ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНО-ТЕХНІЧНОЇ ДІЯЛЬНОСТІ ПОЛІЦІЇ





УДК 351.74:004(477)
DOI https://doi.org/10.32782/2709-9261-2026-2-18-17

Габорець Ольга Андріївна,
доктор філософії в галузі освіти, доцент
(Донецький державний університет внутрішніх справ, м. Кропивницький)
ORCID: https://orcid.org/0000-0002-7138-5847

Лунгол Ольга Миколаївна,
кандидат педагогічних наук, доцент
(Донецький державний університет внутрішніх справ, м. Кропивницький)
ORCID: https://orcid.org/0000-0001-8128-0072

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ ЯК СКЛАДНИК ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ПРАВООХОРОННИХ ОРГАНІВ УКРАЇНИ

У статті досліджено роль інформаційно-комунікаційних технологій у цифровій трансформації правоохоронних органів України. Обґрунтовано розширене розуміння ІКТ як інтеграційної основи цифрової правоохоронної екосистеми, систематизовано її структурні компоненти та розкрито функціональне значення ІКТ. Визначено роль інтероперабельності інформаційних ресурсів та окреслено перспективні напрями розвитку інформаційно-аналітичного забезпечення правоохоронної діяльності.

Ключові слова: *інформаційно-комунікаційні технології, цифрова трансформація, правоохоронна діяльність, цифрова правоохоронна екосистема, інтероперабельність, інформаційно-аналітичне забезпечення.*

Постановка проблеми. Цифрова трансформація суспільства стала одним із ключових чинників модернізації державного управління, істотно змінюючи механізми функціонування публічних інституцій, форми взаємодії держави із суспільством та підходи до прийняття управлінських рішень. У цих умовах правоохоронні органи вже не можуть ефективно виконувати покладені на них функції, спираючись виключно на традиційні організаційні та інформаційні механізми. Стрімке зростання обсягів цифрової інформації, поширення транснаціональної організованої злочинності, розвиток кіберзлочинності, використання злочинними угрупованнями технологій штучного інтелекту, криптовалют, анонімних мереж та цифрових платформ формують принципово нові виклики для правоохоронної системи, адекватне реагування на які можливе лише за умови комплексної цифрової трансформації її діяльності.

Для України зазначена проблематика набуває особливої актуальності в умовах повномасштабної збройної агресії. Сучасна війна супроводжується безпрецедентним використанням цифрових технологій як інструментів інформаційного впливу, кібероперацій, документування воєнних злочинів, протидії диверсійній діяльності, пошуку осіб, аналізу відкритих джерел інформації,

© Габорець О. А., Лунгол О. М., 2026
Стаття поширюється на умовах ліцензії відкритого доступу (CC BY 4.0)

а також забезпечення міжвідомчої взаємодії суб'єктів сектору безпеки й оборони. За таких умов цифровізація правоохоронної діяльності перестає бути лише одним із напрямів адміністративної реформи, перетворюючись на необхідну передумову забезпечення національної безпеки, стійкості державних інституцій та ефективної реалізації правоохоронної функції.

Водночас сучасний етап розвитку правоохоронної системи характеризується переходом від окремих процесів інформатизації до комплексної цифрової трансформації, яка охоплює зміну організаційної моделі діяльності, механізмів інформаційної взаємодії та прийняття рішень. За таких умов ІКТ слід розглядати як інтеграційну основу інформаційно-аналітичного середовища, що об'єднує інформаційні ресурси, аналітичні платформи, кримінальний аналіз, штучний інтелект, OSINT і цифрову криміналістику. Водночас комплексне осмислення ІКТ як системоутворювальної основи цифрової трансформації правоохоронних органів залишається недостатнім, що зумовлює необхідність визначення їх функціонального призначення, взаємозв'язків і ролі у формуванні цифрової правоохоронної екосистеми.

Аналіз останніх досліджень і публікацій. Проблематика використання інформаційно-комунікаційних технологій у правоохоронній діяльності останніми роками набула особливої актуальності в українській правовій науці, що зумовлено одночасним впливом цифрової трансформації публічного управління, розвитком кіберзлочинності, поширенням технологій штучного інтелекту та необхідністю адаптації правоохоронних органів до умов гібридних загроз. Сучасні наукові дослідження засвідчують поступовий перехід від розуміння ІКТ як допоміжного інструменту автоматизації окремих службових процесів до їх сприйняття як чинника зміни самої моделі правоохоронної діяльності.

Вагомий внесок у дослідження ризиків цифрової трансформації правоохоронних органів в умовах гібридних загроз здійснив В. М. Василенко [1], який розглядає цифровізацію не лише як технологічне оновлення, а як комплексне явище, що охоплює нормативно-правове регулювання, інституційну організацію, управлінські підходи та взаємодію з громадянами. Особливо цінним у його підході є акцент на необхідності балансу між ефективністю діяльності органів правопорядку та дотриманням прав і свобод людини, а також виділення ризиків кіберзалежності, несанкціонованого доступу до конфіденційної інформації, дефіциту нормативного забезпечення цифрових процедур і можливих зловживань цифровими інструментами.

Близькою за проблематикою є позиція Т. І. Моргунової [2], яка досліджує інформаційно-комунікаційні технології у правозастосуванні крізь призму сучасних викликів і перспектив. Авторка наголошує, що ІКТ дають змогу автоматизувати ключові процеси, підвищити ефективність оперативно-розшукової роботи, покращити аналітику злочинності та оптимізувати прийняття рішень. Водночас окрему увагу вона приділяє етичним викликам цифровізації, зокрема ризикам втручання у приватне життя, алгоритмічної дискримінації, порушення прав людини через масове використання технологій стеження та проблемі відповідальності за рішення, ухвалені автоматизованими системами.

О. Д. Жученко досліджує вплив сучасних інформаційних технологій на діяльність правоохоронних органів крізь призму трансформації їх традиційних функцій [3]. Науковець обґрунтовує, що розвиток інформаційних технологій впливає не лише на виконання класичних правоохоронних завдань, а й на появу нових функцій, пов'язаних із цифровою криміналістикою, електронною поліцією, віртуальними поліцейськими дільницями, автоматизацією слідчих процедур і стратегічним прогнозуванням. Важливим є висновок автора про те, що сучасні ІКТ підвищують ефективність правоохоронної діяльності, однак одночасно породжують ризики порушення безпеки даних, етичні проблеми та технологічну залежність.

