**ЦЮПРИК Н. О.,**
кандидат юридичних наук,
доцент кафедри адміністративно-правових дисциплін
*(Національна академія внутрішніх справ)*
orcid.org/ 0009-0005-5542-1026

**УДК 004.056.5:17:341.231.14:341.645.5:351.74**
**DOI https://doi.org/10.32842/2078-3736/2025.5.2.48**

# ЕТИЧНІ ТА ПРАВОВІ ВИКЛИКИ ЗАСТОСУВАННЯ OSINT: ЗАРУБІЖНИЙ ДОСВІД У КОНТЕКСТІ ЄВРОПЕЙСЬКИХ СТАНДАРТІВ

У статті аналізуються ключові питання, пов'язані з використанням відкритих джерел інформації (OSINT) у сучасних умовах глобалізації та цифровізації. Окрему увагу приділено правовим, етичним та безпековим аспектам використання OSINT у демократичних суспільствах, зокрема щодо захисту приватності осіб та обмеження державного спостереження. У статті розглядається роль OSINT у національній безпеці, зокрема для державних установ, правоохоронних органів та організацій, що займаються кібербезпекою. Особливий акцент зроблено на дослідженні правових рамок, що визначають дозволені межі збору та використання відкритої інформації, а також на етичних питаннях, що виникають у контексті цифрового нагляду.

У статті також акцентується на міжнародних стандартах та судових практиках, зокрема рішень Європейського суду з прав людини, які стосуються балансу між державним наглядом і правами на приватність. У роботі висвітлено важливість забезпечення прозорості і підзвітності у використанні OSINT, а також необхідність дотримання етичних принципів у процесі збору та аналізу інформації з відкритих джерел. Автор акцентує увагу на розвитку технологій, що дозволяють удосконалювати методи збору даних, а також на викликах, які виникають у зв'язку з використанням новітніх інструментів для автоматизованого моніторингу інформації в інтернеті.

Особлива увага приділяється впливу відкритих джерел на права людини, зокрема на приватність та свободу вираження думок. У статті аналізується, як зміни у правовому полі та етичні стандарти можуть забезпечити захист інтересів громадян у процесі застосування OSINT, зберігаючи баланс між безпекою і правами людини. Таким чином, наукова робота надає цілісне уявлення про актуальні проблеми та тенденції у сфері використання відкритих джерел інформації, пропонуючи рішення для збереження демократичних цінностей в умовах цифрових трансформацій.

***Ключові слова:*** *розвідка з відкритих джерел, приватність, безпека, етичні питання розслідування, правові рамки цифрової безпеки, демократичні цінності, цифрова трансформація.*

**Tsiupryk N. O. Ethical and legal challenges of OSINT application: foreign experience in the context of european standards**

The article analyzes key issues related to the use of open-source intelligence (OSINT) in the context of globalization and digitalization. Particular attention is given to the legal, ethical, and security aspects of OSINT use in democratic societies, especially regarding the protection of individual privacy and the limits of state

surveillance. The article examines the role of OSINT in national security, focusing on its use by government agencies, law enforcement agencies, and cybersecurity organisations. Special emphasis is placed on the legal frameworks that define the permissible boundaries for collecting and using open-source information, as well as the ethical concerns that arise in the context of digital surveillance.

The article also focuses on international standards and judicial practices, in particular the decisions of the European Court of Human Rights, which concern the balance between state surveillance and privacy rights. The work highlights the importance of ensuring transparency and accountability in the use of OSINT, as well as the need to adhere to ethical principles in the collection and analysis of open-source data. The author stresses the role of emerging technologies that enhance data collection methods and the challenges that arise with the use of new tools for automated online monitoring.

Special attention is given to the impact of open-source intelligence on human rights, particularly privacy and freedom of expression. The article examines how changes in legal frameworks and ethical standards can ensure the protection of citizens' interests in the use of OSINT, maintaining a balance between security and human rights. Thus, the research paper provides a comprehensive overview of current issues and trends in the field of open-source intelligence, offering solutions for preserving democratic values amid digital transformations.

