УДК 351.74:004.5
DOI https://doi.org/10.32689/3083-7731-2026-2(38)-31-37

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

Григоренко О. О., Архіпов В. І.

SPECIFICS OF THE APPLICATION OF INFORMATION TECHNOLOGIESIN THE ACTIVITIES OF LAW ENFORCEMENT AGENCIES

Oleksandr Hryhorenko, Valerii Arkhipov

Анотація

У статті досліджено особливості застосування сучасних інформаційних технологій у діяльності правоохоронних органів в умовах цифрової трансформації суспільства. Розглянуто основні напрями використання інформаційних систем, баз даних, систем відеоспостереження та розпізнавання облич, біометричних технологій, інструментів BigData, геоінформаційних систем, цифрової криміналістики та технологій штучного інтелекту.

Проаналізовано значення цифрових технологій для інформаційно-аналітичного забезпечення правоохоронної діяльності, підвищення оперативності реагування на правопорушення, пошуку та аналізу інформації, виявлення закономірностей і встановлення обставин кримінальних правопорушень.

Окрему увагу приділено використанню цифрових доказів, автоматизованих систем аналізу даних та сучасних засобів електронної взаємодії між правоохоронними органами. Визначено основні переваги цифровізації, серед яких підвищення ефективності роботи, скорочення часу на оброблення інформації, оптимізація використання ресурсів та вдосконалення міжвідомчої взаємодії.

Разом із тим досліджено проблемні аспекти застосування інформаційних технологій, зокрема ризики несанкціонованого доступу до інформації, порушення конфіденційності, незаконного використання персональних і біометричних даних, алгоритмічних помилок та недостатнього нормативно-правового регулювання окремих цифрових процесів.

Обґрунтовано необхідність комплексного підходу до впровадження інформаційних технологій у правоохоронну діяльність, що передбачає поєднання технологічного розвитку з належним правовим регулюванням, забезпеченням кібербезпеки, захистом прав і свобод людини та підвищенням рівня цифрової компетентності працівників правоохоронних органів.

Зроблено висновок, що подальша цифровізація правоохоронної сфери є важливою передумовою підвищення ефективності протидії сучасній злочинності та вдосконалення механізмів забезпечення громадської безпеки.

Ключові слова: *інформаційні технології, правоохоронні органи, цифровізація, інформаційно-аналітичне забезпечення, інформаційні системи, цифрові докази, цифрова криміналістика, кібербезпека, штучний інтелект, BigData, персональні дані, інформаційна безпека, електронний документообіг, цифрові технології, розслідування кримінальних правопорушень, захист інформації.*

Abstract

The article examines the specifics of applying modern information technologies in the activities of law enforcement agencies amid the digital transformation of society. It explores the key areas of application of information systems, databases, video surveillance and facial recognition systems, biometric technologies, Big Data tools, geographic information systems, digital forensics, and artificial intelligence technologies.

The significance of digital technologies for the information and analytical support of law enforcement activities, enhancing the speed of response to offenses, searching for and analyzing information, identifying patterns, and establishing the circumstances of criminal offenses is analyzed.

Particular attention is paid to the use of digital evidence, automated data analysis systems, and modern tools for electronic interaction between law enforcement agencies. The key benefits of digitalization are identified, including increased operational efficiency, reduced information processing time, optimized resource utilization, and improved interagency cooperation.

At the same time, the problematic aspects of applying information technologies are examined, particularly the risks of unauthorized access to information, breaches of confidentiality, the illicit use of personal and biometric data, algorithmic errors, and the lack of adequate legal regulation of certain digital processes.

The necessity of a comprehensive approach to implementing information technologies in law enforcement activities is substantiated. This approach entails combining technological development with appropriate legal regulation, ensuring cybersecurity, protecting human rights and freedoms, and enhancing the digital competence of law enforcement personnel.

It is concluded that the further digitalization of the law enforcement sector is a crucial prerequisite for enhancing the effectiveness of combating modern crime and improving mechanisms for ensuring public safety.

