцюг цифрової залежності, включно з постачальниками хмарних послуг, дата-центрами, процесингами та провайдерами програмного забезпечення.

Водночас цифрова стійкість фінансового сектору не може розглядатися ізольовано від загальнодержавної політики кібербезпеки, адже багато інцидентів мають перехресний характер, охоплюючи і фінансові сервіси, і інші критичні сектори. Директива ЄС щодо заходів для високого спільного рівня кібербезпеки задає комплексний підхід до кіберуправління, вимагаючи належних заходів управління ризиками, звітування про інциденти та контролю виконання для широкого кола суттєвих і важливих суб'єктів [7]. Для механізмів державного управління це означає, що безпека фінансових установ повинна бути вбудована в національні режими координації інцидентів, взаємодії з командами реагування, процедур обміну інформацією та планування стійкості. У практичному вимірі виникає завдання гармонізувати вимоги різних регуляторів і уникнути дублювання, коли одна й та сама подія вимагає множинних повідомлень у різні органи за різними форматами, що відволікає ресурси під час інциденту. Оптимальним є підхід, за якого держава забезпечує єдині стандарти класифікації інцидентів, інтероперабельність каналів зв'язку та спільні пороги суттєвості, а фінансовий регулятор уточнює галузеві специфікації, не руйнуючи єдності загального режиму. Таке управлінське рішення підвищує швидкість реакції, зменшує адміністративний тиск і підсилює доказовість аналізу інцидентів на рівні держави.

Система державного управління безпекою фінансових установ потребує також опори на міжнародні мінімальні стандарти пруденційного регулювання і нагляду, які встановлюють вимоги до корпоративного управління, внутрішнього контролю, управління ризиками та раннього втручання. Оновлені базові принципи ефективного банківського нагляду відображають логіку ризик-орієнтованого підходу та необхідність своєчасних наглядових дій, що прямо пов'язано з сучасними ризиками, включно з цифровізацією та операційною стійкістю [8]. Для українських умов це означає, що державі недостатньо контролювати формальні показники капіталу чи ліквідності без аналізу якості управління, культури комплаєнсу, технологічної архітектури та здатності банку виявляти ризики до того, як вони стануть матеріальними збитками.

Окремої уваги вимагає макрофінансовий аспект кіберризику, який дедалі більше розглядається як потенційне джерело системної нестабільності. Міжнародні аналітичні матеріали свідчать про зростання частоти кібератак і підвищення ймовірності екстремальних втрат, при цьому фінансовий сектор є одним із найбільш уражуваних через концентрацію даних і критичність сервісів [9]. Для державного управління це змінює методологію: кіберризик має бути інтегрований у макропруденційний нагляд і сценарне планування поряд із кредитним, ринковим і ліквідним ризиком. Практично це означає потребу в регулярних секторальних навчаннях, моделюванні відмови ключових провайдерів, оцінці міжсекторальних ефектів і підготовці планів комунікації для запобігання панічним настроям.

Важливим сегментом безпеки фінансових установ є протидія легалізації доходів, фінансуванню тероризму та іншим фінансовим правопорушенням, які посилюються в умовах війни, переміщення капіталу, тіньових схем і зростання транскордонних потоків. Національне законодавство визначає обов'язки суб'єктів первинного фінансового моніторингу, підходи до належної перевірки клієнтів, управління ризиками та взаємодії з уповноваженими органами [10], формуючи правову основу того, що в управлінській логіці можна назвати фінансовою «санітарією» економіки. Державне управління тут має дві взаємопов'язані цілі: з одного боку, мінімізувати використання фінансової

системи для злочинних цілей, а з іншого, не допустити паралічу легальних транзакцій через надмірну бюрократизацію процедур. Ефективний механізм реагування передбачає ризик-орієнтоване налаштування процедур KYC, інтеграцію аналітики транзакцій, використання типологій і червоних прапорців, розвиток інформаційного обміну між установами та державними органами, а також посилення відповідальності за комплаєнс на рівні керівництва установи. Для економічної безпеки це має прямий сенс: «брудні» потоки підривають конкурентні умови, викривляють ціни, фінансують дестабілізуючу діяльність і руйнують міжнародну репутацію держави, що знижує доступ до зовнішніх ринків капіталу. Отже, безпека фінансових установ у цьому вимірі є інструментом захисту легального економічного обігу та підвищення стійкості фінансової системи до криміналізації.

Висновки. Державне управління безпекою фінансових установ у системі економічної безпеки слід розглядати як комплексну публічно-управлінську функцію, спрямовану на збереження фінансової стабільності, безперервності критичних сервісів і довіри до фінансового сектору в умовах підвищеної невизначеності. У сучасних реаліях саме поєднання воєнних ризиків, цифровізації та високої взаємозалежності інфраструктур створює передумови для швидкої ескалації окремих інцидентів до системних наслідків, а отже визначальним стає превентивний характер державної політики та її здатність працювати в режимі раннього попередження і швидкого відновлення.