***Key words:*** *open source intelligence, privacy, security, ethical issues in investigation, legal frameworks of digital security, democratic values, digital transformation.*

**Постановка проблеми.** Стрімка цифровізація суспільства докорінно трансформувала як характер загроз безпеці, так і інструменти, що використовуються державами для їхнього виявлення та нейтралізації. Тероризм, транснаціональна організована злочинність, гібридні інформаційні операції та кіберзлочини дедалі частіше формуються й реалізуються в онлайн-середовищі, що зумовлює зростання ролі розвідки з відкритих джерел (Open Source Intelligence (OSINT)) у діяльності правоохоронних і безпекових інституцій. Використання публічно доступних цифрових даних – *соціальних мереж, форумів, відкритих баз даних, медіаресурсів* – позиціонується як ефективний, відносно ненасильницький та превентивний інструмент забезпечення безпеки.

Водночас експансія OSINT у практику державного управління актуалізує фундаментальну проблему демократичних суспільств: яким чином поєднати потребу в ефективному цифровому контролі з дотриманням прав людини, зокрема права на приватність, свободу вираження поглядів і захист персональних даних. На відміну від традиційних форм спостереження, OSINT не має чітко окреслених фізичних меж, є малопомітною для громадськості та часто спирається на алгоритмічні рішення, принципи функціонування яких залишаються непрозорими. Це створює ризик поступової нормалізації прихованого нагляду та підриву суспільної довіри до державних інституцій.

Проблематика ускладнюється фрагментарністю та застарілістю нормативно-правових рамок, які в багатьох країнах не були спроєктовані з урахуванням специфіки інтернет-середовища та масового аналізу даних. У результаті OSINT-практики часто функціонують у зоні правової невизначеності, де межі між законним збором інформації та надмірним втручанням у приватне життя залишаються розмитими. Це, своєю чергою, підживлює протилежні публічні наративи – від беззастережної підтримки жорстких безпекових заходів до звинувачень у масовому стеженні та зловживанні владою.

У такому контексті особливого значення набуває аналіз досвіду демократичних держав із розвиненими механізмами контролю за діяльністю силових органів, що дозволяє адаптувати найкращі практики до національного контексту, не втрачаючи при цьому зв’язку з фундаментальними принципами правової держави. Осмислення такого підходу є критично

важливим з огляду на необхідність формування легітимної, етично обґрунтованої та сумісної з європейськими стандартами системи цифрової безпеки.

Разом з тим, аналіз сучасної літератури з теми OSINT показує різноманітні погляди на це питання. Ключові роботи зосереджуються на питаннях безпеки, приватності, а також етичних і правових межах використання технологій збору та аналізу даних. Зокрема, дослідження, пов'язані з використанням відкритих джерел, часто торкаються проблеми забезпечення балансу між безпекою та свободою особистості й висвітлюють етичні й правові дилеми, що є важливими у створенні прозорих і зрозумілих нормативних рамок для регулювання використання OSINT. Крім того, дослідження наголошують на необхідності чіткої комунікації між державними органами і громадськістю щодо мети й методів збору інформації.

Зважаючи на швидкий розвиток технологій і зростаючі загрози безпеці, підхід до дослідження OSINT не може обмежуватись лише теоретичними роздумами, тому важливим є також вивчення численних аналітичних звітів міжнародних організацій, таких як Amnesty International, які критично оцінюють використання таких технологій для моніторингу та стеження.

**Виклад основного матеріалу дослідження.** Після терактів 11 вересня більша частина західного демократичного світу дедалі більше намагається знайти баланс між традиційними ліберальними цінностями та сучасними проблемами безпеки [1]. У світлі міжнародних терористичних атак, кількість яких зросла в п’ять разів з 2000 року [2], а також атак у Брюсселі, Парижі та Тунісі, з’явилися повідомлення, що уряди дедалі частіше підштовхують технології спостереження та розслідування до нових прецедентів [3]. Хоча уряд захищає таку політику сек’юритизації як необхідну, вона все частіше зустрічається з критикою як з боку опозиційних партій, так і з боку громадськості, політичних активістів навіть неурядових організацій, таких як «Міжнародна амністія» (Amnesty International). Хоча таке занепокоєння викликане насамперед тероризмом, додаткову критику викликала нещодавня невизначеність потенційного внутрішнього екстремізму та серйозні кримінальні прояви [4], які потрапляють під нагляд. Часто ЗМІ та групи активістів називають такі підходи загальною «масовою істерією» щодо недоречного та невиправданого профілювання [5].