Key words: *information technologies, law enforcement agencies, digitalization, information and analytical support, information systems, digital evidence, digital forensics, cybersecurity, artificial intelligence, Big Data, personal data, information security, electronic document management, digital technologies, investigation of criminal offenses, information protection.*

1. Вступ. Сучасний етап розвитку суспільства характеризується стрімким поширенням інформаційних технологій у всіх сферах суспільного життя. Цифровізація державного управління, розвиток телекомунікаційних мереж, значне збільшення обсягів інформації та поширення кіберзлочинності зумовлюють необхідність постійного вдосконалення діяльності правоохоронних органів. У таких умовах інформаційні технології стають одним із важливих інструментів забезпечення громадської безпеки, протидії злочинності, розслідування кримінальних правопорушень та організації ефективної роботи правоохоронних підрозділів.

Сучасна правоохоронна діяльність все більше спирається на використання інформаційних технологій, які кардинально змінюють методи роботи органів правопорядку. Впровадження цифрових рішень, таких як штучний інтелект, біометрична ідентифікація, системи відеоспостереження та аналізу великих даних, сприяє підвищенню ефективності правоохоронних органів, швидкості розслідувань та точності ухвалення рішень. Проте разом із цими перевагами виникають і нові проблеми, пов'язані з правовими та етичними аспектами використання цифрових технологій у правозастосувальній сфері [1].

Метою дослідження є дослідження особливостей застосування сучасних інформаційних технологій у діяльності правоохоронних органів, визначення основних напрямів їх використання для підвищення ефективності правоохоронної діяльності, інформаційно-аналітичного забезпечення, попередження та розслідування кримінальних правопорушень, а також аналіз проблем і перспектив цифровізації правоохоронної сфери з урахуванням вимог інформаційної безпеки, захисту персональних даних та дотримання прав і свобод людини.

Аналіз останніх досліджень і публікацій. Проблематика застосування інформаційних технологій у діяльності правоохоронних органів останніми роками набуває особливої актуальності у зв'язку з активною цифровізацією державного управління, розвитком кіберзлочинності, поширенням електронних доказів та необхідністю підвищення ефективності правоохоронної діяльності. У науковій літературі досліджуються як загальні питання інформаційно-аналітичного забезпечення правоохоронних органів, так і окремі напрями використання цифрової криміналістики, штучного інтелекту, інформаційних систем та засобів кібербезпеки [2–11].

Значний внесок у дослідження інформаційно-аналітичного забезпечення правоохоронної діяльності зробив П. П. Латковський, який розглядає інформаційно-аналітичне забезпечення як важливу складову сучасної правоохоронної діяльності. Автор акцентує увагу на значенні баз даних, інформаційних технологій та міжнародного інформаційного обміну для підвищення ефективності роботи правоохоронних органів.

О. Д. Жученко досліджує вплив сучасних інформаційних технологій на діяльність правоохоронних органів та звертає увагу на їх значення для розкриття, розслідування і попередження кримінальних правопорушень. Науковець підкреслює, що цифрові технології сприяють автоматизації окремих слідчих процедур, підвищенню оперативності прийняття рішень та ефективності забезпечення громадської безпеки. Водночас серед основних ризиків визначаються проблеми безпеки даних, етичні питання та технологічна залежність.

Окремий напрям сучасних досліджень становить цифрова криміналістика. У наукових працях наголошується, що цифровізація суспільства призвела до збільшення кількості цифрових слідів та електронної інформації, яка може використовуватися під час кримінального провадження. Досліджуються питання виявлення, фіксації, вилучення, збереження та аналізу цифрових доказів, а також забезпечення їх допустимості та достовірності.

Важливе місце у сучасних публікаціях займає проблема використання штучного інтелекту. Останні дослідження демонструють можливості застосування штучного інтелекту для аналізу великих масивів даних, виявлення аномалій, прогнозування кіберзагроз та автоматизації ок-

ремих процесів інформаційної безпеки. Водночас дослідники звертають увагу на необхідність правового регулювання таких технологій, контролю за алгоритмічними рішеннями та запобігання порушенням прав людини.

В умовах цифровізації особливого значення набуває проблема захисту персональних даних та інформаційних прав людини. Д. Калюжний зазначає, що використання інформаційно-комунікаційних технологій правоохоронними органами, поряд із підвищенням ефективності їхньої діяльності, створює додаткові ризики для права на приватність та захист персональних даних. Автор обґрунтовує необхідність дотримання принципів законності, пропорційності та прозорості під час збирання, зберігання, передачі й використання інформації.

