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

С. А. Іванов
Кібербезпека в системі національної безпеки України *540*

М. М. Мурга
Роль сучасної журналістики у забезпеченні національної безпеки *543*

О. Л. Сокур, О. З. Клименко
Цифрові технології у професійній діяльності інформаційно-бібліотечних працівників Національної академії наук України *546*

А. С. Нагорна
Відповідальність і санкції в міжнародному праві *548*

М. Д. Авраменко
Національна безпека *549*

Т. П. Палієнко
Національна безпека в умовах посилення глобальної інтеграції *552*

Ю. І. Кулінська
Міжнародне право *555*

М. Г. Гордієнко
Геноцидні практики російської агресії як інструмент асиміляційної політики *557*

Д. Д. Макаров
Правила виконання больових прийомів при силовому затриманні *560*

О. В. Сушко
Державна зрада посадовців як інструмент підриву державності: український вимір *562*

Є. Д. Шакун
Концептуалізація поняття "фінансово-економічна безпека" в наукових публікаціях: вітчизняний контекст *567*

І. В. Кудрявський
Способи підвищення ефективності механізмів державного управління у сфері захисту безпеки інформаційного простору *569*

С. О. Мартинюк
Роль OSINT для безпеки бізнесу: організаційно-правовий аспект *572*

В. В. Ровний
Правове регулювання державної політики у галузі освіти, як інструменту національної безпеки *574*

Т. Костюк
Political, social and humanitarian dimensions of war and post-war sustainability of Ukraine *576*

І. Л. Дідюк, Н. Д. Присяч
Людський капітал як фактор національної безпеки: виклики міграції та демографічної кризи в Україні *579*

10. *Євмєшкіна О.* Реалізація функції прогнозування на різних рівнях державного управління. *Державне управління та місцеве самоврядування*. 2017. Вип. 1(32). URL: https://scholar.googleusercontent.com/scholar?q=cache:vJnIMqsViesJ:scholar.google.com/+%D0%94%D0%B5%D1%80%D0%B6%D0%B0%D0%B2%D0%BD%D0%B5+%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D1%96%D0%BD%D0%BD%D1%8F:+%D1%81%D1%82%D1%80%D0%B0%D1%82%D0%B5%D0%B3%D1%96%D1%87%D0%BD%D0%B5,+%D1%81%D0%B5%D1%80%D0%B5%D0%B4%D0%BD%D1%8C%D0%BE%D1%81%D1%82%D1%80%D0%BE%D0%BA%D0%BE%D0%B2%D0%B5+%D1%96+%D0%BA%D0%BE%D1%80%D0%BE%D1%82%D0%BA%D0%BE%D1%81%D1%82%D1%80%D0%BE%D0%BA%D0%BE%D0%B2%D0%B5+%D0%BF%D0%BB%D0%B0%D0%BD%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F&hl=uk&as_sdt=0,5 (дата звернення 19.01.2025)
11. *Плаумен К. Д., Вілсон К.* (2018). Стратегія і тактика в стратегічній комунікації: вивчення їх перетину з використанням соціальних медіа. *Міжнародний журнал стратегічних комунікацій*. 12 (2). 125–144. https://doi.org/10.1080/1553118X.2018.1428979 (дата звернення 19.01.2025).

С. О. МАРТИНЮК

аспірант у галузі права, ПрАТ "ВНЗ "МАУП"
ORCID ID: https://orcid.org/0000-0001-7994-0828
sergeymartunyk98@gmail.com