У ширшому соціально-філософському вимірі значення ІКТ для цифрової трансформації суспільства розглядають А. Г. Крупа [4] та В. Ю. Мар'єнко [4]. Їхній підхід є корисним для формування загальнотеоретичного підґрунтя цього дослідження, оскільки автори акцентують увагу на тому, що ІКТ є ключовим рушієм цифрової трансформації суспільства, впливаючи на економіку, освіту, охорону здоров'я, державне управління, інформаційну культуру та соціальні процеси. Водночас для цілей цього дослідження їхні висновки потребують конкретизації саме щодо правоохоронної сфери, де цифровізація має підвищений рівень правових, етичних і безпекових ризиків.

Окремий напрям сучасних досліджень становлять праці, присвячені кримінальному аналізу, Intelligence-Led Policing, OSINT, цифровій криміналістиці та штучному інтелекту. Вагомий внесок у розвиток відповідних напрямів здійснили О. Є. Користін та співавтори [5], К. Ю. Ісмайлов [6], А. В. Мовчан [7], Д. Ю. Узлов, О. О. Власов і В. М. Струков [8], Д. М. Рибка [9], М. О. Думчиков [10] та інші науковці. Аналіз їхніх праць свідчить про формування вагомого наукового підґрунтя для розвитку окремих складників цифрової модернізації правоохоронної діяльності. Водночас переважна частина таких досліджень зосереджена на окремих технологічних або методологічних напрямах, що актуалізує потребу в їх системному осмисленні як взаємопов'язаних компонентів єдиної цифрової правоохоронної екосистеми.

Узагальнення наукових джерел дає підстави виокремити кілька основних підходів до розуміння ролі ІКТ у правоохоронній діяльності. Перший підхід можна визначити як інструментально-технологічний: у його межах ІКТ розглядаються переважно як засоби автоматизації документообігу, обліку, комунікації, відеоспостереження, обробки даних і підвищення оперативності службових процесів. Другий підхід є ризик-орієнтованим і акцентує увагу на загрозах цифровізації: кібербезпеці, захисті персональних даних, алгоритмічній упередженості, порушенні приватності та прав людини. Третій підхід можна охарактеризувати як функціонально-трансформаційний, оскільки він пов'язує розвиток ІКТ зі зміною традиційних функцій правоохоронних органів, появою цифрової криміналістики, електронної поліції та нових моделей взаємодії з громадянами. Водночас не досить розробленим залишається четвертий – системно-екосистемний підхід, у межах якого ІКТ розглядаються не як сукупність окремих цифрових інструментів, а як інтеграційна основа єдиного інформаційно-аналітичного середовища правоохоронної діяльності.

Саме ця прогалина визначає наукову нішу цього дослідження. Наявні праці переконливо доводять значення ІКТ для автоматизації правоохоронних процесів, підвищення ефективності розслідування, розвитку цифрової криміналістики, впровадження штучного інтелекту та посилення кібербезпеки. Проте в них не досить розкрито взаємозв'язок між інформаційними системами, OSINT, Big Data, штучним інтелектом, цифровою криміналістикою, кримінальним аналізом, Intelligence-Led Policing

та системами підтримки прийняття рішень як компонентами єдиної цифрової правоохоронної екосистеми. Отже, подальшого наукового осмислення потребує саме концептуальна модель ІКТ як інтеграційної основи цифрової трансформації правоохоронних органів України.

Метою статті є комплексне дослідження ролі інформаційно-комунікаційних технологій у цифровій трансформації правоохоронних органів України, обґрунтування їх місця як інтеграційної основи цифрової правоохоронної екосистеми, визначення основних компонентів, функціональних взаємозв'язків, сучасних викликів і перспектив розвитку, а також розроблення концептуальних підходів до підвищення ефективності інформаційно-аналітичного забезпечення правоохоронної діяльності в умовах цифровізації.

Виклад основного матеріалу. Стрімкий розвиток цифрових технологій, глобальна цифровізація суспільних процесів та зміна характеру сучасної злочинності зумовили необхідність переосмислення традиційних підходів до організації правоохоронної діяльності. Якщо ще донедавна інформаційно-комунікаційні технології розглядалися переважно як допоміжний інструмент автоматизації окремих службових процесів, то нині вони дедалі більше визначають принципи функціонування правоохоронної системи, впливаючи не лише на способи збирання, накопичення та оброблення інформації, а й на механізми прийняття управлінських, оперативно-службових і процесуальних рішень. Така трансформація є закономірною відповіддю на появу нових форм злочинної діяльності, що дедалі частіше здійснюється у цифровому середовищі, характеризується високим рівнем технологічності, транскордонністю, швидкістю поширення та використанням інструментів штучного інтелекту, анонімних комунікаційних платформ, криптовалют і цифрових сервісів.

Сучасний етап розвитку суспільства характеризується переходом до економіки даних, у межах якої інформація набуває ознак стратегічного ресурсу, а здатність державних інституцій ефективно працювати з інформаційними потоками визначає їхню інституційну спроможність. У таких умовах правоохоронні органи дедалі більше функціонують у середовищі безперервного інформаційного обміну, де швидкість отримання, інтеграції, аналізу та використання відомостей безпосередньо впливає на ефективність запобігання, виявлення, документування та розслідування кримінальних правопорушень. Це зумовлює переорієнтацію правоохоронної діяльності від реагування на вже вчинені кримінальні правопорушення до прогнозування ризиків, аналітичного супроводу управлінських рішень та випереджувального реагування на загрози.

Такі зміни свідчать про поступовий перехід від моделі, у якій інформаційні технології виконували виключно сервісну функцію, до моделі, за якої вони стають інтегруючою основою всієї правоохоронної діяльності. У науковій літературі цей процес традиційно описується через категорії «інформатизація», «цифровізація» та «цифрова трансформація», які нерідко використовуються як тотожні. Водночас їх зміст істотно відрізняється як за масштабом, так і за характером змін, що відбуваються в діяльності правоохоронних органів.

Еволюція використання цифрових технологій у діяльності правоохоронних органів характеризується послідовним переходом від інформатизації до цифровізації, а згодом – до цифрової трансформації. Якщо інформатизація була спрямована переважно на автоматизацію окремих інформаційних процесів, а цифровізація забезпечила переведення службових процедур у цифровий формат, то цифрова трансформація передбачає системну зміну організаційної моделі правоохоронної діяльності, механізмів інформаційної взаємодії та процесів прийняття рішень на основі інтегрованих інформаційних ресурсів і сучасних аналітичних технологій. Її результатом має стати не збільшення кількості цифрових сервісів, а формування єдиного інформаційно-аналітичного середовища.

