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*

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

суб'єкт володіє фрагментарними наборами показників, що відображають окремі аспекти загальнонаціональної безпекової мапи, проте відсутність інтегрованого реєстру або єдиного онтологічного словника, ускладнює горизонтальний обмін даними та провокує дублювання функцій. Саме тому запровадження міжвідомчих протоколів сумісності метаданих, обов'язкових стандартів класифікації інцидентів і спільних аналітичних платформ є фундаментальною умовою підвищення якості управлінських рішень [2].

Джерела офіційної статистики залишаються базовою опорою для урядового планування, хоча їхня актуальність суттєво залежить від періодичності збору, репрезентативності вибірок і прозорості алгоритмів агрегації. Звіти Держстату, Служби безпеки України, НКЦК, ДПСУ та казначейських органів формують "хребет" національної інформаційної системи безпеки, проте, без належного контексту відкритих даних і динамічних індикаторів, вони ризикують втратити оперативну цінність. У таких умовах, першочергового значення набувають технології автоматизованого стрімерінгу даних, які дозволяють урядовим аналітикам у режимі близькому до реального часу відстежувати зміни у фінансових потоках, критичних навантаженнях енергосистем і сплесках кіберінцидентів.

Широке поширення концепції open-source intelligence детермінує зростання ролі неурядових джерел, зокрема — агрегаторів соціальних мереж, краудсорсингових геоінформаційних платформ та незалежних OSINT-спільнот [3]. У публічному управлінні такі ресурси виступають каталізатором ранньої детекції кризових феноменів: цифрові сліди користувачів, патерни пошукових запитів і кореляції новинних потоків нерідко випереджають офіційні бюрократичні звіти. Разом із тим відсутність гарантованої вірогідності, наявність деструктивних інформаційних операцій і обмеженість верифікаційних інструментів ставлять перед державною владою складне завдання — розрізняти автентичні сенсори ризиків і умисні інформаційні атаки.

Аналітичні центри, академічні інституції та галузеві дослідницькі лабораторії забезпечують методологічну глибину аналізу, генеруючи експертні оцінки, порівняльні дослідження та сценарні моделі. Залучення університетів і think-tank-платформ до розроблення державно управлінських рішень посилює доказовий характер політик, підвищує прозорість і сприяє залученню міжнародного досвіду. Усе ж таки академічна сфера стикається з бар'єрами доступу до оперативної службової інформації, а відтак — формування механізмів контрольованого розсекречування та грантування дослідницьких ліцензій стає необхідною умовою збалансування безпекових і демократичних інтересів.

На глобальному рівні ключовими хабами даних виступають міжнародні організації — ООН, НАТО, ЄС, ENISA, Interpol, OECD, які акумулюють великі масиви статистики щодо кібернетичних, терористичних, екологічних і фінансових загроз [4]. Участь України в багатосторонніх аналітичних обмінах посилює горизонт порівняння, дозволяє коригувати національні методики оцінювання ризиків відповідно до європейських стандартів, а також пришвидшує адаптацію до директив NIS-2, CER, RESILION та інших нормативних рамок. Разом із тим ефективність транскордонного інформаційного співробітництва залежить від сумісності юридичних режимів конфіденційності, що зумовлює необхідність гармонізації положень про державну таємницю й захист персональних даних.

Приватний сектор, передусім оператори критичної інфраструктури — банки, телекомунікаційні компанії, енергетичні та транспортні системи — генерує високоточні відомості про стан інформаційної безпеки, фінансової стабільності та техногенної стійкості. Запровадження обов'язкових аудитів, зовнішніх penetration-тестів за

моделлю TIBER-UA та стандартизованого звітування про кіберінциденти перетворює бізнес на активного учасника національної системи ризик-менеджменту. Однак комерційна чутливість даних породжує ризик небажання розкривати повний обсяг інформації; вирішення цієї дилеми потребує створення правових стимулів і режимів захищеного обміну, коли учасники отримують гарантований імунітет від регуляторних санкцій за умови добросовісного ділення з державою релевантним індикативним мінімумом.

Громадянське суспільство та медійні платформи функціонують як незалежні монітори безпекових процесів, висвітлюючи інциденти, які можуть бути проігноровані через політичну доцільність або бюрократичну інерцію. Фактчекінгові проєкти, журналістські розслідування, платформи публічних звернень і сервіси е-петицій не лише сигналізують про загрози, а й створюють тиск на органи влади, змушуючи їх адаптувати політику реагування. Для легітимації такої взаємодії необхідно інституціоналізувати процедури inclusion governance — інтегрувати механізми громадського аналізу даних у національні платформи управління ризиками, одночасно забезпечуючи безпеку критичних свідчень через закони про захист викривачів і цифрові програми анонімізації.

Джерела

1. Про національну безпеку України: Закон України 21 червня 2018 р. № 2469-VIII. *Офіц. веб-сайт Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text
2. Директива (ЄС) 2022/2555 Європейського Парламенту і Ради від 14 грудня 2022 р. про заходи для забезпечення високого спільного рівня кібербезпеки в усьому Союзі. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj
3. ENISA. Threat Landscape 2024. European Union Agency for Cybersecurity. URL: https://www.enisa.europa.eu/publications/threat-landscape-2024
4. Global Cybersecurity Outlook 2025. *WEF Publishing*, 2025. 49 p. URL: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

О. В. ПОЛЯКОВ

старший викладач кафедри правоохоронної та антикорупційної діяльності Навчально-наукового інституту права імені князя Володимира Великого, ПрАТ "ВНЗ "МАУП", м. Київ, Україна
ORCID ID: https://orcid.org/0009-0003-3941-1165

ПЕРСПЕКТИВИ РОЗВИТКУ НОТАРІАТУ В УМОВАХ ЦИФРОВІЗАЦІЇ: ПРАВОВИЙ АСПЕКТ

У сучасному інформаційному суспільстві цифровізація поступово трансформує усталені підходи до функціонування класичних інституцій, зокрема й нотаріату. Нотаріальна діяльність, яка традиційно асоціюється із формалізацією правочинів, засвідченням фактів, перевіркою юридичної доброчесності угод і забезпеченням юридичної безпеки, дедалі більше потребує адаптації до електронного формату. Проблематика цифровізації нотаріату охоплює не лише технічні інструменти ав-