Сучасні дослідження також враховують специфіку функціонування правоохоронних органів України в умовах воєнного стану. Зокрема, науковці розглядають цифрову трансформацію правоохоронної системи у контексті гібридних загроз, кібератак та інформаційної агресії. Наголошується на необхідності одночасного розвитку цифрових спроможностей, кібербезпеки, правового регулювання та цифрової компетентності працівників правоохоронних органів.

Окремо досліджується правове забезпечення цифрової взаємодії правоохоронних органів. У новітніх наукових працях 2026 року аналізуються інформаційні електронні ресурси єдиної інформаційної системи МВС та рівні цифрової взаємодії правоохоронних органів, а також пропонуються підходи до систематизації відповідних цифрових відносин.

Таким чином, аналіз останніх досліджень і публікацій свідчить про формування комплексного наукового підходу до проблеми застосування інформаційних технологій у правоохоронній діяльності. Науковці переважно погоджуються, що цифрові технології підвищують оперативність, якість інформаційно-аналітичної роботи та ефективність розслідування правопорушень. Водночас недостатньо дослідженими залишаються питання комплексного поєднання технологічних можливостей із гарантіями прав людини, стандарти використання штучного інтелекту, уніфікація цифрових систем різних правоохоронних органів, підготовка кадрів та забезпечення належного захисту інформації. Саме ці аспекти потребують подальшого наукового осмислення та можуть становити перспективний напрям дослідження особливостей застосування інформаційних технологій у діяльності правоохоронних органів.

2. Матеріали та методи. Матеріальну основу дослідження становлять положення Конституції України, законів України, нормативно-правових актів Кабінету Міністрів України, інших актів законодавства, що регулюють суспільні відносини у сфері застосування інформаційних технологій у діяльності правоохоронних органів, забезпечення інформаційної та кібербезпеки, захисту інформації, а також міжнародно-правові акти, наукові праці вітчизняних і зарубіжних учених, матеріали судової практики та офіційні аналітичні документи органів державної влади.

Методологічну основу дослідження становить сукупність загальнонаукових і спеціально-юридичних методів, зокрема діалектичного, системно-структурного, формально-юридичного, порівняльно-правового, логіко-семантичного та методу правового моделювання. Їх застосування дало змогу комплексно дослідити особливості використання інформаційних технологій у діяльності правоохоронних органів, визначити сучасний стан і проблемні аспекти їх нормативно-правового регулювання, а також сформулювати пропозиції щодо вдосконалення правових та організаційних механізмів застосування інформаційних технологій у правоохоронній діяльності.

3. Результати та обговорення. Інформаційні технології у діяльності правоохоронних органів можна розглядати як сукупність технічних, програмних та організаційних засобів, призначених для збирання, зберігання, оброблення, пошуку, передачі та захисту інформації. Їх застосування спрямоване не лише на автоматизацію окремих процесів, а й на формування сучасної системи інформаційного забезпечення правоохоронної діяльності.

Одним із ключових напрямів використання інформаційних технологій є створення та функціонування інформаційно-аналітичних систем і баз даних.

Такі системи дають можливість накопичувати значні масиви відомостей, здійснювати їх швидкий пошук, систематизацію та аналіз. Для правоохоронних органів це має особливе значення, оскільки під час виконання службових завдань працівникам необхідно оперативно отримувати інформацію про осіб, події, транспортні засоби, документи, кримінальні правопорушення та інші обставини, що можуть мати доказове або оперативне значення.

Сучасні інформаційні технології – це сукупність методів, процесів та програмно-технічних засобів, які поєднані з метою збирання, обробки, зберігання, розповсюдження, відтворення і використання інформації у користувачів. Вони ма-

ють різні види, такі як технологія опрацювання даних, керування, підтримки прийняття рішень та експертних систем.

Основними тенденціями розвитку інформаційних технологій у правоохоронних органах є: 1) вдосконалення форм і методів управління системами інформаційного забезпечення; 2) централізація та інтеграція комп'ютерних банків даних; 3) впровадження новітніх комп'ютерних інформаційних технологій для ведення кримінологічних записів; 4) розвиток та широке використання ефективних та потужних комп'ютерних мереж; 5) використання спеціалізованих засобів захисту інформації; 6) встановлення ефективного обміну кримінологічною інформацією на міждержавному рівні [12].

