УДК / UDC: 343.1:004
DOI: https://doi.org/10.37750/2616-6798.2026.2(57).364226

Михайло Васильович Гуцалюк
Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю при РНБО України. Київ, Україна
ORCID: https://orcid.org/0000-0003-4496-5173
Анатолій Іванович Марущак
ГО "Міжнародна академія інформації"
ORCID https://orcid.org/0000-0003-0069-3727

ДОСТУП ПРАВООХОРОННИХ ОРГАНІВ ДО ДЕРЖАВНИХ І ПРИВАТНИХ РЕЄСТРІВ: ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ В УКРАЇНІ

Анотація. *У статті досліджено правові, організаційні та технічні аспекти доступу правоохоронних органів до державних і приватних інформаційних систем в Україні. Визначено ключові проблеми, зокрема фрагментарність правового регулювання, відсутність інтегрованих систем обміну даними, процесуальні обмеження та технічні бар'єри. Проаналізовано європейський досвід забезпечення доступу до інформації в кримінальних провадженнях. Запропоновано напрями вдосконалення законодавства та практики, спрямовані на підвищення ефективності розслідувань і забезпечення балансу між потребами кримінальної юстиції та захистом прав людини.*

Ключові слова: *електронні докази, державні реєстри, доступ до інформації, кіберзлочинність, кримінальне провадження, персональні дані.*

Mykhaylo V. Gutsalyuk
Interagency Research Center for Combating Organized Crime under the National Security and Defense Council of Ukraine. Kyiv, Ukraine
ORCID: https://orcid.org/0000-0003-4496-5173
Anatolii I. Marushchak
NGO "International Academy of Information"
ORCID https://orcid.org/0000-0003-0069-3727

ACCESS OF LAW ENFORCEMENT AUTHORITIES TO STATE AND PRIVATE REGISTERS: PROBLEMS AND PROSPECTS FOR DEVELOPMENT IN UKRAINE

Summary. *The article examines legal, organizational, and technical aspects of law enforcement access to public and private information systems in Ukraine. Key challenges are identified, including fragmented regulation, lack of integrated data exchange systems, procedural constraints, and technical limitations. The study analyzes European practices of data access in criminal proceedings. It proposes directions for improving legislation and practice to enhance investigative efficiency while ensuring a balance between criminal justice needs and human rights protection.*

Keywords: *electronic evidence, public registers, data access, cybercrime, criminal proceedings, personal data.*

Постановка проблеми. Глобальна цифровізація державного управління та економіки докорінно змінила архітектуру суспільних відносин, що, своєю чергою, спричинило якісну трансформацію механізмів вчинення та протидії організованій злочинності. Сучасні кримінальні правопорушення, особливо у сферах високотехнологічних фінансових операцій, транснаціональної кіберзлочинності, легалізації доходів, одержаних злочинним шляхом, торгівлі людьми та контрабанди, характеризуються високим рівнем латентності та активним використанням складних інформаційно-телекомунікаційних систем.

Цифровізація публічного управління зумовила об'єктивну необхідність модернізації оперативної та слідчої діяльності. Згідно з *Комплексним стратегічним планом реформування органів правопорядку як частини сектору безпеки і оборони України на 2023-2027 роки*, одним із пріоритетних векторів розвитку є здійснення консолідованої цифрової трансформації на основі інструментів стратегічного менеджменту, що відповідають найкращим практикам ЄС [1]. Це свідчить про перехід від точкових технологічних рішень до системної перебудови правоохоронної архітектури.

Якщо класична модель оперативно-розшукової діяльності (ОРД) була орієнтована переважно на фізичний простір та матеріальні носії інформації, то сучасний етап розвитку характеризується домінуванням цифрового середовища як основного простору підготовки та маскування злочинів. У цифрову епоху об'єктом прискіпливої уваги правоохоронних органів стають: електронні комунікації (месенджери, хмарні сховища), цифрові транзакції (криптовалюти, fintech-платформи), метадані та цифрові сліди в розгалужених системах.

Відповідно, ефективність протидії організованій злочинності сьогодні прямо корелює зі здатністю суб'єктів кримінальної юстиції своєчасно отримувати та аналізувати масиви комп'ютерних даних. Особливе місце в цьому процесі посідає доступ до державних та приватних реєстрів у цифровому форматі. Інтеграція автоматизованих інформаційних систем перетворює традиційну оперативну діяльність на превентивно-аналітичну. Можливість автоматизованого аналізу даних дозволяє правоохоронцям виявляти приховані зв'язки між учасниками злочинних угруповань та ідентифікувати реальних бенефіціарів [2].