Загалом, можливим є виділення трьох критичних наративів, які впливають на громадську, політичну та поліцейську сферу OSINT епохи Інтернету:

відсутність ясності в суспільстві щодо теми OSINT;

протилежні наративи та контрдиктаторські аргументи, висунуті проти легітимності та пропорційності;

розглядається інформація та твердження з незалежних і загальнодоступних оглядів, що стосуються практики OSINT.

Випадок Великої Британії заслуговує на увагу широкої аудиторії. Трагічна тенденція до зростання кількості терористичних атак і жертв, а також постійні руйнування, переміщення і дезорганізація в різних частинах Близького Сходу призвели до того, що багато країн ЄС стали перед необхідністю посилення безпеки і спостереження, зокрема, для боротьби з тероризмом, імміграцією та організованою злочинністю. Таким чином, будучи однією з найбільш географічно безпечних і ретельно контрольованих країн Європи [6], Велика Британія є чудовим прикладом для наслідування, оскільки широка європейська аудиторія може наслідувати її приклад, якщо тенденції продовжуватимуться надалі. Дійсно, щодо насильницької радикалізації такі країни, як Іспанія, Франція, Бельгія і Німеччина, посилили заходи безпеки і спостереження [7]. Водночас, навіть тимчасове посилення безпеки може викликати значний суспільний резонанс, тому врахування наслідків британського OSINT і спостереження є важливою умовою для забезпечення стійкості і безперервності діяльності.

У публічному дискурсі OSINT нерідко асоціюється з масовим стеженням, що посилюється прикладами з міжнародної практики. Це створює ризик ототожнення OSINT із порушенням приватності, навіть коли йдеться про законні та етично обґрунтовані розслідування. Водночас, недостатня комунікація з боку державних інституцій щодо цілей,

методів і обмежень OSINT лише поглиблює розрив між фаховою практикою і громадським сприйняттям.

З огляду на постійні дебати про безпеку і свободу між політичними групами, а також представниками громадськості та чинним урядом, можна припустити, що відносно сучасна інтеграція інтернет-можливостей OSINT для спостереження і розслідування значно перебільшена (наприклад, витоки Сноудена, які більше стосуються секретних служб) або неправильно зрозуміла з точки зору фактичної практики і правових рамок, в яких вони діють [8]. Наприклад, одна з таких варіацій програмного забезпечення OSINT, що використовується різними правоохоронними органами, «COSAIN», є значною мірою секретною філією Capita [9], яку купила компанія «Barrachd Ltd», компанія з розробки рішень для великих даних, що базується в Единбурзі, Великобританія. COSAIN має дуже обмежену інформацію у відкритому доступі [10], не має офіційного веб-сайту і не може бути розміщена в домені веб-сайту Barrachd Ltd. Хоча це не означає, що інформація обов'язково є суперечливою, недостатня прозорість може підірвати відносини між поліцією та громадськістю, посилити підозри, недовіру та поширення дезінформації.