До основних сучасних інформаційних технологій, які активно впроваджуються у діяльність правоохоронних органів, належать системи відеоспостереження та автоматизованого аналізу зображень, біометричні технології, інформаційно-аналітичні системи BigData, технології штучного інтелекту, цифрова криміналістика, геоінформаційні системи та засоби автоматизованого обміну даними.

Системи відеоспостереження та технології розпізнавання облич. Використання сучасних камер відеоспостереження дозволяє здійснювати постійний моніторинг об'єктів і територій, фіксувати події та оперативно реагувати на потенційно небезпечні ситуації. На відміну від традиційного відеоспостереження, сучасні системи можуть автоматично аналізувати відеопотоки, виявляти певні об'єкти або події, встановлювати часові та просторові взаємозв'язки між ними. Технології автоматизованого розпізнавання облич можуть застосовуватися для встановлення особи за наявними інформаційними базами, зокрема під час розшуку осіб або перевірки обставин правопорушення.

Водночас застосування таких технологій потребує особливої уваги до питань захисту приватності та персональних даних. Автоматизована ідентифікація особи не завжди забезпечує абсолютну точність, тому результати роботи алгоритмів мають перевірятися уповноваженими працівниками та використовуватися виключно в межах законодавчо визначених повноважень.

Біометричні технології та інформаційні бази даних. Важливим напрямом цифровізації правоохоронної діяльності є використання біометричної інформації для встановлення та підтвердження особи. До таких даних можуть належати відбитки пальців, параметри обличчя, голосові характеристики, характеристики райдужної оболонки ока та інші індивідуальні ознаки. Застосування автоматизованих біометричних систем дає можливість значно скоротити час ідентифікації особи та підвищити ефективність пошукових заходів.

Поєднання біометричної інформації з іншими інформаційними ресурсами дозволяє здійснювати комплексний аналіз відомостей про особу, встановлювати відповідність між різними інформаційними записами та сприяти розшуку осіб. При цьому особливого значення набувають питання законності отримання, зберігання, оброблення та передачі біометричних даних, оскільки вони належать до інформації, яка потребує підвищеного рівня захисту.

Технології BigData та інформаційно-аналітичні системи. Діяльність правоохоронних органів пов'язана з обробленням значних обсягів різноманітної інформації. Це можуть бути відомості про кримінальні правопорушення, результати оперативно-розшукової діяльності, матеріали кримінальних проваджень, дані відеоспостереження, інформація з відкритих джерел, географічні відомості та інші цифрові дані. Технології BigData дозволяють об'єднувати та структурувати значні масиви інформації, здійснювати їх швидкий пошук і виявляти взаємозв'язки, які складно встановити шляхом традиційного аналізу.

Варто зауважити, що застосування таких інструментів сприяє виявленню повторюваних моделей поведінки, встановленню зв'язків між особами та подіями, аналізу криміногенної ситуації на певній території та формуванню інформаційної основи для прийняття управлінських рішень. Водночас ефективність BigData безпосередньо залежить від якості вихідних даних, їх актуальності, достовірності та належного захисту.

Штучний інтелект і машинне навчання. Одним із найбільш перспективних напрямів розвитку інформаційних технологій у правоохоронній сфері є використання штучного інтелекту. Алгоритми машинного навчання здатні обробляти великі обсяги інформації та виявляти статистичні закономірності, які можуть бути використані для аналізу криміногенної ситуації, виявлення підозрілих операцій, класифікації інформації та прогнозування певних ризиків.

Штучний інтелект також може використовуватися для автоматизованого аналізу документів, текстових повідомлень, зображень та відеоматеріалів, що дозволяє скоротити час виконання окремих операцій і зменшити навантаження на працівників. Разом із тим використання алгоритмічних систем у правоохоронній діяльності має

супроводжуватися належним контролем, оскільки результати автоматизованого аналізу можуть містити помилки або відображати упередження, присутні у вихідних даних.