На відміну від цифровізації, цифрова трансформація передбачає не лише впровадження нових технологічних рішень, а докорінну зміну організаційної моделі функціонування правоохоронних органів, управлінських підходів, інформаційної взаємодії, процесів прийняття рішень та механізмів реалізації правоохоронної функції. У центрі таких змін перебувають не окремі цифрові інструменти, а інформація як основний ресурс діяльності, що потребує інтегрованого управління протягом усього її життєвого циклу – від отримання до використання для вироблення управлінського або процесуального рішення. Саме тому цифрова трансформація повинна розглядатися як якісно новий етап розвитку правоохоронної системи, що передбачає зміну її архітектури, а не лише модернізацію окремих елементів.

Зазначений підхід повністю узгоджується із сучасними міжнародними тенденціями розвитку правоохоронної діяльності, у межах яких дедалі ширшого поширення набувають концепції Intelligence-Led Policing, Data-Driven Policing, Evidence-Based Policing та Digital Policing. Попри відмінності у методологічних підходах, усі вони ґрунтуються на спільному принципі: основою ефективної правоохоронної діяльності стають своєчасні, достовірні та належним чином проаналізовані дані, інтегровані в єдине інформаційне середовище. Це свідчить про поступову зміну парадигми функціонування правоохоронних органів – від діяльності, орієнтованої переважно на реагування, до діяльності, що ґрунтується на аналізі інформації, оцінці ризиків, прогнозуванні криміногенних процесів та підтримці прийняття управлінських рішень [14].

На нашу думку, саме на цьому етапі доцільно відмовитися від традиційного розуміння інформаційно-комунікаційних технологій як сукупності технічних засобів передачі та оброблення інформації. Такий підхід був цілком виправданим на початкових етапах інформатизації, однак уже не відображає сучасного рівня розвитку цифрових технологій та їх ролі у функціонуванні правоохоронних органів. Нині ІКТ виконують значно ширші функції: вони забезпечують інтеграцію інформаційних ресурсів, формують єдиний інформаційний простір, створюють умови для міжвідомчої взаємодії, підтримують функціонування аналітичних платформ, кримінального аналізу, цифрової криміналістики, технологій штучного інтелекту, інструментів розвідки на основі відкритих джерел (OSINT), геоінформаційних систем та інших цифрових сервісів, без яких реалізація сучасної правоохоронної функції стає практично неможливою.

У зв'язку з цим пропонуємо розглядати інформаційно-комунікаційні технології не як окремий інструмент цифровізації, а як інтеграційну основу цифрової правоохоронної екосистеми, під якою слід розуміти цілісне інформаційно-аналітичне середовище, що забезпечує безперервний цикл збору, накопичення, інтеграції, верифікації, аналізу, візуалізації, передачі та використання інформації для реалізації правоохоронних функцій. У межах такої екосистеми інформацій-

ні системи, цифрові реєстри, аналітичні платформи, технології штучного інтелекту, кримінальний аналіз, цифрова криміналістика, OSINT та системи підтримки прийняття рішень функціонують не ізольовано, а як взаємопов'язані компоненти єдиного інформаційного середовища, спрямованого на забезпечення ефективного управління безпекою.

Структурні компоненти цифрової правоохоронної екосистеми, їх функціональне призначення та приклади практичної реалізації систематизовано в табл. 1.

Таблиця 1

Структурні компоненти цифрової правоохоронної екосистеми та їх функціональне призначення

Компонент цифрової правоохоронної екосистеми	Основне функціональне призначення	Приклади реалізації
Інформаційні ресурси та реєстри	Формування, накопичення, актуалізація та зберігання цифрових даних	ЄІС МВС, ІПНП, ЄРДР, державні реєстри, відомчі бази даних
Інформаційно-комунікаційна інфраструктура	Забезпечення інформаційної взаємодії, телекомунікацій та міжвідомчого обміну інформацією	Захищені мережі передачі даних, електронна взаємодія інформаційних систем
Аналітичні технології та інструменти	Виявлення закономірностей і взаємозв'язків, оцінювання ризиків, прогнозування тенденцій та інформаційно-аналітична підтримка прийняття рішень	Кримінальний аналіз, аналіз зв'язків, геопросторовий аналіз, аналіз великих даних, прогнозна аналітика
Технології та інструменти розвідки на основі відкритих джерел	Пошук, верифікація та документування інформації з відкритих джерел	OSINT, SOCMINT, WEBINT, аналіз відкритих геопросторових даних
Технології штучного інтелекту	Автоматизований аналіз великих масивів даних, прогнозування, інтелектуальна підтримка прийняття рішень	Машинне навчання, комп'ютерний зір, NLP, прогнозна аналітика
Цифрова криміналістика	Виявлення, дослідження та документування цифрових доказів	Комп'ютерна, мобільна, мережева криміналістика
Геоінформаційні та візуалізаційні системи	Просторовий аналіз, картографування криміногенних процесів, візуалізація інформації	GIS, Heat Maps, Crime Mapping
Системи підтримки прийняття рішень	Інформаційно-аналітична підтримка стратегічних, тактичних та оперативних рішень	Decision Support Systems (DSS), Risk Assessment Systems
Кібербезпека та захист інформації	Захист інформаційних ресурсів, забезпечення конфіденційності, цілісності та доступності даних	Засоби криптографічного захисту, SIEM, контроль доступу, моніторинг інцидентів

Джерело: розроблено авторами.

Наведена систематизація дає підстави визначити цифрову правоохоронну екосистему як багатокомпонентне середовище, ефективність якого залежить від узгодженої взаємодії інформаційних ресурсів, комунікаційної інфраструктури, аналітичних технологій і систем підтримки прийняття рішень. Наскрізними умовами її функціонування є кібербезпека, захист інформації та належне управління даними.

Практичним прикладом поступового формування цифрової правоохоронної екосистеми в Україні є розвиток Єдиної інформаційної системи Міністерства внутрішніх справ України (ЄІС МВС), створення та функціонування якої спрямоване на забезпечення інформаційної взаємодії між органами системи МВС, а також інтеграцію інформаційних ресурсів у межах єдиного цифрового середовища [11]. На відміну від традиційних автоматизованих інформаційних систем, що функціонували автономно та забезпечували виконання окремих службових завдань, ЄІС МВС ґрунтується на принципах централізованого управління інформаційними ресурсами, стандартизації інформаційного обміну, уніфікації цифрових процесів та забезпечення міжвідомчої взаємодії.