Аналогічний аргумент можна навести щодо таких сервісів, як RepKnight, ще одного розвідувального рішення, яке використовують «урядові, правоохоронні, оборонні та безпекові органи в усьому світі» [11]. Незважаючи на наявність публічного веб-сайту і навіть сторінки у Facebook, існує дуже мало інформації про те, як працює цей сервіс, незважаючи на опис його здатності аналізувати мільйони повідомлень щохвилини, виявляти злочини і викривати тих, хто за ними стоїть. RepKnight стверджує, що робить це за допомогою аналізу «найширшого спектру відкритих цифрових джерел, соціальних мереж і dark web джерел» [11]. Зокрема, занепокоєння громадськості може викликати відсутність ясності щодо здатності рішення «збирати мільйони повідомлень щохвилини» без належного пояснення. Можна припустити, що мається на увазі обробка повідомлень відкритого формату, таких як публічні твіти або оновлення статусів Facebook з відкритих профілів. Однак можна також припустити, що йдеться про обробку приватних повідомлень і контенту, доступ до якого обмежений налаштуваннями приватності акаунтів у соціальних мережах. Такі припущення не можна вважати повністю ірраціональними, особливо після звинувачень на адресу британського уряду та Служби зовнішньої розвідки у зв'язку з проектами «Призма» і «Темпора» [12].

Крім того, існує явна нестача опублікованої літератури та знань законодавства цього питання, особливо у вільному доступі для громадськості. Сучасна урядова, поліцейська та юридична література часто є найбільш доступною через «багатосторінкові та термінологічно насичені» звіти та документи, такі як Закон про регулювання слідчих повноважень 2000 року [13] (Regulation of Investigatory Powers Act - RIPA), Закон про захист свободи 2012 року (Protection of Freedom Act) та поточні огляди ОБСЄ [14]. Звичайно, важливо зазначити, що такі закони, як RIPA, були написані до появи OSINT в Інтернеті і не призначені для нього. Міністерство внутрішніх справ опублікувало лише рекомендації щодо керівництва з розслідування OSINT, а не цілісну законодавчо затверджену структуру [15]. Крім того, поліцейське відомство не поспішає завантажувати інформацію у своєму розділі веб-сайту, присвяченому OSINT [16]. Така непрозорість щодо простоти доступу громадськості до інформації може посилити комплекс «старшого брата», що продовжує існувати. Останній момент, на який слід звернути увагу, стосується навмисної дезінформації, що використовується в антиполіцейських та антиурядових наративах.

Наразі видається, що використання OSINT в Інтернеті, особливо щодо аналізу великих обсягів даних, в основному використовується для збору розвідувальної інформації та розслідувань, а не для загальної роботи поліції з громадою. Зазначається, що загалом більшість поліцейських сил і практиків OSINT використовували «соціальні медіа ... для інформування про такі стратегії, як превентивні арешти, перехоплення діяльності, наближення до конкретних осіб і груп або зміна тактики під час подій ... ще не є частиною поліцейської практики і викликає занепокоєння в поліції щодо рівня дублювання між розвідкою взаємодією» [17].

Як і в багатьох інших аспектах поліцейської діяльності, охорони правопорядку та інших відповідних практик безпеки, рівень взаємодії соціальними мережами значно відрізняється в різних поліцейських підрозділах, причому більшість з них в основному використовують їх для взаємодії з громадою щодо спеціальних повідомлень, таких як оголошення для громадськості та повідомлення про дрібні злочини. Це саме по собі може викликати занепокоєння у представників громадськості, які можуть вважати, що моніторинг OSINT може бути «двостороннім дзеркалом», коли фахівці з розвідки можуть спостерігати і проводити розслідування з мінімальним залученням і взаємодією з громадськістю.

Звичайно, важливо розуміти і поважати той факт, що багато елементів OSINT-розслідувань є корисними і не повинні розкривати повну природу використовуваних тактик і рішень. Громадськості слід все більше роз'яснювати, що жорсткі правила і норми виправдовують і санкціонують розгортання, а також, що громадська безпека може виграти від нерозголошення і мінімізації розкриття інформації про взаємодію, що може допомогти відстежити загрози суспільству, захистити вразливі місця і забезпечити максимальний порядок. Також може бути корисним запевнити громадськість, що поліція та інші сертифіковані OSINT-спеціалісти повинні дотримуватися набагато суворіших стандартів, ніж більшість приватних корпорацій і підприємств, які використовують аналітику великих даних і збирають, зберігають і співставляють персональні дані. Для комп'ютерно грамотних поколінь втрата організаціями і корпораціями контролю і права власності на персональні дані не є революційним або особливо страшним відкриттям; однак може виявитися корисним запевнити колектив, що OSINT має дотримуватися набагато суворіших протоколів, ніж такі агентства, як Google, Facebook, Microsoft і Amazon [18].