Геоінформаційні технології. Значний потенціал для правоохоронної діяльності мають геоінформаційні системи (GIS), які забезпечують можливість аналізувати інформацію з урахуванням її географічного розташування. За допомогою таких систем можна відображати на електронних картах місця вчинення правопорушень, аналізувати їх територіальну концентрацію, визначати криміногенні зони та планувати розміщення сил і засобів правоохоронних органів.

Геоінформаційний аналіз дозволяє виявляти просторові закономірності та оцінювати зміни криміногенної ситуації протягом певного періоду. Це може використовуватися для планування патрулювання, розподілу ресурсів і визначення пріоритетних напрямів профілактичної роботи.

Цифрова криміналістика. В умовах активного використання цифрових пристроїв особливого значення набувають технології цифрової криміналістики. Вони застосовуються для виявлення, фіксації, вилучення, збереження та дослідження цифрової інформації, яка може мати значення для кримінального провадження. Об'єктами дослідження можуть бути комп'ютери, мобільні телефони, електронні носії інформації, системи відеоспостереження та інші цифрові пристрої.

Застосування спеціалізованого програмного забезпечення дає можливість відновлювати видалені дані, аналізувати метадані, встановлювати часові послідовності цифрових подій та виявляти інші відомості, які можуть сприяти встановленню обставин правопорушення. Водночас робота з цифровими доказами повинна здійснюватися з дотриманням установлених процедур, оскільки порушення порядку їх отримання або збереження може вплинути на можливість подальшого використання відповідної інформації.

Хмарні технології та електронний обмін інформацією. Перспективним напрямом є використання хмарних технологій для зберігання та оброблення інформації, а також створення захищених систем електронної взаємодії між різними підрозділами та державними органами. Це дозволяє забезпечувати швидкий доступ уповноважених працівників до необхідної інформації незалежно від їхнього місця перебування та сприяє оперативному обміну даними.

Отже, інформаційні технології відіграють важливу роль у процесі розкриття та розслідування кримінальних правопорушень. Використання сучасних програмних засобів дає змогу аналізувати великі обсяги інформації, встановлювати взаємозв'язки між окремими подіями та особами, виявляти закономірності у злочинній діяльності. Інструменти цифрової аналітики можуть сприяти формуванню версій щодо обставин правопорушення та визначенню напрямів подальшого розслідування.

Особливого значення набувають технології роботи з цифровими доказами. У сучасних умовах значна частина інформації, яка може мати доказове значення, створюється та зберігається в електронній формі. Йдеться про електронні документи, дані мобільних пристроїв, записи камер відеоспостереження, інформацію з комп'ютерних систем, електронне листування та інші цифрові дані. Їх виявлення, вилучення, збереження та дослідження потребують використання спеціальних технічних і програмних засобів, а також дотримання встановлених законодавством процедур.

Окремої уваги потребує питання кібербезпеки. Збільшення кількості інформаційних систем і обсягів даних одночасно створює нові ризики. Правоохоронні органи самі можуть ставати об'єктами кібератак, несанкціонованого доступу, викрадення або знищення інформації. Тому ефективне застосування інформаційних технологій неможливе без належного рівня технічного та організаційного захисту інформаційних ресурсів.

Забезпечення інформаційної безпеки передбачає використання сучасних засобів автентифікації, шифрування, резервного копіювання, контролю доступу та моніторингу інформаційних систем. Водночас важливим елементом захисту є підготовка персоналу. Навіть найсучасніші технічні засоби не можуть повністю гарантувати безпеку інформації, якщо працівники не дотримуються встановлених правил роботи з інформаційними ресурсами.

Однією з основних проблем цифровізації правоохоронної діяльності є необхідність забезпечення балансу між ефективністю використання інформаційних технологій та дотриманням прав людини. Оброблення персональних даних, використання систем відеоспостереження, аналіз електронної інформації та застосування автоматизованих систем повинні здійснюватися відповідно до принципів законності, необхідності, пропорційності та належного захисту інформації.

Іншою проблемою є недостатній рівень цифрової компетентності окремих працівників. Швидкий розвиток технологій вимагає постійного професійного навчання та підвищення кваліфікації. Працівник правоохоронного органу повинен не лише вміти користуватися інфор-

маційними системами, а й розуміти принципи інформаційної безпеки, правила роботи з цифровими доказами, особливості захисту персональних даних та ризики, пов'язані з використанням сучасних цифрових інструментів.