Функціонування ЄІС МВС забезпечує інформаційну взаємодію між Національною поліцією України, Державною прикордонною службою України, Державною міграційною службою України, Державною службою України з надзвичайних ситуацій, Національною гвардією України, сервісними центрами МВС та іншими структурними підрозділами системи Міністерства внутрішніх справ. Такий підхід створює передумови для формування єдиного інформаційного простору, у якому цифрові дані можуть використовуватися комплексно незалежно від суб'єкта їх первинного формування. Це істотно підвищує оперативність інформаційного обміну, зменшує дублювання інформації, забезпечує актуальність відомостей та сприяє прийняттю більш обґрунтованих управлінських і процесуальних рішень.

Особливістю сучасної моделі функціонування ЄІС МВС є її орієнтація не лише на накопичення інформації, а й на створення умов для її подальшого аналітичного використання. За сучасних умов інформація перестає виконувати виключно облікову функцію та трансформується у стратегічний ресурс правоохоронної діяльності. Саме тому ефективність інформаційної системи визначається не обсягом накопичених даних, а можливістю їх інтеграції, автоматизованого опрацювання, візуалізації, аналізу та використання для підтримки прийняття управлінських, оперативно-службових і процесуальних рішень.

Водночас розвиток цифрової правоохоронної екосистеми не обмежується функціонуванням ЄІС МВС. Важливе місце у її структурі посідають інформаційні ресурси Національної поліції України, зокрема Інформаційний портал Національної поліції України (ІПНП), який забезпечує інтеграцію відомчих інформаційних підсистем, автоматизує інформаційний обмін між структурними підрозділами поліції та створює умови для комплексного використання інформації під час виконання оперативно-службових завдань [12]. Інтеграція інформаційних ресурсів ІПНП із підсистемами ЄІС МВС значно розширює можливості оперативного отримання відомостей, їх аналітичного опрацювання та використання під час реалізації правоохоронної функції.

Поряд із цим цифрова інфраструктура правоохоронних органів України охоплює низку спеціалізованих інформаційних систем, реєстрів, баз даних та електронних сервісів, кожен із яких виконує визначені законодавством функції. Однак їх ефективність дедалі більше залежить не від рівня технічної досконалості окремої інформаційної системи, а від можливості функціонувати у межах єдиного інформаційно-аналітичного середовища. Саме тому одним із ключових напрямів подальшої цифрової трансформації правоохоронних органів має стати забезпечення інтероперабельності інформаційних ресурсів, що передбачає їх технічну сумісність, використання уніфікованих форматів даних, стандартизованих протоколів інформаційного обміну та єдиних механізмів автентифікації користувачів.

На нашу думку, саме розвиток Єдиної інформаційної системи МВС та інтегрованих інформаційних ресурсів Національної поліції України свідчить про поступовий перехід від моделі інформатизації окремих напрямів діяльності до формування цифрової правоохоронної екосистеми, у межах якої інформаційно-комунікаційні технології забезпечують не лише автоматизацію службових процесів, а і створюють єдине інформаційно-аналітичне середовище для підтримки прийняття рішень, розвитку кримінального аналізу, використання технологій штучного інтелекту, цифрової криміналістики та інструментів OSINT. Саме така інтеграційна модель, на нашу думку, відповідає сучасним європейським підходам до цифрової трансформації правоохоронної діяльності та визначає стратегічний напрям подальшої модернізації системи органів правопорядку України.

Сучасна роль ІКТ виходить за межі традиційного розуміння їх як сукупності програмних, технічних і телекомунікаційних засобів. Наявні визначення переважно сформувалися в період інформатизації державного управління і неповною мірою враховують розвиток штучного інтелекту, інтелектуального аналізу даних, цифрової криміналістики, OSINT, прогнозної аналітики та геоінформаційних систем. Ізольований розгляд цих технологій також не відповідає мережевому характеру сучасної правоохоронної діяльності, ефективність якої визначається рівнем інтеграції цифрових ресурсів і можливістю комплексного аналізу даних.

З огляду на це вважаємо, що інформаційно-комунікаційні технології у правоохоронній діяльності доцільно визначати як інтегровану сукупність цифрових технологій, інформаційних систем, програмно-апаратних комплексів, телекомунікаційних засобів, аналітичних платформ і цифрових сервісів, які забезпечують безперервний цикл формування, накопичення, інтеграції, оброблення, аналізу, візуалізації, передачі та використання інформації для підтримки управлінських, оперативно-службових, оперативно-розшукових і процесуальних рішень, спрямованих на забезпечення публічної безпеки, протидію злочинності та захист прав і свобод людини.

Запропоноване визначення акцентує увагу не лише на технологічній природі ІКТ, а передусім на їх інтеграційній функції. Інформаційно-комунікаційні технології забезпечують взаємодію компонентів цифрової правоохоронної екосистеми, безперервність інформаційних процесів, сумісність цифрових ресурсів і комплексне використання даних. Ефективність такої моделі визначається не кількістю впроваджених цифрових рішень, а рівнем їх функціональної узгодженості.

Інтеграційний характер сучасних ІКТ зумовлює поступову зміну парадигми правоохоронної діяльності та трансформацію ролі інформації у процесах забезпечення публічної безпеки і протидії злочинності. Якщо раніше інформація використовувалася переважно для документування вже вчинених правопорушень, то в умовах цифрової трансформації вона стає основою оцінювання ризиків, виявлення прихованих закономірностей і взаємозв'язків, прогнозування криміногенних процесів та аналітичної підтримки управлінських рішень. У межах цифрової правоохоронної екосистеми інформаційні потоки проходять послідовний цикл отримання, верифікації, накопичення, інтеграції, аналітичного опрацювання, візуалізації та використання. При цьому цінність даних визначається не лише їх достовірністю і повнотою, а й можливістю зіставлення з іншими інформаційними масивами, унаслідок чого окремі відомості трансформуються в аналітичний продукт, придатний для підтримки стратегічних, тактичних та оперативних рішень. Саме така модель створює передумови для розвитку проактивної правоохоронної діяльності, орієнтованої не лише на реагування на вчинені правопорушення, а й на своєчасне виявлення та попередження загроз.