Застосування OSINT у цифровому середовищі дедалі більше перетинається з етикою, правом і політикою, породжуючи суперечливі наративи щодо його легітимності та меж допустимого втручання. З одного боку, аналітика великих даних і моніторинг соціальних мереж стали незамінними інструментами для виявлення загроз, розслідування злочинів і захисту національної безпеки. З іншого, саме ці технології викликають занепокоєння щодо приватності, підзвітності та впливу комерційних інтересів на державну безпеку.

Напруження між правом на недоторканність приватного життя і потребою ефективному цифровому контролі стало точкою зіткнення державних інституцій, технологічних корпорацій і громадянського суспільства. Конфлікти, подібні до справи Apple/ФБР, демонструють, наскільки глибокими можуть бути розбіжності у трактуванні прав, обов'язків і меж цифрового втручання. У таких умовах OSINT-практики змушені діяти в зоні постійного балансу – між законністю і довірою, між ефективністю і прозорістю, між безпекою і свободою.

Використання рішень на основі великих даних та аналізу соціальних мереж, безсумнівно, відіграє важливу роль у сучасних OSINT-розслідуваннях і спостереженні в Інтернеті. Однак ця практика діє як палиця з двома кінцями в руках протилежних наративів. Зокрема, такі питання, як підзвітність, розслідування великих обсягів даних та збереження інформації, є основними причинами публічних дебатів. Крім того, виникають відносно нові питання щодо етичної, правової та соціальної придатності ринково орієнтованих програмних продуктів для авторитетної практики OSINT.

Існує критика, особливо з боку захисників приватності [19] і критиків стеження [20], щодо відносин між державою, правоохоронними органами і службами безпеки, а також приватними компаніями і організаціями [21]. Останніми роками терористи, злочинці та підозрювані все частіше використовують складні технології, такі як «темна мережа» і послуги шифрування, для збереження анонімності. Зокрема, зростання послуг шифрування, які за замовчуванням пропонують такі компанії, як Apple, і програмні сервіси, такі як WhatsApp, створили бар'єр для виконання урядових і правоохоронних обов'язків. Стрілянина в Сан-Бернардіно в грудні 2015 року, здійснена подружжям ісламських екстремістів, перетворилася національної трагедії на складну міжнародну битву між ФБР і світовим технологічним гігантом Apple [22]. Юридична ескалація між двома воюючими сторонами сталася через

відмову Apple розблокувати зашифрований iPhone, який був вилучений у одного з нападників. Ця справа, ймовірно, розділила громадську та приватну думку, причому кожна зі сторін викликала значну реакцію уряду та правоохоронних органів. З одного боку, прихильники стеження стверджували, що «держава втратила контроль», а демократичний капіталізм, представлений легітимністю та авторитетом вищого керівництва держави, підривається технологічною індустрією [23]. З іншого боку, захисники приватності стверджували, що право на недоторканність приватного життя є першорядним, а підпорядкування ФБР дозволить виявити слабкі місця і вразливості в усіх продуктах Apple, які в подальшому можуть бути використані в недоброчесних цілях.

Ці два моменти, хоча і не пов'язані з конкретними випадками з відкритих джерел, тим не менш, є важливим сучасним нагадуванням про розбіжності в думках, які в будь-якому випадку будуть кидати виклик сучасним можливостям OSINT. Ця ситуація, звичайно, погіршується дезінформацією, яка часто порівнює повноваження та інтереси національної безпеки з повсякденними OSINT-операціями. Незважаючи на це, обидві думки висвітлюють складну серединну лінію, якою повинні йти фахівці-практики; залежність від соціальних мереж, великих даних та інших комерційних сервісів їх залучення відкриває їм можливість для спекуляцій щодо етичних і законних міркувань використання комерційних сервісів до такої міри, що вони можуть ефективно підірвати легітимний авторитет державної влади. Тому може знадобитися переконати зовнішню громадськість у тому, що OSINT є цінним активом, який може співіснувати з сучасними технологічними організаціями для надання цінної інформації в інтересах соціальної стійкості та безпеки суспільства.