Проте, правозастосовна практика в Україні стикається з низкою критичних викликів: нормативною фрагментарністю, технологічною асиметрією реєстрів та складністю механізмів отримання даних від приватних структур. Особливої гостроти набуває проблема забезпечення балансу між інтересами слідства та правом на приватність, що випливає з практики ЄСПЛ та положень Загального регламенту про захист даних (GDPR) [3]. Крім того, законодавство ЄС щодо ШІ, в якому відображено механізми врахування і захисту прав людини від імовірного негативного впливу, також опосередковано стосується питань діяльності правоохоронних органів. В умовах євроінтеграційного курсу України питання законності та пропорційності доступу до інформаційних ресурсів набуває стратегічного значення.

Попри задекларований курс на цифрову трансформацію, сьогодні спостерігається суттєвий дисонанс між стрімким розвитком технологій, що використовуються організованою злочинністю, та інертністю процесуальних механізмів отримання доступу до цифрових даних. Центральною проблемою дослідження є недосконаліть правового та технічного інструментарію, який би дозволяв правоохоронним органам у режимі реального часу взаємодіяти з державними та приватними реєстрами без порушення фундаментальних прав людини. Існуюча процедура тимчасового доступу до

речей і документів, закріплена в КПК України, часто виявляється занадто тривалою для специфіки електронних доказів, які характеризуються високим ступенем волатильності та можуть бути знищені за лічені секунди.

Крім того, наукового вирішення потребує питання інституційної розрізненості інформаційних масивів. Відсутність єдиних стандартів інтероперабельності між відомчими реєстрами та базами даних приватних провайдерів створює "інформаційні лакуни", якими успішно користуються злочинні угруповання для маскування своїх активів. Відтак, виникає гостра необхідність у розробці науково обґрунтованої моделі доступу до даних, яка б поєднувала в собі оперативність автоматизованого обміну інформацією з жорстким судовим контролем та міжнародними стандартами кібербезпеки, що і визначає основний вектор нашого дослідження.

Результати аналізу наукових публікацій

Аналіз сучасних наукових розвідок свідчить про те, що проблема доступу правоохоронних органів до цифрових ресурсів перебуває у центрі дискусій як українських, так і зарубіжних правників. Значна частина досліджень присвячена загальнотеоретичним аспектам трансформації кримінального процесу в умовах інформаційного суспільства. Зокрема, науковці наголошують, що традиційні методи збирання доказів поступово витісняються високотехнологічними процедурами, де реєстри виступають основним джерелом первинної інформації [4].

У працях вітчизняних дослідників, зокрема В. Бєлєвцевої, О. Корнейко, С. Чернявського, М. Погорецького та інших підкреслюється, що ефективність протидії організованій злочинності сьогодні нерозривно пов'язана з використанням аналітичних систем та баз даних. Автори вказують на необхідність подолання "відомчих бар'єрів" при обміні інформацією між суб'єктами оперативно-розшукової діяльності [5]. Водночас, питання нормативного регулювання доступу до приватних інформаційних систем залишається менш дослідженим, що створює прогалини у правозастосуванні.

Міжнародний науковий дискурс зосереджений на забезпеченні балансу між публічним інтересом та приватністю. Дослідники звертають увагу на те, що масовий доступ до даних (bulk access) потребує суворого дотримання принципів пропорційності та необхідності, закріплених у практиці ЄСПЛ [6]. Окремі автори (наприклад, Л. Флоріді) розглядають інформацію в реєстрах як елемент "онтологічної безпеки" особи, що вимагає розробки нових етичних стандартів обробки даних у правоохоронній сфері [7].

Результати огляду публікацій за останні роки дозволяють констатувати, що попри значну кількість праць з питань використання електронних доказів, цифровізації правоохоронної діяльності та кібербезпеки, бракує комплексних досліджень, які б поєднували технічні аспекти інтероперабельності реєстрів із процесуальними гарантіями автентичності електронних доказів. Це підтверджує актуальність нашого дослідження щодо розробки цілісної моделі доступу до державних та приватних інформаційних ресурсів в Україні.