У зв'язку з цим інформаційно-комунікаційні технології виконують не лише інформаційну, а й інтеграційну, аналітичну, прогностичну та координаційну функції. Інтеграційна функція полягає в об'єднанні різнорідних інформаційних ресурсів у єдиному цифровому середовищі. Аналітична функція забезпечує перетворення масиву різнорідних даних на інформацію, придатну для оцінювання оперативної обстановки, виявлення закономірностей злочинної діяльності та встановлення взаємозв'язків між окремими подіями. Прогностична функція спрямована на виявлення тенденцій розвитку криміногенних процесів, оцінювання ризиків та прогнозування можливих сценаріїв розвитку оперативної обстановки. Координаційна функція забезпечує інформаційну взаємодію між правоохоронними органами, іншими суб'єктами сектору безпеки і оборони, органами державної влади та міжнародними партнерами.

Водночас інтеграція ІКТ не повинна зводитися до механічного об'єднання окремих інформаційних систем. Її сутність полягає у забезпеченні функціональної узгодженості всіх етапів роботи з інформацією, за якої результати одного інформаційного процесу стають основою для реалізації наступного. За такого підходу технологічна досконалість окремих компонентів набуває практичного значення лише за умови їх включення в узгоджений інформаційно-аналітичний процес, орієнтований на формування аналітичного продукту та підтримку прийняття рішень.

Сучасна цифрова трансформація правоохоронних органів не повинна зводитися до впровадження нових інформаційних систем чи цифрових сервісів. Визначальною умовою є їх інтероперабельність, тобто здатність цифрових платформ, інформаційних ресурсів та аналітичних систем функціонувати в єдиному інформаційному просторі. Практика держав-членів Європейського Союзу свідчить, що інтеграція інформаційних ресурсів є однією з передумов розвитку моделей Intelligence-Led Policing та Data-Driven Policing.

Для правоохоронних органів України інтероперабельність має охоплювати технічну сумісність систем, уніфікацію форматів даних, стандартизацію інформаційного обміну, узгоджене управління цифровими ресурсами, захист інформації та нормативне врегулювання міжвідомчої взаємодії. Основним викликом сучасного етапу є не створення нових цифрових рішень, а забезпечення їх комплексної взаємодії в межах цілісної цифрової правоохоронної екосистеми.

Формування цифрової правоохоронної екосистеми має ґрунтуватися на принципах інтероперабельності та аналітичної орієнтованості. Перший передбачає сумісність інформаційних систем, уніфікацію форматів даних, стандартизацію електронної взаємодії та повторне використання інформації відповідно до компетенції суб'єктів. Другий вимагає переходу від накопичення даних до їх інтелектуального опрацювання із застосуванням кримінального аналізу, аналізу великих даних, машинного навчання та сучасних засобів візуалізації.

Водночас ефективність цифрової трансформації неможлива без розвитку людського потенціалу. Досвід держав Європейського Союзу переконливо демонструє, що навіть найсучасніші інформаційні системи не забезпечують очікуваного результату за відсутності належного рівня цифрових компетентностей працівників правоохоронних органів. У зв'язку з цим цифрова трансформація повинна супроводжуватися безперервним професійним розвитком персоналу, упровадженням сучасних програм підготовки та підвищення кваліфікації, спрямованих на формування навичок роботи з аналітичними платформами, технологіями штучного інтелекту, цифровою криміналістикою, інструментами OSINT та засобами інформаційно-аналітичного забезпечення.

Важливим складником розвитку цифрової правоохоронної екосистеми є також забезпечення довіри до цифрових технологій. Її формування неможливе без чіткого нормативно-правового регулювання використання штучного інтелекту, алгоритмів автоматизованого аналізу інформації, біометричних технологій, систем відеоаналітики та інших цифрових інструментів, здатних впливати на права і свободи людини. У цьому контексті доцільним є впровадження ризик-орієнтованого підходу до використання цифрових технологій, який передбачає оцінювання потенційного впливу інформаційних систем на права людини ще на етапі їх розроблення та впровадження. Такий підхід повністю відповідає сучасним європейським тенденціям розвитку цифрового права та сприятиме гармонізації українського законодавства з правом Європейського Союзу [13].

Окремої уваги потребує питання розвитку інформаційно-аналітичного забезпечення правоохоронної діяльності. Проведене дослідження дозволяє стверджувати, що його подальша еволюція буде пов'язана не зі збільшенням кількості інформаційних ресурсів, а з підвищенням якості їх взаємодії. Перспективним напрямом є формування інтегрованих аналітичних платформ, які забезпечуватимуть автоматизоване об'єднання інформації з державних реєстрів, відомчих інформаційних систем, відкритих джерел, результатів цифрової криміналістики та інших інформаційних ресурсів із подальшим застосуванням інструментів кримінального аналізу, технологій штучного інтелекту та прогнозної аналітики. Саме такий підхід дозволить перейти від інформаційного забезпечення окремих процесів до комплексної підтримки прийняття рішень у сфері забезпечення публічної безпеки.

Разом із тим ефективне функціонування цифрової правоохоронної екосистеми неможливе без урахування сучасних міжнародних підходів до організації інформаційно-аналітичного забезпечення правоохоронної діяльності. Практика держав-членів Європейського Союзу свідчить, що цифрова трансформація правоохоронних органів здійснюється не шляхом збільшення кількості інформаційних систем, а завдяки формуванню інтегрованого цифрового середовища, яке забезпечує оперативний інформаційний обмін, міжвідомчу взаємодію та використання сучасних аналітичних технологій під час прийняття управлінських і процесуальних рішень. У цьому контексті особливого значення набувають діяльність Європолу щодо розвитку інформаційних платформ та аналітичних можливостей, стандарти Інтерполу у сфері міжнародного інформаційного обміну, а також освітні ініціативи CEPOL, спрямовані на формування цифрових компетентностей працівників правоохоронних органів. Спільною рисою цих підходів є орієнтація на використання даних як стратегічного ресурсу, інтеграцію інформаційних систем, забезпечення їх інтероперабельності та широке застосування кримінального аналізу, штучного інтелекту й цифрової криміналістики.