На додаток до таких аргументів, проти проактивного спостереження та моніторингу виступають кампанії таких критично налаштованих організацій, як Amnesty International, Bytes for All, Liberty and Privacy International. Зокрема, постійне збільшення використання поліцією проактивного спостереження, починаючи з (не дуже суперечливих) камер розпізнавання номерних знаків закінчуючи (більш суперечливими) камерами розпізнавання обличь, встановленими на центральних вулицях, наштовхнулося на рівновагу повільно зростаючого протесту. Зростаюче занепокоєння з приводу розслідувань і спостереження за допомогою розвідки з відкритих джерел, на відміну від фізичної присутності камер, систем безпеки в аеропортах, поліцейських машин на автострадах – немає фізичного усвідомлення розгортання OSINT. Тому проактивне використання OSINT в Інтернеті, ймовірно, зіткнеться з ще більшим спротивом з боку опозиції, а підстави для цього повинні бути прозорими, пропорційними і виправданими для більшості, щоб мінімізувати негативний вплив.

Громадськість слід запевнити в тому, що чинне законодавство допомагає обмежити зловживання фахівцями-практиками наявними технологіями і владними повноваженнями. Крім того, важливо, щоб фахівці розуміли, були в курсі та реагували на зовнішні скарги і помилкові уявлення.

Незалежні огляди відіграють критичну роль у формуванні довіри до практик OSINT, забезпечуючи зовнішній контроль, об'єктивну оцінку і публічну прозорість. У контексті стрімкого розвитку цифрових технологій і зростання повноважень державних органів, саме такі звіти дозволяють виявити прогалини законодавстві, застарілі норми та ризики зловживань. Відсутність оновлених оглядів, особливо після резонансних подій з міжнародної практики, породжує занепокоєння щодо того, наскільки чинні правові механізми відповідають реаліям сучасного інтернет-середовища.

Таким чином, третій важливий наратив, про який OSINT-практики повинні бути активно обізнані, - це регулярні звіти, що публікуються незалежними органами [24]. Варто зазначити, що, незважаючи на давність звіту, з огляду на останні технологічні розробки, урядові закони (про заборону наскрізного шифрування) і справу ФБР проти Apple в Сан-Бернардіно, більш свіжий огляд не був опублікований. Це може викликати занепокоєння у представників громадськості або членів груп, які борються за свободу та анонімність в Інтернеті, оскільки уряди, на думку деяких, використовують лазівки в застарілій юридичній термінології та законодавстві для виправдовування; це особливо актуально, коли такі закони, як

RIPA, потрапляють під вогонь критики за те, що вони є застарілими, не відповідають сучасному Інтернету та використовуються офшорними компаніями, які мають лазівки для урядового стеження.

Це особливо стосується фрази зі звіту: «Ми живемо в епоху безпрецедентної уваги до використання таємних тактик державними органами, а також до того, як вони санкціоновані і як ними керують. ОБСЄ відіграє і продовжуватиме відігравати ключову роль у постійному нагляді за цими питаннями від імені парламенту, уряду та громадськості. … залишаються деякі невеликі, але важливі прогалини в нагляді» [24]. Такі загальнодоступні коментарі з неупередженої оцінки є надзвичайно важливими для забезпечення максимального рівня достовірності та прозорості. Однак, враховуючи подібні коментарі, зафіксовані в попередніх оглядах, фахівці-практики повинні усвідомлювати, наскільки легко такі матеріали високого рівня можуть бути навмисно або помилково неправильно витлумачені; «багато коментаторів у засобах масової інформації неточно описують ступінь і мету використання цих повноважень» [24]. Тому важливо переконатися, що загальнодоступна інформація про використання OSINT може бути корисно включити у скорочену чи спрощену версію, яку можна просувати і поширювати.