Доведено, що найбільш критичними викликами для фінансових установ є операційні та кіберризики, залежність від ІКТ-постачальників і цифрових платформ, а також необхідність уніфікації вимог до управління інцидентами, звітності та тестування стійкості. У цьому контексті релевантним орієнтиром виступає європейський підхід до цифрової операційної стійкості, який інтегрує управління ІКТ-ризиками, інцидент-репортинг, тестування та контроль ризиків третіх сторін у єдину регуляторну логіку. Паралельно загальносистемні вимоги до кіберуправління та міжсекторальної координації підсилюються підходами NIS2, що підкреслює потребу узгоджувати галузеві фінансові регуляції з національними режимами кібербезпеки.

Обґрунтовано, що результативність механізмів реагування в державному управлінні визначається не тільки жорсткістю нормативів, а й інституційною спроможністю забезпечувати нагляд, координацію, обмін інформацією та кризове управління на основі ризик-орієнтованих підходів і стандартів ефективного банківського нагляду. На національному рівні правова основа має підкріплюватися практичними протоколами взаємодії, спільними сценаріями реагування, вимірюваними показниками стійкості та відповідальністю керівництва фінансових установ за організацію системи безпеки в усіх ключових процесах.

У підсумку, пріоритетним напрямом розвитку державного управління безпекою фінансових установ є побудова інтегрованої моделі, яка поєднує пруденційний нагляд, цифрову операційну стійкість, захист критичної інфраструктури, протидію фінансовим правопорушенням і комунікаційну стійкість у кризах. Така модель має забезпечувати здатність фінансового сектору безперервно надавати базові послуги, швидко відновлюватися після інцидентів і не допускати трансформації локальних порушень у системні загрози економічній безпеці держави.

Список використаної літератури:

1. Про банки і банківську діяльність : Закон України від 07.12.2000 № 2121-III // База даних Законодавство України / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2121-14
2. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII // База даних Законодавство України / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2163-19
3. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX // База даних Законодавство України / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/1882-20
4. Посилюється рівень інформаційної безпеки та кіберзахисту надавачів фінансових послуг // Національний банк України. 12.12.2025. URL: https://bank.gov.ua/ua/news/all/posilyuyetsya-riven-informatsiynoyi-bezpeki-ta-kiberzahistu-nadavachiv-finansovih-poslug
5. Cyber Security Center of the National Bank of Ukraine // National Bank of Ukraine. URL: https://cyber.bank.gov.ua/en
6. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector // EUR-Lex. URL: https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng
7. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2) // EUR-Lex.

URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng
8. Core Principles for effective banking supervision / Basel Committee on Banking Supervision. Basel : Bank for International Settlements, 2024. URL: https://www.bis.org/bcbs/publ/d573.pdf
9. Global Financial Stability Report. April 2024. Chapter 3. Cyber Risk: A Growing Concern for Macrofinancial Stability // International Monetary Fund. 2024. URL: https://www.imf.org/-/media/files/publications/gfsr/2024/april/english/ch3.pdf
10. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. The FATF Recommendations. Updated October 2025 // Financial Action Task Force. 2025. URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf

Tymoshenko O. O., Turskyi O. V., Chertok O. F. State management of financial institution security in the economic security system: current challenges and response mechanisms

The article is devoted to the study of state management of financial institutions' security as a functional element of the economic security system, which is becoming critically important in the context of military risks, digitalization, and structural transformations of the financial market. It focuses on the role of the state in shaping the stability of the banking and non-banking sectors, ensuring confidence in the financial system, and minimizing the systemic consequences of crises for macrofinancial stability.

It analyzes current challenges to the security of financial institutions related to cyberattacks, fraud and social engineering, money laundering, operational failures, business continuity risks, and information asymmetry in digital channels. The management tools of state influence in the areas of supervision and regulation, compliance, risk-based control, incident response, and coordination between regulators, law enforcement agencies, and financial sector entities are analyzed.

The need to move from predominantly reactive practices to a proactive model of state security management based on forecasting, scenario analysis, and integrated risk management is explored. An approach to the formation of response mechanisms is proposed through a combination of regulatory, organizational, technological, and information and analytical measures, including the development of cyber resilience standards, strengthening KYC/AML procedures, improving data exchange, auditing and testing resilience, and enhancing the security culture of personnel.

It has been found that the effectiveness of public administration of financial institutions' security is determined by the ability to ensure the consistency of regulatory requirements, timely response to threats, the evidence base for management decisions, and the balance between innovation and risk control.

Key words: *public administration, economic security, financial institutions, financial security, cybersecurity, compliance, risk-based supervision, business continuity, anti-fraud, AML/CFT.*

Дата першого надходження рукопису до видання: 20.07.2025
Дата прийнятого до друку рукопису після рецензування: 24.08.2025
Дата публікації: 30.09.2025