Метою статті є комплексний аналіз механізмів доступу правоохоронних органів до інформаційних ресурсів та визначення напрямів їх удосконалення.

Виклад основного матеріалу. Сучасна доктрина кримінального процесу перебуває на етапі фундаментальної трансформації, де цифровізація доказування розглядається як зміна самої природи фактичних даних. Теоретичним підґрунтям цього процесу є концепція "мережевого суспільства", обґрунтована М. Кастельсом, згідно з

якою інформація стає стратегічним ресурсом влади, а контроль над її потоками визначає ефективність державних інституцій [8]. У контексті кримінальної юстиції це означає, що державні та приватні реєстри перетворюються на ключові вузли доказової системи.

Методологічно реєстри слід розглядати як системоутворюючі елементи доказування. Докази у кримінальних провадженнях, на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження, сьогодні здебільшого акумулюються в цифрових реєстрах речових прав, юридичних осіб, податкових та банківських системах та інших базах даних, у тому числі і в приватних структурах. Відтак, доступ до цих масивів є базовою процесуальною дією, що забезпечує верифікацію обставин злочину.

Особливого значення цей інструментарій набуває у протидії організованій злочинності. За висновками Європолу (звіти SOCTA, IOCTA), сучасні злочинні угруповання функціонують як гнучкі мережеві структури, що активно використовують цифрові інструменти для конспірації [9]. У такому ракурсі цифрові реєстри стають механізмом деконструкції злочинної мережі. Процесуальне значення доступу полягає у забезпеченні невідворотності покарання через швидке накладення арешту на майно та запобігання виведенню активів.

Водночас методологія дослідження вимагає дотримання стандартів захисту персональних даних. Діяльність правоохоронних органів у цій сфері регулюється не лише національним законом, а й Директивою (ЄС) 2016/680 [10]. Усталена доктрина ЄСПЛ (зокрема, у справі *Gaskin v. United Kingdom*) наголошує, що будь-яке втручання у приватне життя через доступ до даних має бути пропорційним легітимній меті та супроводжуватися незалежним контролем [11].

Науковий інтерес становить трансформація функцій реєстрів: від облікових до превентивно-аналітичних. Завдяки методу перехресних перевірок (*cross-matching*), успішно реалізованому в *Schengen Information System*, реєстри дозволяють виявляти аномальні операції на ранніх стадіях [12]. Судова практика в Україні (наприклад, у справі №210/5936/23) підтверджує, що інформаційні ресурси держави фактично стають елементом цифрової превенції, дозволяючи правоохоронцям встановлювати латентні зв’язки, які неможливо виявити традиційними методами [13].

Сучасний КПК України не містить окремого терміну “електронний доказ”, проте оперує поняттям “матеріальні носії комп’ютерних даних” (жорсткі диски, флеш-накопичувачі, сервери, телефони) що містять електронну інформацію) [14]. Згідно зі статтею 99 КПК, вони прирівнюються до документів, є джерелом доказів і можуть бути вилучені чи оглянуті під час слідчих дій. Стаття 94 КПК України вимагає від слідчого та прокурора всебічного, повного й неупередженого дослідження всіх обставин провадження. У контексті цифрових даних це означає, що кожен файл, лог-запис або інформація з реєстру повинні бути оцінені з точки зору їх належності, допустимості та достовірності.

Ключовим механізмом отримання даних із державних та приватних систем є процедура тимчасового доступу до речей і документів (Глава 15 КПК). Особливу увагу слід приділити статті 161 КПК України, яка визначає перелік речей і документів, до яких заборонено доступ. Цифрові дані часто межують із документами, що містять охоронювану законом таємницю. Наприклад, листування в месенджерах або дані про транзакції можуть підпадати під категорію конфіденційної інформації, що вимагає обов’язкового отримання ухвали слідчого судді.

Важливою новелою в умовах воєнного стану стали зміни до ст. 615 КПК, які розширили повноваження прокурорів щодо надання дозволу на доступ до даних у разі

неможливості виконання слідчим суддею своїх повноважень. Проте, процесуальна легітимність таких доказів у майбутньому залежатиме від чіткої фіксації технічних параметрів отримання даних, що має забезпечувати “ланцюг збереження” (chain of custody).