Крім того, у звіті детально описано, як багато місцевих органів влади намагалися використовувати OSINT. У кількох випадках доступ до сторінок соціальних мереж «був наданий ... з метою проведення розслідувань без будь-якого корпоративного керівництва, нагляду або регулювання» [24]. Особливо важливим є поширена думка про те, що законодавчі акти, приділяють занадто багато уваги фактичним практикам OSINT, а не кращій освіті суддів та інших працівників судової системи. Як наслідок, часто OSINT та супутні операції з нагляду і розслідування, що проводяться поліцією, не завжди отримують належний дозвіл, коли це необхідно. Це ще раз підкреслює той важливий момент, що сучасна OSINT практика рідко функціонує як окремий компонент, а є допоміжним інструментом для більш широкої системи збору розвідувальної інформації. Ці ширші рамки взаємопов'язані і взаємозалежні з широким спектром факторів: від ієрархічного і юридичного дозволу до етичних і політичних міркувань, аж до більш опосередкованих векторів, таких як потенційна реакція громадськості і створення хибних уявлень у ЗМІ.

**Висновок.** Таким чином, розвідка з відкритих джерел є важливим інструментом для забезпечення безпеки в умовах цифрової трансформації суспільства. Вона дає змогу ефективно моніторити та виявляти загрози, такі як тероризм, кіберзлочини, організовану злочинність та гібридні інформаційні операції. Однак, незважаючи на її безумовні переваги у сфері безпеки, застосування OSINT ставить перед державними органами важливі етичні та правові виклики, які потребують ретельного врегулювання. Зростаюча роль цифрових технологій у житті сучасного суспільства породжує ризики порушення приватності, а також створює потенціал для зловживань, що викликає обґрунтоване занепокоєння громадськості.

Однією з головних проблем є необхідність досягнення балансу між забезпеченням національної безпеки і дотриманням прав людини, зокрема права на приватність. Використання публічно доступних даних для аналізу ситуацій та ухвалення рішень часто не супроводжується достатньою прозорістю та підзвітністю, що підриває довіру громадськості до державних органів. Таке становище є особливо критичним у демократичних державах, де принципи відкритості та підзвітності є основою легітимності влади.

Іншою важливою проблемою є відсутність відповідних правових норм для регулювання практик OSINT, що часто функціонують у правовій «сірій зоні». Це створює неоднозначність у питаннях законності збору та використання інформації, а також меж втручання у приватне життя громадян. Як показує досвід Великої Британії, де вже давно ведуться дискусії про доцільність і етичні межі застосування OSINT, необхідно ретельно формулювати законодавчі рамки, які регулюють використання таких технологій. Водночас важливо забезпечити ефективний громадський контроль за діяльністю державних органів та правоохоронних структур, що здійснюють розслідування на основі відкритих джерел.

Для України дослідження міжнародного досвіду в контексті застосування OSINT є надзвичайно важливим. Адаптація європейських стандартів цифрової безпеки та правового регулювання є необхідною для створення ефективної та легітимної системи цифрового нагляду, що відповідатиме вимогам захисту прав людини та демократичних цінностей. Важливо, щоб ці технології служили не тільки інтересам безпеки, але й підтримували довіру громадян до державних інституцій через прозорість, підзвітність та чітке дотримання етичних норм.