РОЛЬ OSINT ДЛЯ БЕЗПЕКИ БІЗНЕСУ: ОРГАНІЗАЦІЙНО-ПРАВОВИЙ АСПЕКТ

У сучасній економіці публічно доступні дані формують багатовимірний інформаційний контур, у межах якого корпоративні активи стають дедалі вразливішими до кібернетичних та фізичних загроз; відстеження сигналів у відкритих джерелах — від офіційної фінансової звітності й судових реєстрів до соцмереж, спеціалізованих форумів і технічних телеметричних потоків — дозволяє компаніям миттєво виявляти репутаційні, операційні та регуляторні ризики, прогнозувати збої в ланцюгах постачання, коригувати маркетингові стратегії й ініціювати кризові протоколи ще до того, як негатив проявиться у фінансових показниках. Саме інтеграція Open Source Intelligence (OSINT) у вертикаль корпоративної безпеки мінімізує "інформаційний лаг" між подією й управлінською реакцією, формує доказову базу для рішень рівня C-suite та забезпечує взаємодію з зацікавленими сторонами на принципах прозорості, що безпосередньо впливає на вартість бренду й капіталізацію компанії; у період цифрової турбулентності навіть кілька годин сліпого вікна здатні коштувати десятків мільйонів доларів, тоді як ефективний OSINT-процес перетворює мінімальний масив відкритих даних на стратегічну перевагу [1]. Усе це підкреслює вагу відкритої розвідки як фундаментального елементу системи управління ризиками, який повинен бути закріплений внутрішніми політиками поряд із кіберзахистом, фізичною охороною та фінансовим контролінгом.

Понятійне підґрунтя OSINT, закріплене у "NATO Open Source Intelligence Handbook", визначає відкриту інформацію як перший, найдешевший і водночас наймасовіший рівень розвідувального циклу; документ докладно описує п'ять фаз:

планування збору, верифікацію достовірності джерел, аналітичну кореляцію, розробку розвідувального продукту та його дистрибуцію споживачам. Якщо в державному секторі ці процеси жорстко регламентовані службовими інструкціями, то у бізнес-середовищі потрібна адаптація до корпоративного управління та комплаєнсу: це означає розробку стандартів відбору легітимних джерел, документування логіки аналітичних висновків, захисту персональних даних клієнтів і комерційної таємниці, а також узгодження із зовнішніми аудиторами, щоби мінімізувати юридичні ризики. Унаслідок цього OSINT переходить від "ентузіастського" використання окремими співробітниками до статусу офіційної, бюджетованої функції, продукція якої вважається доказовою під час внутрішніх розслідувань, переговорів із партнерами й судових проваджень [2]. Отже, поняттєво-процедурна рамка НАТО, адаптована з урахуванням вимог приватного сектора, стає інституційним "хребтом" корпоративної розвідки.

З організаційного погляду OSINT-компонент найчастіше вбудовується у відділи ризик-менеджменту, корпоративної безпеки або GRC-офіси; практичні кейси транснаціональних корпорацій свідчать, що оптимальною є модель кросфункційної команди, до якої входять фахівці з кібербезпеки, юристи, маркетологи, дата-саєнтисти та кризові комунікатори, адже саме такий склад забезпечує повний цикл — від виявлення "сирих" індикаторів до формулювання бізнес-рекомендацій у форматі executive brief. Середньоринкове співвідношення "один аналітик OSINT на п'ятсот співробітників" слугує базовим орієнтиром, однак воно коригується залежно від регуляторного тиску, географічної диверсифікації та рівня публічної уваги до компанії; під час M&A-операцій, виходу на нові ринки чи загострення конфліктів у критичних регіонах OSINT-групи масштабуються експоненційно, аби покрити інформаційну асиметрію. Пріоритетами залишаються побудова аналітичних KPI, навчання співробітників етичним нормам моніторингу й розробка сценаріїв ескалації, коли OSINT-дані інкрустуються в офіційні канали прийняття рішень [3]. Таким чином формується живий, самонавчальний механізм, здатний гнучко реагувати на мінливе середовище загроз.