Якісно новий етап регулювання доступу до інформації, яка зберігається у реєстрах розпочався із прийняттям Закону України “Про публічні електронні реєстри”. Цей акт заклав правову основу для створення єдиного екосистемного підходу до державних даних. Для правоохоронної діяльності ключовим є закріплений у Законі принцип інтероперабельності — здатності різних інформаційних систем до автоматизованого обміну даними.

Запровадження системи “Трембіта” [15] як бази для взаємодії реєстрів дозволяє відійти від застарілої моделі паперових запитів. Згідно зі статтями 25–26 зазначеного Закону, правоохоронні органи як суб’єкти інформаційної взаємодії мають отримувати дані в електронній формі, що забезпечує:

- мінімізацію часових витрат на отримання доказів;
- автентичність отриманої інформації (завдяки використанню кваліфікованого електронного підпису та логуванню запитів);
- можливість автоматизованого співставлення даних з різних джерел.

Для розслідування організованої злочинності це означає можливість миттєвого підтвердження прав власності або статусу юридичної особи, що є критичним для превентивного арешту активів.

Найбільш чутливим аспектом правового регулювання на сьогодні залишається доступ до банківських систем та персональних даних. Згідно із Законом України “Про банки і банківську діяльність” (ст. 62), інформація щодо юридичних та фізичних осіб, яка становить банківську таємницю, розкривається банками за рішенням суду. У справах про фінансову злочинність та відмивання доходів цей етап часто є “вузьким місцем” розслідування через тривалість судового розгляду.

Доступ до персональних даних регулюється Законом України “Про захист персональних даних”. Тут діє принцип цільового призначення: правоохоронці мають право на обробку даних лише в обсязі, необхідному для здійснення кримінального провадження. Особливості обробки даних у поліції мають відповідати стандартам Директиви (ЄС) 2016/680, що передбачає:

1. Розмежування даних про різні категорії осіб (підозрювані, свідки, потерпілі).
2. Встановлення чітких термінів зберігання цифрових профілів.
3. Забезпечення права особи на інформацію про обробку її даних (з урахуванням обмежень, необхідних для слідства).

Специфіка доступу до даних приватних реєстрів (наприклад, клієнтських баз телеком-операторів) вимагає балансування між комерційною таємницею, захистом приватності користувачів та потребами національної безпеки. Судова практика в Україні поступово схиляється до того, що в справах щодо тяжких та особливо тяжких злочинів, вчинених організованими групами, суспільний інтерес у розкритті злочину переважає над інтересом збереження конфіденційності даних.

Таким чином, нормативне поле України перебуває в стані активної адаптації до цифрових реалій. Поєднання процесуальних фільтрів КПК із технологічними можливостями Закону “Про публічні електронні реєстри” створює передумови для формування ефективної системи доказування. Проте, критичною залишається потреба в уніфікації процедур доступу до банківських та приватних баз даних, що забезпечило б

правоохоронним органам необхідну оперативність без порушення стандартів прав людини.

Ефективність сучасного розслідування організованої злочинності значною мірою залежить від інформації, що акумулюється у приватному секторі. Проте взаємодія з держателями цих даних характеризується різним рівнем правової та технічної складності.

Найбільш врегульованою в українському законодавстві є співпраця з телеком-операторами. Згідно із Законом України "Про електронні комунікації", оператори зобов'язані зберігати дані про з'єднання та ідентифікатори абонентів. Проте ключовою проблемою залишається доступ до змісту комунікацій у месенджерах, які використовують наскрізне шифрування (end-to-end encryption). Це створює ситуацію "цифрової темряви" (*going dark*), коли правоохоронні органи, маючи юридичне право на доступ, не мають технічної можливості дешифрувати дані без співпраці з розробниками ПЗ.

Взаємодія з фінансовими установами (банками, платіжними системами) ускладнена жорстким режимом банківської таємниці. Хоча КПК України передбачає механізм тимчасового доступу, на практиці правоохоронці стикаються з відмовами або затягуванням термінів через складні внутрішні процедури комплаєнсу банків. Особливо гостро це питання стосується транскордонних переказів та використання необанків (fintech-платформ), де юрисдикція держателя даних може бути невизначеною.

