МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ

МАУП

ISSN 3083-6557 print

НАУКОВІ ПРАЦІ МАУП

Проблеми модернізації України

Випуск 1 (48), 2025

Київ
2025

УДК 330-339; 321.7; 159.9
М58

Схвалено Вченою радою Міжрегіональної Академії управління персоналом (протокол № 4 від 28.05.2025)

Редакційна колегія:
С. В. Храпатий (голова), д-р фіз.-мат. наук, проф.
І. А. Семенець-Орлова, д-р наук з держ. упр., проф.
Я. М. Раєвська, д-р психол. наук, проф.
С. О. Лисенко, д-р юрид. наук, проф.
А. І. Федосов, д-р мед. наук, проф.
М. І. Зубрицький, д-р. юрид. наук
О. М. Гордієнко, канд. техн. наук
В. І. Меджебель (*Чуєнко*), канд. юрид. наук
Л. М. Крива, канд. істор. наук
І. М. Капеліста (виконавчий редактор), канд. наук з держ. упр.
Є. Я. Черняк

Матеріали подано в авторській редакції.
Відповідальність за зміст та орфографію матеріалів несуть автори.

Міжрегіональна Академія управління персоналом.
М58 Наукові праці МАУП. Проблеми модернізації України / редкол.: С. В. Храпатий (голова) [та ін.]. Вип. 1 (48). Київ: Міжрегіональна Академія управління персоналом, 2025. 686 с. Бібліогр. в кінці ст.

У збірнику висвітлено матеріали X Міжнародної науково-практичної конференції "Розбудова інноваційних економіки, менеджменту та освіти в умовах нової соціальної реальності" (Київ, Міжрегіональна Академія управління персоналом, 20–22 травня 2025 р.).

Наведено тези доповідей учасників науково-практичної конференції МАУП з проблематики широкого кола аспектів процесу системної модернізації України.

Для науковців, громадсько-політичних діячів, студентів, а також усіх, хто цікавиться розвитком Української держави і світовим досвідом проведення модернізаційних процесів.

Видається з 2001 року.
Періодичність: 1 раз на квартал.
Засновник: *ПрАТ "ВНЗ "Міжрегіональна Академія управління персоналом".*
УДК 330-339; 321.7; 159.9

© Міжрегіональна Академія управління персоналом (МАУП), 2025

А. П. Гринчук
Проведення оцінювання діяльності громадських організацій та установ, як окремий вид оціночної діяльності *506*

Ю. Е. Пашко
Охорона земель в містах а також інших населених пунктах *508*

Д. В. Святецький
Банкрутство фермерських господарств у новій реальності: виклики економіки та менеджменту *510*

Р. О. Поливач
Економічні санкції як відповідь міжнародного співтовариства на ядерну програму Ірану *513*

Я. В. Кушнір
Оренда території Гуантанамо як виклик принципу територіальної цілісності держав у міжнародному публічному праві *515*

А. А. Тернавська
Деякі аспекти криміналізації суспільно небезпечних діянь у сфері радіоекологічної безпеки *518*

СУЧАСНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

С. О. Лисенко
Формування державної політики у сфері інформаційної безпеки: пріоритети та інституційне забезпечення *521*

І. В. Сервецький
Моральна риторика, як ширма під час війни: між словом і смертю *523*

С. Г. Голубицький
Фінансові ризики в умовах сучасної геополітичної ситуації, як загроза економічній безпеці *525*

А. І. Тараненко
Забезпечення інформаційної безпеки фінансових установ в системі державного управління: сучасна методологія *528*

О. І. Ткаченко
Ідентифікація джерел інформації щодо викликів і загроз безпеці, крізь призму публічного управління *530*

О. В. Поляков
Перспективи розвитку нотаріату в умовах цифровізації: правовий аспект *532*

О. І. Полотнянко
Технічні інформаційні загрози виборчому процесу: правовий аспект *535*

Д. В. Шейбут
Сучасні міграційні процеси в ЄС: безпековий вимір *537*

5. Національний інститут стратегічних досліджень. Економічна безпека України в умовах довготривалої війни. 2024; Економічна безпека України в умовах високих воєнних ризиків та глобальної нестабільності. 2025. https://niss.gov.ua/
6. *Єфименко Т.* Економічна безпека України в умовах високих воєнних ризиків та глобальної нестабільності. *НІСД*. 10.04.2025. https://niss.gov.ua/

А. І. ТАРАНЕНКО
аспірант, ПрАТ "ВНЗ "Міжрегіональна Академія управління персоналом",
м. Київ, Україна,
ORCID ID: https://orcid.org/0009-0000-5429-1454