Для України зазначений досвід має особливе значення не лише у контексті європейської інтеграції, а й з огляду на необхідність підвищення ефективності правоохоронної діяльності в умовах воєнного стану та післявоєнного відновлення держави. Створення сучасної цифрової правоохоронної екосистеми потребує подальшого розвитку Єдиної інформаційної системи МВС, розширення можливостей інформаційно-комунікаційних систем Національної поліції України, забезпечення сумісності державних інформаційних ресурсів, удосконалення механізмів міжвідомчого інформаційного обміну та впровадження сучасних аналітичних платформ, здатних об'єднувати інформацію з різних джерел у межах єдиного інформаційно-аналітичного середовища. Водночас пріоритетним напрямом має стати розвиток цифрових компетентностей працівників правоохоронних органів, оскільки саме людський потенціал визначає ефективність використання навіть найбільш досконалих інформаційно-комунікаційних технологій.

Подальший розвиток цифрової правоохоронної екосистеми доцільно пов'язувати із впровадженням принципів Data-Driven Policing та Intelligence-Led Policing, які передбачають використання комплексного аналізу даних як основи стратегічного, тактичного та оперативного управління правоохоронною діяльністю. Реалізація таких підходів потребує інтеграції можливостей штучного інтелекту, кримінального аналізу, OSINT, цифрової криміналістики, геоінформаційних технологій, систем підтримки прийняття рішень та інших сучасних інформаційно-комунікаційних технологій у межах єдиного цифрового середовища. Лише за таких умов цифрова трансформація набуде системного характеру та стане не окремим напрямом модернізації, а фундаментальною основою функціонування правоохоронних органів України.

Висновки. Узагальнення результатів дослідження дає підстави стверджувати, що цифрова трансформація правоохоронних органів є якісно новим етапом їх розвитку, який не може бути ототожнений з інформатизацією або цифровізацією. Її сутність полягає у системній зміні організаційної архітектури, механізмів інформаційної взаємодії та моделей прийняття рішень шляхом формування інтегрованої цифрової правоохоронної екосистеми, у межах якої інформаційні ресурси, цифрові технології та аналітичні інструменти функціонують узгоджено.

У результаті дослідження обґрунтовано доцільність розширеного розуміння інформаційно-комунікаційних технологій у правоохоронній діяльності. Запропоновано визначати їх як інтегровану сукупність цифрових технологій, інформаційних систем, програмно-апаратних комплексів, телекомунікаційних засобів, аналітичних платформ і цифрових сервісів, які забезпечують безперервний цикл формування, накопичення, інтеграції, оброблення, аналізу, візуалізації, передачі та використання інформації для підтримки управлінських, оперативно-службових, опера-

тивно-розшукових і процесуальних рішень. Принципова відмінність запропонованого підходу полягає у зміщенні акценту з технологічної природи ІКТ на їх інтеграційне та функціональне значення для правоохоронної діяльності.

Обґрунтовано, що концептуальною основою подальшої цифрової модернізації має стати формування цифрової правоохоронної екосистеми як цілісного інформаційно-аналітичного середовища, у якому інформаційні ресурси та реєстри, інформаційно-комунікаційна інфраструктура, аналітичні технології, інструменти OSINT, технології штучного інтелекту, цифрова криміналістика, геоінформаційні системи, системи підтримки прийняття рішень та засоби кібербезпеки функціонують як взаємопов'язані компоненти. Ефективність такої екосистеми визначається не кількістю впроваджених технологічних рішень, а якістю інформаційних, технологічних та аналітичних взаємозв'язків між ними.

Встановлено, що інформаційно-комунікаційні технології у сучасній правоохоронній діяльності виконують взаємопов'язані інформаційну, інтеграційну, аналітичну, прогностичну та координаційну функції. Їх комплексна реалізація забезпечує перехід від накопичення розрізнених відомостей до формування аналітичного знання, оцінювання ризиків, прогнозування тенденцій розвитку криміногенної ситуації та інформаційно-аналітичної підтримки стратегічних, тактичних і оперативних рішень. У цьому контексті ключовою умовою подальшої цифрової трансформації визначено забезпечення інтероперабельності інформаційних ресурсів, що має охоплювати не лише технічну сумісність систем, а і стандартизацію форматів даних, уніфікацію процедур інформаційного обміну, узгоджене управління даними та нормативне забезпечення міжвідомчої взаємодії.

Перспективи подальшого розвитку цифрової трансформації правоохоронних органів України пов'язані з удосконаленням інтегрованих інформаційних ресурсів, розвитком аналітичних платформ, розширенням можливостей кримінального аналізу, цифрової криміналістики та OSINT, відповідальним упровадженням технологій штучного інтелекту, а також поступовою імплементацією підходів Data-Driven Policing та Intelligence-Led Policing. Водночас технологічна модернізація повинна супроводжуватися розвитком цифрових компетентностей працівників, належним управлінням даними, забезпеченням кіберстійкості та формуванням правових механізмів захисту прав і свобод людини в умовах використання алгоритмічних і автоматизованих систем.

Подальші наукові дослідження доцільно спрямувати на розроблення організаційно-функціональної моделі цифрової правоохоронної екосистеми України, визначення критеріїв оцінювання цифрової зрілості правоохоронних органів, формування методики оцінювання ефективності інтегрованих інформаційно-аналітичних платформ та дослідження правових і етичних меж застосування технологій штучного інтелекту у правоохоронній діяльності.

Список використаних джерел

1. Василенко В. М. Цифрова трансформація правоохоронних органів: ризики в умовах гібридних загроз та шляхи їх подолання. *Вісник Кримінологічної асоціації України.* 2024. № 2 (32). С. 945–958. DOI: https://doi.org/10.32631/vca.2024.2.74

2. Моргунова Т. І. Інформаційно-комунікаційні технології у правозастосуванні: сучасні виклики та перспективи. *Актуальні питання у сучасній науці.* 2025. № 3(33). С. 613–628. DOI: https://doi.org/10.52058/2786-6300-2025-3(33)-613-628

3. Жученко О. Д. Вплив сучасних інформаційних технологій на діяльність правоохоронних органів: основні тенденції та ризики. *Науковий вісник Ужгородського національного університету. Серія : Право*. 2024. Вип. 86. Ч. 5. С. 59–65. DOI: https://doi.org/10.24144/2307-3322.2024.86.5.8

4. Крупа А. Г., Мар'єнко В. Ю. Вплив інформаційно-комунікаційних технологій (ІКТ) на цифрову трансформацію суспільства: соціально-філософський аналіз. *Освітній дискурс :* збірник наукових праць. 2025. Т. 52, № 1–2. С. 53–60. DOI: https://doi.org/10.33930/ed.2019.5007.52(1-2)-7

5. Реалізація філософії «Intelligence-led Policing» в системі кримінального аналізу Національної поліції України : монографія / О. Є. Користін, Д. В. Швець, Б. Бутко, Б. Денисенко та ін. ; за заг. ред. О. Є. Користіна. Київ : ВАІТЕ, 2024.444 с.