Українська нормативна база визнає цінність відкритих даних для комерційних потреб і водночас встановлює чіткі обмеження. Закон України "Про інформацію" (редакція 2024 р.) гарантує суб'єктам господарювання право на вільний збір та опрацювання публічних відомостей за умови поваги до персональних даних і комерційної таємниці, у той час як стаття 10-1 покладає на державні органи обов'язок забезпечувати достовірність і актуальність відкритих реєстрів, що дозволяє бізнесу зменшити операційні ризики, спираючись на гарантовану державою якість джерел. Водночас Кодекс України про адміністративні правопорушення та Кримінальний кодекс містять санкції за несанкціонований збір інформації, тож компаніям належить балансувати між оперативною потребою та правовими рамками, розробляючи чіткі гайдлайни для OSINT-аналітиків, щоб уникнути обвинувачень у "несанкціонованій розвідці" [4]. У підсумку українські підприємства отримують як правовий "зелений коридор" для легальної побудови відкритої розвідки, так і зобов'язання впроваджувати внутрішній контроль за дотриманням етичних стандартів.

Міжнародний вимір формується насамперед Європейським Союзом: Директива (EU) 2022/2557 (NIS 2) вимагає, щоб оператори критичної інфраструктури мали механізми раннього виявлення загроз, зокрема через OSINT-моніторинг, і повідомляли регуляторів протягом двадцяти чотирьох годин після ідентифікації інциденту; за невиконання передбачені штрафи до 2 % глобального обороту компанії. Для українського бізнесу, інтегрованого в європейські ланцюги постачання, імплементація

NIS 2 трансформується з нормативного обов'язку на фактор конкурентної переваги, адже контрагенти дедалі частіше вимагають підтвердження наявності OSINT-процедур у рамках due diligence. Паралельно загальноєвропейський регламент GDPR стимулює корпоративний сектор застосовувати модель "privacy-by-design": автоматичні фільтри деперсоналізують дані, а повна ідентифікація відбувається лише після юридичного скорингу, завдяки чому належна оцінка законних інтересів (LIA) стає ключовим аргументом у судових спорах щодо правомірності інформаційного збору [5]. Таким чином OSINT у бізнесі балансує між імперативом оперативності та правом людини на приватність, формуючи нові етичні й правові стандарти галузі.

Джерела

1. International Organization for Standardization. *Threat intelligence and why it matters for cybersecurity* [Електронний ресурс]. URL: https://www.iso.org/information-security/threat-intelligence
2. NATO. *NATO Open Source Intelligence Handbook*. Brussels : NATO, 2002. 129 с. URL: https://github.com/lawsecnet/OPSEC/blob/master/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf
3. *Gupta V.* OSINT for Corporate Security [Електронний ресурс]. *LinkedIn*. 2024. URL: https://www.linkedin.com/pulse/osint-corporate-security-vijay-gupta--rg9cc
4. Закон України "Про інформацію" від 02.10.1992 р. № 2657-XII (ред. 01.07.2025). URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text
5. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2). *Official Journal of the European Union*. 27.12.2022. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2557

В. В. РОВНИЙ

канд. юрид. наук, доцент кафедри національної безпеки ПрАТ "ВНЗ "МАУП"
victor.rovnuy.ta@gmail.com
ORCID ID: https://orcid.org/0000-0001-8716-5358

ПРАВОВЕ РЕГУЛЮВАННЯ ДЕРЖАВНОЇ ПОЛІТИКИ У ГАЛУЗІ ОСВІТИ, ЯК ІНСТРУМЕНТУ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Сучасна парадигма національної безпеки дедалі активніше інкорпорує поняття "освітня стійкість" як базис соціальної згуртованості й довгострокової конкурентоспроможності держави, адже саме через систему освіти формуються когнітивні та професійні компетентності громадян, які визначатимуть економічний потенціал, обороноздатність і політичну стабільність країни в горизонті двох-трьох десятиліть; відповідно, на рівні стратегічного планування освіта трансформується з "соціального сервісу" на критичний елемент безпекової архітектури, що потребує інтегрованих бюджетних, регуляторних і міжвідомчих механізмів управління, зокрема обов'язкових планів безперервності навчання, цифрової транспарентності фінансування й захищених каналів комунікації між учасниками освітнього процесу. Законодавче закріплення такої ролі освіти здійснене через Стратегію національної безпеки 2020 р.