Найскладнішим аспектом є отримання даних від міжнародних технологічних платформ (Meta, Google, Apple). Така ситуація склалася через те, що основний масив цифрових слідів українських громадян зберігається на серверах у США чи країнах ЄС. Отримання цієї інформації через механізми міжнародної правової допомоги (MLA) є надзвичайно тривалим процесом, що може тривати від 6 до 18 місяців [16]. Хоча компанії мають власні портали для запитів правоохоронних органів (*Law Enforcement Portals*), вони зазвичай надають лише базову інформацію про абонента (basic subscriber information), відмовляючи у наданні змісту повідомлень без відповідних міжнародних судових доручень.

Одним із головних процесуальних бар'єрів є тривалість отримання ухвал слідчого судді на тимчасовий доступ до речей і документів. В умовах надмірного навантаження на судову систему розгляд клопотання може тривати тижнями, тоді як цифрові докази, особливо у справах про кіберзлочини, можуть бути видалені протягом кількох годин. Відсутність у КПК України дієвого механізму термінового збереження даних (data preservation), аналогічного ст. 16 Будапештської конвенції, призводить до незворотної втрати доказової бази [17].

Другою групою перешкод є технічні бар'єри, серед яких домінують:

1. Несумісність форматів даних: Кожна приватна система (банківська, телекомунікаційна чи хмарна) використовує власні стандарти структурування логів та звітів. Отримання даних у форматах PDF або сканованих копій унеможливлює їх автоматизовану обробку та проведення кримінального аналізу за допомогою спеціалізованого ПЗ.
2. Динамічна природа цифрових слідів: Використання технологій динамічних IP-адрес телеком-операторами вимагає від правоохоронців не лише знання номеру, а й точного часу з точністю до мілісекунд, що не завжди фіксується при первинному документуванні.
3. Відсутність єдиного шлюзу доступу: На відміну від державних реєстрів, де впроваджується інтероперабельність, взаємодія з приватним сектором

залишається “ручною”. Кожен запит потребує фізичного або електронного пересилання окремих документів, що збільшує ризик витоку інформації та помилок.

Також проблема доступу до приватних систем нерозривно пов’язана з етичними та правовими питаннями захисту персональних даних. Приватні компанії часто використовують аргумент захисту приватності користувачів як засіб уникнення співпраці з правоохоронними органами. В Україні ця проблема посилюється недостатньою чіткістю критеріїв “необхідності та пропорційності” втручання. Брак спеціалізації слідчих суддів у питаннях цифрових технологій призводить або до безпідставних відмов у доступі, або, навпаки, до надання занадто широких дозволів, що порушує права невинних осіб, чиї дані зберігаються у тій же системі.

Наявність окреслених процесуальних та технічних бар’єрів в Україні зумовлює необхідність пошуку ефективних рішень у міжнародному правовому полі. У цьому контексті особливої ваги набуває досвід країн Європейського Союзу та інструменти Другого додаткового протоколу до Будапештської конвенції про кіберзлочинність, що пропонують дієві механізми подолання подібних викликів.

Сучасна архітектура безпеки Європейського Союзу базується на поєднанні національних механізмів доступу до даних, наднаціональних інформаційних систем та інструментів транскордонного обміну. Такий багаторівневий підхід дозволяє ефективно протидіяти організованій злочинності, яка в умовах цифрового середовища остаточно втратила прив'язку до національних кордонів.

Ключовим кроком у гармонізації міжнародних стандартів стало прийняття Другого додаткового протоколу до Будапештської конвенції (2022 р.) [18]. Цей документ запроваджує революційні для кримінальної юстиції механізми:

- Пряма взаємодія з провайдерами: можливість звернення правоохоронних органів однієї держави безпосередньо до постачальника послуг в іншій юрисдикції для отримання реєстраційної інформації (subscriber information).
- Термінове збереження даних (Data Preservation): встановлення чіткого обов'язку швидкої фіксації електронної інформації, що запобігає її видаленню до моменту отримання офіційного судового рішення.
- Спрощена процедура правової допомоги: скорочення бюрократичних етапів при транскордонних запитах щодо даних про трафік та контент.

Ці інструменти спрямовані на подолання тривалих процедур міжнародної правової допомоги (MLA), що є критично важливим для розслідування кіберзлочинів.

5.2. Досвід Нідерландів та Німеччини: інтеграція проти контролю

Аналіз національних моделей Нідерландів та Німеччини демонструє два різні, але взаємодоповнюючі підходи до структурування доступу.