Важливою умовою ефективної цифровізації є також сумісність інформаційних систем різних правоохоронних органів. Наявність розрізнених баз даних та систем, які не забезпечують належного обміну інформацією, може знижувати оперативність реагування та створювати додаткове навантаження на працівників. Тому перспективним завданням є розвиток інтегрованого інформаційного середовища, у якому обмін даними здійснюється швидко, безпечно та на законних підставах.

Таким чином, інформаційні технології є невід'ємною складовою сучасної правоохоронної діяльності. Їх використання сприяє підвищенню оперативності роботи, покращенню інформаційно-аналітичного забезпечення, ефективнішому розслідуванню правопорушень, розвитку електронного документообігу та вдосконаленню взаємодії з громадянами. Водночас цифровізація створює нові виклики, пов'язані із захистом інформації, кібербезпекою, конфіденційністю персональних даних та дотриманням прав людини.

4. Висновки. Перспективи подальшого розвитку інформаційних технологій у діяльності правоохоронних органів пов'язані з поглибленням цифрової трансформації, інтеграцією інформаційних ресурсів, удосконаленням технологій штучного інтелекту, цифрової криміналістики та аналітичних систем. Водночас їх ефективне використання потребує не лише технічного забезпечення, а й формування належної нормативно-правової бази, підвищення цифрової компетентності працівників та впровадження дієвих механізмів контролю за обробленням інформації. Особливого значення набуває забезпечення балансу між оперативністю та технологічною ефективністю правоохоронної діяльності, з одного боку, і гарантуванням законності, приватності та основоположних прав людини — з іншого. Саме комплексний підхід до цифровізації дозволить максимально реалізувати потенціал сучасних технологій та підвищити результативність протидії сучасним формам злочинності.

Отже, подальший розвиток інформаційних технологій у правоохоронній сфері має здійснюватися комплексно та ґрунтуватися на поєднанні технологічних інновацій, належного правового регулювання, професійної підготовки працівників і надійного захисту інформації. Саме такий підхід дозволить підвищити ефективність діяльності правоохоронних органів та забезпечити використання цифрових можливостей відповідно до принципів законності й верховенства права.

Конфлікт інтересів. Автор заявляє про відсутністьконфліктуінтересівщодопідготовки, написання та публікаціїцієї статті.

Фінансування. Дослідженняпроводилося без фінансовоїпідтримки.

Доступність даних. Дані, використані в дослідженні, отримані з відкритих офіційних джерел та з матеріалів, досліджених автором під час підготовки рукопису.

Використання засобів штучного інтелекту. У процесі підготовки цієї статті мовна модель штучного інтелекту ChatGPT (OpenAI, GPT-5.5) використовувалася виключно як допоміжний інструмент для мовно-стилістичного редагування, удосконалення структури викладу, технічного оформлення бібліографічних посилань і описів, а також підготовки англомовних складових статті, зокрема анотації та списку References. Окремі інструменти штучного інтелекту також застосовувалися для опрацювання деяких вступних положень, редакційного доопрацювання та стилістичного вдосконалення окремих частин рукопису.

Пошук, добір і критичне опрацювання наукових джерел, аналіз нормативно-правової бази, визначення авторських наукових положень, формулювання висновків і розроблення відповідних пропозицій здійснювалися авторами самостійно. Усі результати та матеріали, створені або відредаговані із застосуванням технологій штучного інтелекту, підлягали обов'язковій перевірці та верифікації шляхом їх зіставлення з положеннями чинного законодавства України, науковими працями, офіційними документами та матеріалами правозастосовної практики.

Застосування технологій штучного інтелекту в межах підготовки статті мало виключно допоміжний і редакційно-технічний характер. Воно не вплинуло на самостійність проведеного дослідження, його методологічні засади, зміст отриманих наукових результатів, а також не визначало та не змінювало авторських висновків і пропозицій.

Внесок авторів. Олександром Григоренком здійснено основний обсяг дослідження особливостей застосування інформаційних технологій у діяльності правоохоронних органів, проведено аналіз нормативно-правового регулювання, наукових джерел та практики використання інформаційно-технологічних засобів у правоохоронній діяльності, визначено основні напрями й особливості їх застосування, сформульовано теоретичні положення, висновки та пропозиції щодо вдосконалення правових і організаційних механізмів використання інформаційних техно-

логій у діяльності правоохоронних органів.