6. Ісмайлов К. Ю. Теоретико-правові підходи до проблем інформаційно-аналітичної діяльності Національної поліції на сучасному етапі державотворення. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2020. № 1 (104). С. 306–318.

7. Мовчан А. В. Актуальні проблеми впровадження в органах Національної поліції України моделі поліцейської діяльності, керованої аналітикою. *Соціально-правові студії*. 2018. Вип. 1. С. 17–22.

8. Uzlov D., Vlasov O., Strukov V. Using Data Mining for Intelligence-Led Policing and Crime Analysis. *International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T).* 2018. P. 499–502. DOI: https://doi.org/10.1109/INFOCOMMST.2018.8632122

9. Рибка Д. OSINT у забезпеченні національної безпеки. *Науковий вісник Ужгородського національного університету. Серія : Право.* 2025. Вип. 91. Ч. 4. С. 431–437. DOI: https://doi.org/10.24144/2307-3322.2025.91.4.59

10. Думчиков М. О. Відкрита розвідка (OSINT) у протидії інформаційним війнам: аналітичні інструменти та правові межі. *Аналітично-порівняльне правознавство.* 2025. № 6. Ч. 2. С. 273–277. DOI: https://doi.org/10.24144/2788-6018.2025.06.2.43

11. Про затвердження Положення про єдину інформаційну систему Міністерства внутрішніх справ та переліку пріоритетних електронних інформаційних ресурсів її суб'єктів : Постанова Кабінету Міністрів України; Положення, Перелік від 14.11.2018 № 1024. *База даних «Законодавство України»* / *Верховна Рада України*. URL: https://zakon.rada.gov.ua/go/1024-2018-п (дата звернення: 06.07.2026).

12. Про затвердження Положення про інформаційно-комунікаційну систему «Інформаційний портал Національної поліції України» : Наказ; МВС України від 03.08.2017 № 676. *База даних «Законодавство України»* / *Верховна Рада України*. URL: https://zakon.rada.gov.ua/go/z1059-17 (дата звернення: 06.07.2026).

13. Europol. AI and Policing: The Benefits and Challenges of Artificial Intelligence for Law Enforcement. Luxembourg : Publications Office of the European Union, 2024. URL: https://www.europol.europa.eu/publication-events/main-reports/ai-and-policing?utm_source=chatgpt.com (дата звернення: 06.07.2026).

14. INTERPOL. Scanning for the Future(s) of Policing: First Steps Towards a New Global Paradigm. INTERPOL Working Paper. Lyon : International Criminal Police Organization – INTERPOL, 2022. URL: https://www.interpol.int/content/download/18111/file/INTERPOL%20Working%20Paper%20on%20the%20Future%20of%20Policing-EN-22062022.pdf?utm_source=chatgpt.com (дата звернення: 06.07.2026).

References

1. Vasylenko, V. M. (2024). Tsyfrova transformatsiia pravookhoronnykh orhaniv: Ryzyky v umovakh hibrydnykh zahroz ta shliakhy yikh podolannia [Digital transformation of law enforcement agencies: Risks under hybrid threats and ways to overcome them]. *Visnyk Kryminolohichnoi asotsiatsii Ukrainy – Bulletin of the Criminological Association of Ukraine*, 32(2), 945–958. DOI: https://doi.org/10.32631/vca.2024.2.74 [in Ukrainian].
2. Morhunova, T. I. (2025). Informatsiino-komunikatsiini tekhnolohii u pravozastosuvanni: Suchasni vyklyky ta perspektyvy [Information and communication technologies in law enforcement: Current challenges and prospects]. *Aktualni pytannia u suchasnii nautsi – Current Issues in Modern Science*, 3(33), 613–628. DOI: https://doi.org/10.52058/2786-6300-2025-3(33)-613-628 [in Ukrainian].
3. Zhuchenko, O. D. (2024). Vplyv suchasnykh informatsiinykh tekhnolohii na diialnist pravookhoronnykh orhaniv: Osnovni tendentsii ta ryzyky [The impact of modern information technologies on the activities of law enforcement agencies: Main trends and risks]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: Pravo – Uzhhorod National University Herald. Series: Law*, 86(5), 59–65. DOI: https://doi.org/10.24144/2307-3322.2024.86.5.8 [in Ukrainian].
4. Krupa, A. H., & Marienko, V. Yu. (2025). Vplyv informatsiino-komunikatsiinykh tekhnolohii (IKT) na tsyfrovu transformatsiiu suspilstva: Sotsialno-filosofskyi analiz [The impact of information and communication technologies (ICT) on the digital transformation of society: A socio-philosophical analysis]. *Osvitnii dyskurs: Zbirnyk naukovykh prats – Educational Discourse: Collection of Scientific Papers*, 52(1–2), 53–60. DOI: https://doi.org/10.33930/ed.2019.5007.52(1-2)-7 [in Ukrainian].
5. Korystin, O. Ye. (Ed.). (2024). Realizatsiia filosofii "Intelligence-led Policing" v systemi kryminalnoho analizu Natsionalnoi politsii Ukrainy: Monohrafiia [Implementation of the "Intelligence-Led Policing" philosophy in the criminal analysis system of the National Police of Ukraine: Monograph]. VAITE. DOI: https://doi.org/10.36486/978-966-2310-66-5 [in Ukrainian].
6. Ismailov, K. Yu. (2020). Teoretyko-pravovi pidkhody do problem informatsiino-analitychnoi diialnosti Natsionalnoi politsii na suchasnomu etapi derzhavotvorennia [Theoretical and legal approaches to the problems of information and analytical activities of the National Police at the current stage of state-building]. *Naukovyi visnyk Dnipropetrovskoho derzhavnoho universytetu vnutrishnikh sprav –Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs*, 1(104), 306–318 [in Ukrainian].
7. Movchan, A. V. (2018). Aktualni problemy vprovadzhennia v orhanakh Natsionalnoi politsii Ukrainy modeli politseiskoi diialnosti, kerovanoi analitykoiu [Current issues of implementing the Intelligence-Led Policing model in the National Police of Ukraine]. *Sotsialno-pravovi studii – Social and Legal Studios*, 1(1), 17–22. DOI: https://doi.org/10.32518/2617-4162-2018-1-17-22 [in Ukrainian].
8. Uzlov, D., Vlasov, O., & Strukov, V. (2018). Using data mining for Intelligence-Led Policing and crime analysis. In 2018 *International Scientific-Practical Conference Problems of Infocommunications: Science and Technology (PIC S&T)* (pp. 499–502). IEEE. DOI: https://doi.org/10.1109/INFOCOMMST.2018.8632122 [in English].
9. Rybka, D. (2025). OSINT u zabezpechenni natsionalnoi bezpeky [OSINT in ensuring national security]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: Pravo – Uzhhorod National University Herald. Series: Law*, 91(4), 431–437. DOI: https://doi.org/10.24144/2307-3322.2025.91.4.59 [in Ukrainian].
10. Dumchykov, M. O. (2025). Vidkryta rozvidka (OSINT) u protydii informatsiinym viinam: Analitychni instrumenty ta pravovi mezhi [Open-source intelligence (OSINT) in countering information warfare: Analytical tools and legal boundaries]. *Analitychno-porivnialne pravoznavstvo – Analytical and Comparative Jurisprudence*, 6(2), 273–277. DOI: https://doi.org/10.24144/2788-6018.2025.06.2.43 [in Ukrainian].
11. Cabinet of Ministers of Ukraine. (2018, November 14). Pro zatverdzhennia Polozhennia pro yedynu informatsiinu systemu Ministerstva vnutrishnikh sprav ta pereliku priorytetnykh elektronnykh informatsiinykh resursiv yii subiektiv [On approval of the Regulation on the Unified Information System of the Ministry of Internal Affairs and the list of priority electronic information resources of its entities] (Resolution No. 1024). *Verkhovna Rada of Ukraine*. Retrieved from https://zakon.rada.gov.ua/go/1024-2018-п
12. Ministerstvo vnutrishnikh sprav Ukrainy. (2017, August 3). Pro zatverdzhennia Polozhennia pro informatsiino-komunikatsiinu systemu "Informatsiinyi portal Natsionalnoi politsii Ukrainy" [On approval of the Regulation on the information and communication system "Information Portal of the National Police of Ukraine"] (Order No. 676). *Verkhovna Rada of Ukraine*. Retrieved from https://zakon.rada.gov.ua/go/z1059-17 [in Ukrainian].
13. Europol. (2024). AI and policing: The benefits and challenges of artificial intelligence for law enforcement. Publications Office of the European Union. Retrieved from https://www.europol.europa.eu/publication-events/main-reports/ai-and-policing [in English].
14. INTERPOL. (2022). Scanning for the future(s) of policing: First steps towards a new global paradigm (INTERPOL Working Paper). International Criminal Police Organization. Retrieved from https://www.interpol.int/content/download/18111/file/INTERPOL%20Working%20Paper%20on%20the%20Future%20of%20Policing-EN-22062022.pdf [in English].