**Список використаних джерел:**

1. Moss, K. (2011). Balancing liberty and security: Human rights, human wrongs. Springer.
2. Institute for Economics and Peace. (2014). Global Terrorism Index 2014: Measuring and understanding the impact of terrorism.
3. Elworthy, S. (2015). Beyond deterrence: Rethinking UK Security Doctrine. Oxford Research Group. Retrieved July 20, 2016, from http://www.oxfordresearchgroup.org.uk/publications/briefing_papers_and_reports/beyond_deterrence_rethinking_uk_security_doctrine
4. Jones, J. (2015, December 1). The day I found out I'm a 'Domestic Extremist'. The Telegraph. Retrieved from http://www.telegraph.co.uk/news/uknews/terrorism-in-theuk/11357175/The-day-I-found-out-Im-a-Domestic-Extremist.html
5. Evans, R., & Bowcott, O. (2014, June 15). Green Party peer put on database of 'extremists' after police surveillance. The Guardian. Retrieved from http://www.theguardian.com/politics/2014/jun/15/green-party-peer-put-on-database-of-extremists-by-police
6. Barrett, D. (2013, July 9). One surveillance camera for every 11 people in Britain, says CCTV survey. The Telegraph. Retrieved from http://www.telegraph.co.uk/technology/10172298/One-surveillance-camera-for-every-11-people-in-Britain-says-CCTV-survey.html
7. Ryan, M. (2016, March 26). Brussels attacks rekindle privacy vs. security debate in Europe. Washington Post. Retrieved from https://www.washingtonpost.com/world/europe/brusselsattacks-rekindle-privacy-vs-security-debate-in-europe/2016/03/26/60a68558-f2dc-11e5-a2a3-d4e9697917d1_story.html
8. Carey, H. P. (2015). Managing 'Threats': Uses of social media for policing domestic extremism and disorder in the UK.
9. Cameron, G. (2015, March 11). Capita buys Scottish analytics firm Barrachd. Herald Scotland. Retrieved from http://www.heraldscotland.com/business/13416378.Capita_buys_Scottish_analytics_firm_Barrachd/
10. Cosain, E. (2015). Barrachd Edinburgh, UK. Retrieved from http://assets-production.govstore.service.gov.uk/G4/Barrachd-0879/523c2390354067df0ce14172/QD5/13_0125_BAR_Cosain_A4_flyer.pdf
11. RepKnight. (n.d.). Retrieved from https://www.facebook.com/RepKnight/info?tab=page_info
12. Pitt-Payne, T. (2013). PRISM and TEMPORA: ECtHR proceedings issues against UK.
13. Best, R. A., & Cumming, A. (2007). Open source intelligence (OSINT): Issues for congress (Vol. 5). December 2007.
14. Carey, H. P. (2015). Managing 'Threats': Uses of social media for policing domestic extremism and disorder in the UK.
15. Home Office. (2012, April). Open source software options for government: Version 2.0. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/78964/Open_Source_Options_v2_0.pdf
16. College of Policing. (2016). Intelligence and counter terrorism. Retrieved from http://www.college.police.uk/What-wedo/Learning/Curriculum/Intelligence/Pages/default.aspx
17. Carey, H. P. (2015). Managing 'Threats': Uses of social media for policing domestic extremism and disorder in the UK.
18. Compare Business Products. (2010). Top 10 Big Brother companies: Ranking the worst consumer privacy infringers. Retrieved from http://www.comparebusinessproducts.com/fyi/top-10-big-brother-companies-privacy-infringement

19. Schulz, G. W. (2012, April 27). Private companies pitch Web surveillance tools to police. Reveal Online. Retrieved from https://www.revealnews.org/article/private-companies-pitch-web-surveillance-tools-to-police/

20. Crushing, T. (2014, March 26). Police utilizing private companies, exploits to access data from suspects' smartphones. Wireless. Retrieved from https://www.techdirt.com/blog/wireless/articles/20140326/

21. Wallis Simons, J. (2012, May 22). Who watches the private detectives? The Telegraph. Retrieved from http://www.telegraph.co.uk/culture/tvandradio/9344659/Who-watches-the-private-detectives.html

22. Yadron, D. (2016, April 27). FBI confirms it won't tell Apple how it hacked San Bernardino shooter's iPhone. The Guardian. Retrieved from https://www.theguardian.com/technology/2016/apr/27/fbi-apple-iphone-secret-hack-san-bernardino

23. Morozov, E. (2016). The state has lost control: Tech firms now run western politics.

24. Rose, C. (2015). Annual Report of the Chief Surveillance Commissioner. House of Commons Print. Presented to the Scottish Parliament, June 2015. Retrieved from https://osc.independent.gov.uk/wp-content/uploads/2015/06/OSC-Annual-Report-2014-15-web-accessible-version.pdf

Дата першого надходження рукопису до видання: 27.09.2025
Дата прийнятого до друку рукопису після рецензування: 29.10.2025
Дата публікації: 28.11.2025