Валерієм Архіповим здійснено наукове консультування дослідження, визначено концептуальні засади та методологічні підходи до розгляду проблематики, проведено наукове редагування та уточнення окремих положень статті з позицій адміністративного права, забезпечено відповідність сформульованих висновків загальним засадам юридичної науки.

Усіма авторами погоджено остаточну редакцію статті та підтверджено відповідальність за зміст проведеного дослідження.

References:

1. Morhunova, T. I. (n.d.). Ethical challenges and legal regulation of the use of information technologies in law enforcement activities. [PDF].
2. Latkovskyi, P. P. (2025). Information and analytical support for law enforcement activities. *Scientific Bulletin of Uzhhorod National University. Series: Law, 90*, 61–66. https://doi.org/10.24144/2307-3322.2025.90.5.61
3. Zhuchenko, O. D. (2024). The impact of modern information technologies on the activities of law enforcement agencies: Key trends and risks. *Scientific Bulletin of Uzhhorod National University. Series: Law, 86*, 53–58. https://doi.org/10.24144/2307-3322.2024.86.5.8
4. Hora, I. V., Kolesnyk, V. A., & Popovych, I. I. (2024). Digital forensics in supporting crime counteraction activities. *Scientific Bulletin of Uzhhorod National University. Series: Law*.
5. Ryzhkov, E. V., Synitsina, Yu. P., Prokopov, S. O., et al. (2024). *Information and analytical support for law enforcement activities: Study guide*. Dnipropetrovsk State University of Internal Affairs.
6. Skrypnyk, A. V. (n.d.). *The use of digital information in criminal procedural proof: Monograph*. Pravo.
7. Stepaniuk, R. L. (2026). Digital forensic intelligence: Concept and prospects for development. *Law and Security, 1*(100), 34–45. https://doi.org/10.32631/pb.2026.1.03
8. Matsyborska, O. M. (2026). Challenges of implementing artificial intelligence-based information systems in the activities of law enforcement agencies. *Analytical and Comparative Jurisprudence, 1*. https://doi.org/10.24144/2788-6018.2026.01.3.14
9. Shopina, I. M. (2026). Use of artificial intelligence technologies by law enforcement entities: Aspects of legal regulation. *Central Ukrainian Bulletin of Law and Public Administration, 1*. https://doi.org/10.32782/cuj-2026-1-16
10. Bondarenko, O. H. (2026). Digital evidence in Ukrainian criminal proceedings: Issues of admissibility and assessment. *Central Ukrainian Bulletin of Law and Public Administration, 1*. https://doi.org/10.32782/cuj-2026-1-2
11. Hlynska, N. V. (Ed.). (2024). *Conceptual foundations of the digitalization of criminal proceedings in Ukraine: A monograph*. Pravo. https://doi.org/10.31359/9786178612139
12. *General characteristics of modern information technologies in law enforcement activities*. (n.d.). Zhytomyr Polytechnic. https://learn.ztu.edu.ua

ВІДОМОСТІ ПРО АВТОРІВ

Григоренко Олександр Олександрович
викладач кафедри кримінології та інформаційних технологій
Національної академії внутрішніх справ
e-mail: sss_angel@ukr.net
ORCID: 0009-0001-0106-9785

Архіпов Валерій Іванович
кандидат юридичних наук, доцент кафедри кримінології
Національної академії внутрішніх справ
e-mail: chpn1306@gmail.com
ORCID: 0000-0002-9942-9936

Oleksandr Hryhorenko
Lecturer at the Department of Criminology and Information Technologies, National Academy of Internal Affairs
e-mail: sss_angel@ukr/net
ORCID: 0009-0001-0106-9785

Valerii Arkhipov
Candidate of Legal Sciences,
Associate Professor at the Department of Criminology,
National Academy of Internal Affairs
e-mail: chpn1306@gmail.com
ORCID: 0000-0002-9942-9936

Дата надходження статті: 12.04.2026
Дата надходження виправленої версії статті: 23.06.2026
Дата прийняття статті: 21.07.2026
Дата публікації статті: 14.09.2026