Haborets Olha,
PhD in Education, Associate Professor
(Donetsk State University of Internal Affairs, Kropyvnytskyi)
ORCID: https://orcid.org/0000-0002-7138-5847

Lunhol Olha,
Candidate of Pedagogical Sciences, Associate Professor
(Donetsk State University of Internal Affairs, Kropyvnytskyi)
ORCID: https://orcid.org/0000-0001-8128-0072

ISSN 2709-9261 (Print), ISSN 2709-927X (Online)

INFORMATION AND COMMUNICATION TECHNOLOGIES AS A COMPONENT OF THE DIGITAL TRANSFORMATION OF LAW ENFORCEMENT AGENCIES IN UKRAINE

The article investigates the role of information and communication technologies (ICT) in the digital transformation of law enforcement agencies in Ukraine within the context of rapid technological development, increasing cyber threats, and the growing digitalization of public administration. The relevance of the study is determined by the need to reconsider the place of ICT in modern law enforcement, where digital technologies have evolved beyond auxiliary technical tools and now serve as the technological foundation of an integrated digital law enforcement ecosystem.

The purpose of the study is to examine the role of ICT in the digital transformation of Ukrainian law enforcement agencies, to substantiate their significance as the core integrating component of the digital law enforcement ecosystem, to identify its structural elements and functional relationships, and to determine the key directions for improving information and analytical support for law enforcement activities.

The research is based on a combination of general scientific and special legal methods, including analysis, synthesis, the systemic approach, comparative legal analysis, and the functional method. The study analyses current Ukrainian legislation, international approaches to digital policing, and contemporary scientific research on digital transformation, criminal intelligence analysis, Intelligence-Led Policing, open-source intelligence (OSINT), artificial intelligence, digital forensics, and information support for law enforcement agencies.

The findings substantiate an expanded understanding of ICT as an integrated system of digital technologies, information resources, analytical platforms, software and hardware solutions, communication infrastructure, and decision-support tools that ensure the collection, integration, processing, analysis, exchange, visualization, and practical use of information in managerial, operational, investigative, and procedural activities. The article proposes a conceptual model of a digital law enforcement ecosystem comprising interconnected information resources, communication infrastructure, analytical technologies, artificial intelligence, OSINT, digital forensics, geospatial technologies, cybersecurity mechanisms, and decision-support systems.

The study demonstrates that the effectiveness of digital transformation depends not on the implementation of isolated digital solutions but on ensuring interoperability between information systems and the integration of technological, organizational, and analytical components into a unified information environment. Particular attention is paid to the role of the Unified Information System of the Ministry of Internal Affairs of Ukraine and the Information Portal of the National Police of Ukraine as key components of the national digital law enforcement infrastructure.

The novelty of the study lies in substantiating a systemic approach to ICT as the conceptual and technological foundation of the digital transformation of law enforcement agencies. Unlike existing studies that mainly focus on individual digital technologies, the proposed approach considers ICT as an integrated mechanism that ensures the effective interaction of all components of the digital law enforcement ecosystem.

The practical value of the research lies in the possibility of applying the proposed conceptual approaches to improving information and analytical support, strengthening interoperability between law enforcement information systems, enhancing digital capabilities, and implementing advanced analytical technologies in the activities of Ukrainian law enforcement agencies.

Key words: *information and communication technologies, digital transformation, law enforcement agencies, digital law enforcement ecosystem, information and analytical support, interoperability, Intelligence-Led Policing, open-source intelligence (OSINT).*

Дата першого надходження статті до видання: 16.07.2026
Дата прийняття статті до друку після рецензування: 03.08.2026
Дата публікації (оприлюднення) статті: 14.10.2026