У Нідерландах держава впровадила інтегровані IT-платформи, які забезпечують правоохоронцям прямий електронний доступ до реєстрів населення, транспортних засобів та нерухомості в режимі реального часу. Це дозволяє здійснювати превентивний кримінальний аналіз та будувати профілі ризику без необхідності подання окремих запитів на кожному етапі [19].

Натомість Німеччина демонструє модель, де ефективність поєднується з жорстким дотриманням приватності. Тут діє принцип суворого розмежування повноважень та диференційований доступ залежно від тяжкості злочину. Особливістю є використання централізованих платформ обміну, що працюють за принципом “hit/no hit” (наявність/відсутність збігу). Це дозволяє слідчому дізнатися, чи є інформація в базі

іншого відомства, не розкриваючи змісту персональних даних до отримання відповідного процесуального дозволу.

При цьому ефективність боротьби з організованою злочинністю в ЄС забезпечується через:

1. Прюмські рішення (Prüm Decision): автоматизований обмін ДНК-профілями, відбитками пальців та даними реєстрації транспортних засобів між країнами ЄС. Децентралізована архітектура системи дозволяє кожній країні зберігати контроль над своїми базами, забезпечуючи при цьому миттєву ідентифікацію злочинців у транскордонному масштабі [20].
2. Шенгенську інформаційну систему (SIS): найбільша база даних безпеки в Європі. У Німеччині та Нідерландах SIS повністю інтегрована в щоденну поліцейську діяльність, що дозволяє миттєво отримувати оперативні сигнали (alerts) щодо розшукуваних осіб, зниклого майна або підозрілих переміщень членів злочинних угруповань [21].

Аналіз передових європейських практик закладає необхідне підґрунтя для ревізії вітчизняного законодавства. З огляду на це, доцільно окреслити конкретні інноваційні кроки та нормативні пропозиції, спрямовані на адаптацію української системи доступу до реєстрів до сучасних цифрових стандартів

Трансформація оперативної та слідчої діяльності з традиційної моделі у високотехнологічну систему управління ризиками потребує не лише технічного переоснащення, а й фундаментальних змін у нормативній базі. На основі аналізу міжнародних стандартів та виявлених системних проблем у вітчизняній практиці, пропонуються наступні концептуальні новації та конкретні кроки щодо реформування системи.

Першочерговим кроком має стати імплементація механізму термінового збереження даних (data preservation) у Кримінальний процесуальний кодекс України [17]. На відміну від процедури тимчасового доступу, цей інструмент дозволить слідчому негайно (до отримання ухвали суду) зобов’язати провайдера або держателя реєстру зафіксувати інформацію на строк до 90 днів. Це критично важливо для збереження волатильних цифрових слідів, які можуть бути видалені зловмисниками.

Також потребує вдосконалення процедура доступу до даних, що становлять банківську таємницю. Пропонується запровадження спеціалізованих шлюзів електронної взаємодії між правоохоронними органами та банківськими установами під контролем уповноважених слідчих суддів. Це дозволить замінити паперову переписку на автоматизовані запити, підписані КЕП, зі збереженням логування кожного звернення.

Реформування має базуватися на переході від “запитно-відповідної” моделі до моделі автоматизованої взаємодії на основі принципу інтероперабельності. Конкретні заходи включають:

1. Створення системи, яка дозволяє правоохоронцям здійснювати попередній пошук у всіх державних реєстрах одночасно. Система має повідомляти лише про *наявність* збігу (наприклад, реєстрації майна або рахунку), а повний доступ до змісту даних надаватиметься лише після завантаження в систему відповідної ухвали слідчого судді.
2. Уніфікація форматів/ Розробка та затвердження на рівні Кабінету Міністрів єдиних стандартів вивантаження даних із реєстрів. Інформація має надаватися у машиночитних форматах (JSON, XML, CSV), що дозволить використовувати спеціалізоване аналітичне програмне забезпечення для візуалізації зв’язків між об'єктами.

3. Централізована система аудиту: створення незалежного модуля логування всіх запитів до державних реєстрів. Це забезпечить прозорість дій правоохоронців, унеможливить несанкціонований збір даних та підвищить рівень довіри суспільства до цифрових методів розслідування.