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ФІНАНСОВИХ УСТАНОВ В СИСТЕМІ ДЕРЖАВНОГО УПРАВЛІННЯ: СУЧАСНА МЕТОДОЛОГІЯ

У XXI столітті стрімка цифровізація фінансових послуг, глибока інтеграція інформаційних технологій у банківську, страхову, фондову та інші підсистеми фінансового ринку, а також зростання кіберзагроз і гібридних форм впливу перетворили інформаційну безпеку на критичний аспект функціонування держави. Особливо актуальним постає це питання для країн, які перебувають у стані зовнішньої агресії, трансформаційних викликів або глибоких реформ, як-от Україна. Фінансова система є не лише об'єктом атак, а й елементом національної безпеки, вразливість якої у сфері ІБ може призвести до колапсу бюджетної, банківської або платіжної системи, паніки на ринку або втрати міжнародної довіри. У такій ситуації інформаційна безпека має розглядатися не як вузько технічна чи суто галузева функція, а як об'єкт повноцінного державного управління, з чіткою стратегією, політикою, механізмами реалізації та контролю ефективності [1]. Формування сучасної методології забезпечення інформаційної безпеки фінансових установ вимагає синергії правових, інституційних, технологічних та аналітичних рішень, здатних відповідати на динаміку ризиків у цифровому середовищі.

Формування дієвої державної політики у сфері інформаційної безпеки фінансових установ потребує чіткого розмежування ролей між учасниками системи управління: центральними органами виконавчої влади, регуляторами, спеціалізованими кіберпідрозділами, аналітичними центрами, а також самими фінансовими структурами. Державне управління в цій сфері має передбачати не лише функцію нагляду та контролю, а й стратегічне прогнозування, координацію між суб'єктами, забезпечення обміну інформацією та стимулювання інновацій. Ключовими інституціями мають бути Національний банк України, як регулятор банківської та платіжної інфраструктури; Національний координаційний центр кібербезпеки при РНБО, як стратегічний аналітичний вузол; Держспецзв'язку, як оператор кіберзахисту державного рівня; та CERT-UA, як оперативна структура реагування [2]. Для ефективного функціонування цієї системи потрібно формувати єдину архітектуру державного управління ІБ фінансового сектору, в якій кожен елемент має чітко визначену компетенцію, канали зв'язку, механізми координації та відповідальності.

Не менш важливою є побудова методології, що враховує зміну характеру інформаційних загроз. Сучасні атаки на фінансові установи мають не лише технологічний, а й психологічний, економічний і навіть геополітичний зміст. Вони часто здійснюються в рамках комплексних інформаційно-психологічних операцій, спрямованих на дестабілізацію банківської системи, виведення коштів, компрометацію державних органів або зниження довіри до грошово-кредитної політики. Тому державне управління ІБ фінансового сектору має переходити від пасивного реагування до активного управління ризиками [3].

У цьому контексті слід застосовувати інструменти стратегічного аналізу, включно з прогнозуванням поведінки атакувальних груп, ідентифікацією вразливих секторів, аналізом сценаріїв порушення стабільності та моделюванням впливу атак на макроекономічні показники.

Методологія управління інформаційною безпекою повинна включати створення національної системи збору, зберігання, аналізу та обміну інформацією про інциденти. Така система має інтегрувати державні бази даних, корпоративні платформи фінансових установ, міжнародні стандартизовані формати (STIX, TAXII) та автоматизовані інструменти обміну (MISP, ThreatConnect). Особливу роль у цьому відіграє CERT-UA, який має функціонувати не лише як реактивна одиниця, а як центр розповсюдження знань, індикаторів компрометації, сигнатур атак, уразливостей, методик захисту. Держава має забезпечити зворотний зв'язок між учасниками фінансового ринку, сприяти добровільному, але захищеному обміну інформацією про інциденти без ризику репутаційних або санкційних наслідків.

Необхідним елементом є також гармонізація нормативно-правової бази. Національне законодавство має відповідати міжнародним стандартам — як у сфері кібербезпеки (ISO/IEC 27001, NIST Cybersecurity Framework), так і в частині регулювання фінансових послуг (PSD2, GDPR, EBA Guidelines). При цьому слід адаптувати ці вимоги до українського контексту, зокрема до реалій війни, відсутності повноцінної захищеної ІТ-інфраструктури, дефіциту кадрів та обмежених фінансових ресурсів. Законодавча модель має передбачати не лише обов'язки фінансових установ щодо забезпечення ІБ, а й гарантії з боку держави, включно з механізмами підтримки, субсидування впровадження технологій захисту, забезпечення сертифікації та навчання персоналу.