Реалізація запропонованих кроків дозволить Україні сформувати модель цифрової оперативної діяльності, яка буде сумісною з європейськими стандартами (зокрема SIS та Прюмськими рішеннями), але адаптованою до національних безпекових викликів. Ключовим орієнтиром залишається створення інтегрованої системи, де швидкість доступу до інформації збалансована жорстким процесуальним контролем та захистом персональних даних із урахуванням методів правового регулювання інформаційного права України [22]. Вже сьогодні прикладом успішної імплементації систем контролю в реальному часі в Україні є Державна система онлайн-моніторингу (ДСОМ), яка забезпечує прозорість ринку азартних ігор та створює масив верифікованих цифрових даних, необхідних для виявлення фінансових злочинів та ідентифікації прихованих активів організованих злочинних груп [23].

Висновки

У ході дослідження встановлено, що в умовах мережевого суспільства державні та приватні реєстри трансформувалися з інструментів суто статистичного обліку в системоутворюючі елементи доказової бази у кримінальному провадженні. Цифровізація розслідування організованої злочинності потребує переходу від фрагментарного отримання даних до системного використання інформаційних ресурсів як механізму деконструкції злочинних мереж.

Підсумовуючи, зазначимо, що реформування системи доступу до реєстрів в Україні має базуватися на балансі між ефективністю розслідування та суворим дотриманням стандартів захисту персональних даних. Побудова інтегрованої системи цифрового доказування є не лише технічним завданням, а й необхідною умовою євроінтеграції України у сфері юстиції та безпеки. Своєчасна імплементація Другого додаткового протоколу до Будапештської конвенції та адаптація передових технологій аналізу даних (Big Data) дозволять правоохоронним органам діяти на випередження, забезпечуючи невідворотність покарання в умовах глобальних цифрових викликів.

ПОДЯКИ: Немає

КОНФЛІКТ ІНТЕРЕСІВ: Немає

Використана література:

1. Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023–2027: схвалений Указом Президента України від 11 травня 2023 року № 273/2023. URL: https://zakon.rada.gov.ua/laws/show/273/2023#Text
2. Jerry H. Ratcliffe. Intelligence-Led Policing URL: https://doi.org/10.4324/9781315717579
3. General Data Protection Regulation (GDPR). URL: https://gdpr-info.eu/
4. Концептуальні основи цифровізації кримінального провадження України : монографія / за заг. ред. Н. В. Глинської ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса Нац. акад. прав. наук України. – Харків : Право, 2024. – 452 с. URL: https://doi.org/10.31359/9786178612139.
5. Погорецький М.А Застосування новітніх технологій у розслідуванні та доказуванні воєнних злочинів (проблемні питання) URL: https://doi.org/10.17721/2413-5372.2023.3-4/84-102
6. General Data Protection Regulation (GDPR). URL: https://gdpr-info.eu/

7. Floridi, L. *The Ethics of Information*. Oxford University Press, 2013

8. Castells M., Cardoso G. The Network Society: From Knowledge to Policy. Washington, DC: Johns Hopkins Center for Transatlantic Relations, 2005. URL: https://www.dhi.ac.uk/san/waysofbeing/data/communication-zangana-castells-2006.pdf

9. Internet Organised Crime Threat Assessment (IOCTA) / Europol Report. URL: https://www.europol.europa.eu/publications-events/main-reports/iocta-report

10. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities. URL: https://eur-lex.europa.eu/eli/dir/2016/680/oj/eng

11. CASE OF GASKIN v. THE UNITED KINGDOM. Judgment of 7 July 1989. URL: https://hudoc.echr.coe.int/tur#{%22itemid%22:[%22001-57491%22]}

12. Schengen Information System (SIS). Official policy website. URL: https://home-affairs.ec.europa.eu/policies/schengen/schengen-information-system_en

13. Ухвала Дзержинського районного суду м. Кривого Рогу від 30.01.2024 по справі № 210/5936/23. URL: https://opendatabot.ua/court/116651810-ecd10fb1355d2f576c39ae098a8cf138

14. Гуцалюк М.В. Антонюк П.Є. Проблемні аспекти процесуальної спроможності використання електронної (цифрової) інформації як доказів в кримінальному провадженні // Інформація і право. – № 2(41)/2022. – С.116-122. URL: https://doi.org/10.37750/2616-6798.2022.2(41).270373

15. Трембіта URL: https://trembita.gov.ua/ua

16. Гуцалюк М.В. Імплементація європейських стандартів у боротьбі з кіберзлочинністю: проблеми правового регулювання електронних доказів в Україні // Слово Національної школи суддів України. - № 2 (51) 2025. – С. 167-176. URL: https://doi.org/10.37566/2707-6849-2025-2(51)-16

17. Гуцалюк М. Процесуальний механізм термінового збереження електронних доказів у світлі Будапештської конвенції та Другого додаткового протоколу: потреба імплементації в КПК України : Матеріали круглого столу «Євроінтеграційні процеси та їх вплив на правову політику України: теоретичні та практичні аспекти» від 13 березня 2026 р., м. Київ, 2026.

18. Ахтирська Н., Гуцалюк М. Правові засоби боротьби з кіберзагрозами під час воєнного стану в світлі використання механізмів Другого додаткового протоколу до Конвенції про кіберзлочинність. *Актуальні питання розвитку юридичної науки та практики*: матеріали Міжнародної науково-практичної конференції (12 травня 2022 року) / За заг. ред. д.ю.н., акад. НАПрН України О.П. Орлюк, к.ю.н., доц. Г.З Остапенко, к.ю.н. А.В. Айдинян. К., 2022. – С. 283-286

19. Marc Schuilenburg, Melvin Soudijn Big data policing: The use of big data and algorithms by the Netherlands Police Open Access // Policing: A Journal of Policy and Practice, Volume 17, 2023. URL: https://doi.org/10.1093/police/paad061

20. Stepping up cross-border cooperation – the Prüm decision. URL: https://eur-lex.europa.eu/EN/legal-content/summary/stepping-up-cross-border-cooperation-the-pr-m-decision.html

21. Schengen Information System (SIS). Official policy overview. URL: https://home-affairs.ec.europa.eu/policies/schengen/schengen-information-system_en

22. Марущак А. І. Методи правового регулювання безпеки особи, суспільства, держави в інформаційній сфері. Вісник Національної академії правових наук України. – 2019. -№ 3. С. 75-89. http://visnyk.kh.ua/ru/article/metodi-pravovogo-regulyuvannya-bezpeki-osobi-suspilstva-derzhavi-v-informatsiyniy-sferi

23. В Україні запустили Державну систему онлайн-моніторингу грального бізнесу URL: https://www.kyivpost.com/uk/post/73661

Михайло Васильович Гуцалюк
кандидат юридичних наук, доцент, старший науковий співробітник
провідний науковий співробітник Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при РНБО України
03035 Україна м. Київ-ДСП, пл. Солом'янська, 1
email: mykhaylogutsalyuk@gmail.com
Анатолій Іванович Марущак
доктор юридичних наук, професор
ГО «Міжнародна академія інформації», професор Національної академії Служби безпеки України
03022, м. Київ, вул. Михайла Максимовича, 7
email: amarushchak@ukr.net

Mykhaylo V. Gutsalyuk
Candidate of Legal Sciences (PhD in Law), Associate Professor, Senior Research Fellow
Leading Researcher of the Interagency Research Center for Combating Organized Crime under the National Security and Defense Council of Ukraine
03035 Ukraine Kyiv-DSP, Solomyanska Square, 1
email: mykhaylogutsalyuk@gmail.com
Anatolii I. Marushchak
Doctor of Juridical Sciences, Professor
Co-founder, Strategic Adviser (pro-bono), NGO International Information Academy
03022, Kyiv, Mykhaylo Maksymovycha St., 7 Kyiv, Ukraine
email: amarushchak@ukr.net

Рекомендоване цитування: Гуцалюк М.В., Марущак А.І. Доступ правоохоронних органів до державних і приватних реєстрів: проблеми та перспективи розвитку в Україні. *Інформація і право*. № 2(57)/2026. 2026. С. 22-32. https://doi.org/10.37750/2616-6798.2026.2(57).364226

Suggested Citation: Gutsalyuk M., Marushchak A. (2026) Access of Law Enforcement Authorities to State and Private Registers: Problems and Prospects for Development in Ukraine. *Information and Law*. 2(57)/2026. 22-32. https://doi.org/10.37750/2616-6798.2026.2(57).364226

Дата надходження статті до редакції: 20.04.2026 р.
Дата прийняття статті до друку після рецензування: 27.04.2026 р.
Дата публікації (оприлюднення): 26.05.2026 р.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~