У структурі державного управління інформаційною безпекою важливим напрямом є оцінка готовності та стійкості фінансових установ до інформаційних загроз. Цей процес повинен базуватися на методиках аудиту інформаційної безпеки, з урахуванням специфіки сектору, рівня цифрової зрілості, типу операцій і масштабів ризику. Доцільно впроваджувати так звані TIBER-програми (Threat Intelligence Based Ethical Red-teaming), які дозволяють державі тестувати стійкість установ до реалістичних сценаріїв атак [4]. Водночас слід забезпечити перехід від формального аудиту до динамічного моніторингу — через створення обов'язкових індикаторів кіберстійкості, систем обліку інцидентів, а також щорічного публічного звіту про стан ІБ у фінансовому секторі.

Ключовим викликом у забезпеченні інформаційної безпеки фінансових установ є проблема кадрового дефіциту та нерівномірної цифрової компетентності. Державна методологія має передбачати механізми довгострокового інвестування у людський капітал: створення програм магістерської підготовки з ІБ у фінансовій сфері, запуск міжвідомчих академій кіберзахисту, проведення сертифікації фахівців, а також розвиток шкільної та університетської освіти у сфері цифрової грамотності. Крім того, важливо запроваджувати регулярні навчання і тестування знань працівників банків,

НФУ та регуляторів, із використанням симуляцій інцидентів, моделей фішингу, внутрішніх політик безпеки.

Джерела

1. *Бакалинський О. О.* Модель та методи визначення проектних характеристик систем управління інформаційною безпекою: монографія. Київ : ТОВ "Три К", 2020. 162 с. URL: https://www.researchgate.net/publication/348788054_Model_ta_metodi_viznacenna_proektnih_harakteristik_sistem_upravlinna_informacijnou_bezpekou_Monografia
2. *Зачосова Н. В.* Формування системи економічної безпеки фінансових установ : монографія. Черкаси : ПП Чабаненко Ю. А. Черкаси, 2016. 375 с. URL: https://eprints.cdu.edu.ua/563/1/%D0%BC%D0%BE%D0%BD%D0%BE%D0%B3%EF%BF%BD%2580%D0%B0%EF%BF%BD%2584%EF%BF%BD%2596%EF%BF%BD%258F_%D0%B7%D0%B0%EF%BF%BD%2587%D0%BE%EF%BF%BD%2581%D0%BE%D0%B2%D0%B0.pdf
3. *Скочиляс Павлів О. В.* Правові механізми забезпечення інформаційної безпеки в Україні. *Вісник НУ "Львівська політехніка"*. Серія: "Юридичні науки". 2024. Вип. 2 (42). С. 151–159. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2024/jul/35421/skochilyas-pavlivvisnik2.pdf
4. *Benjamin Fraser Scott*. 2020. Red teaming financial crime risks in the banking sector. *Journal of Financial Crime, Emerald Group Publishing Limited*. Vol. 28(1). P. 98–111. URL: https://ideas.repec.org/a/eme/jfcpps/jfc-06-2020-0118.html

О. І. ТКАЧЕНКО

викладач кафедри інформаційної безпеки
Інституту безпеки, ПрАТ "ВНЗ "МАУП"
oreol1606@gmail.com
ORCID ID: https://orcid.org/0009-0001-9073-5814

ІДЕНТИФІКАЦІЯ ДЖЕРЕЛ ІНФОРМАЦІЇ ЩОДО ВИКЛИКІВ І ЗАГРОЗ БЕЗПЕЦІ, КРІЗЬ ПРИЗМУ ПУБЛІЧНОГО УПРАВЛІННЯ

Сучасна парадигма публічного управління безпекою базується на визнанні інформації ключовим ресурсом формування державної політики, стратегічного прогнозування та превентивного реагування. Державні інститути оперують у середовищі багатовимірних загроз, де економічні, військові, екологічні й кібернетичні чинники переплітаються в єдині гібридні конфігурації, а отже доступність, достовірність і своєчасність даних про ризики перетворюється на критичну умову національної стійкості [1]. Відтак, ідентифікація, систематизація та верифікація джерел інформації набуває статусу пріоритетного управлінського інструмента, що визначає здатність держави коректно оцінювати динаміку загроз, розробляти обґрунтовані сценарії протидії та забезпечувати демократичну підзвітність.

Інституційний контекст формування інформаційної картини безпеки характеризується поліцентричністю: поряд із центральними органами виконавчої влади діє мережа розвідувальних структур, спеціалізованих регуляторів критичної інфраструктури, місцевих адміністрацій і профільних державних підприємств. Кожен