УДК 347.96+007:004.7
DOI https://doi.org/10.24144/2307-3322.2024.86.5.8

ВПЛИВ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ НА ДІЯЛЬНІСТЬ ПРАВООХОРОННИХ ОРГАНІВ: ОСНОВНІ ТЕНДЕНЦІЇ ТА РИЗИКИ

Жученко О.Д.,
ORCID: 0009-0009-2795-7068
e-mail: olegzucenko@gmail.com

Жученко О.Д. Вплив сучасних інформаційних технологій на діяльність правоохоронних органів: основні тенденції та ризики.

Розглянуто цифрову трансформацію розкриття, розслідування та попередження кримінальних правопорушень, яка значною мірою впливає на слідчу діяльність та процес розслідування, змінює практики у сфері прийняття рішень. Доведено, що поява та розвиток інформаційних технологій багато в чому визначає виконання покладених на правоохоронні органи традиційних функцій, а також впливає на появу нових функцій. Зокрема майбутнє реалізації правоохоронними органами функції з розслідування кримінальних правопорушень багато в чому визначатиметься розвитком нової підгалузі криміналістики – цифрової криміналістики. Розглянуто появу нових концепцій функціонування правоохоронних органів, серед яких електронна поліція, віртуальна поліцейська ділянка та ін., як елементів електронного управління. Створення електронної поліції з точки зору ефективності та результативності має ґрунтуватися на етичних засадах, таких як повага до конфіденційності, підзвітність та прозорість. Визначено, що віртуальна поліцейська ділянка, як інноваційна новаторська технологічна платформа, оптимізує діяльність правоохоронних органів, пов'язує громадськість та правоохоронні органи через інтуїтивно зрозумілу платформу для повідомлення про злочини та доступ до послуг та багато іншого.

Доведено, що використання цифрових технологій та інформаційних систем підвищує ефективність правоохоронних органів та відкриває нові можливості запобігання злочинності, сприяє консультуванню та покращенню операційної ефективності, зокрема шляхом автоматизації слідчих процедур. Сучасні інформаційно-комунікаційні технології пропонують правоохоронним органам інструменти для оптимізації слідчих процесів, підвищення ефективності забезпечення ними громадської безпеки тощо. Однак, поряд з перевагами є ризики, серед яких порушення безпеки даних, етичні проблеми, технологічна залежність та ін. Стратегічне прогнозування, пов'язане з визначенням перспектив досудового розслідування і судового розгляду, моделюванням наслідків процесуальних рішень, що приймаються з використанням цифрових технологій і плануванням заходів щодо сучасного процесу доказування.

Ключові слова: цифрова трансформація, функції правоохоронних органів, цифрова криміналістика, електронна поліція, віртуальна поліцейська ділянка, штучний інтелект.

Zhuchenko O.D. Influence of modern information technologies on the activities of law enforcement agencies: main trends and risks.

The article considers the digital transformation of the disclosure, investigation and prevention of criminal offenses, which greatly affects the investigative activities and the investigation process, changes practices in the field of decision-making. It is proved that the emergence and development of information technologies largely determines the performance of traditional functions assigned to law enforcement agencies, and also affects the emergence of new functions. In particular, the future of implementation by law enforcement agencies of the function of investigating criminal offenses will largely be determined by the development of a new sub-branch of forensics – digital forensics. It has been considered the emergence of new concepts of functioning of law enforcement agencies, among which electronic police, virtual police station and others, as elements of electronic control. Creating e-policing in terms of efficiency and effectiveness should be based on ethical principles such as respect

for confidentiality, accountability and transparency. It is determined that the virtual police station, as an innovative innovatory technological platform, optimizes the activities of law enforcement agencies, connects the public and law enforcement agencies through an intuitive platform for reporting crimes and access to services and much more.

It is proved that the use of digital technologies and information systems increases the efficiency of law enforcement agencies and opens up new opportunities for crime prevention, facilitates counseling and improving operational efficiency, in particular by automating investigative procedures. Modern information and communication technologies offer law enforcement agencies tools to optimize investigative processes, increase the efficiency of ensuring public safety by them, etc. However, along with the advantages, there are risks, among which data security violations, ethical problems, technological dependence, etc. Strategic forecasting associated with determining the prospects for pre-trial investigation and trial, modeling the consequences of procedural decisions which are making using digital technologies, and planning measures for the modern evidence process.

Key words: digital transformation, functions of law enforcement agencies, digital forensics, electronic police, virtual police station, artificial intelligence.

Постановка проблеми. Цифрова трансформація розкриття, розслідування та попередження кримінальних правопорушень значною мірою впливає на слідчу діяльність та процес розслідування, змінює практики у сфері прийняття рішень. Досягнення у галузі ІТ надають правоохоронним органам інструменти та ресурси, необхідні для захисту громадян та розкриття кримінальних правопорушень – від сканування номерних знаків та камер спостереження до технологій керування даними, дозволяють повніше формувати доказову базу в розслідуванні кримінальних правопорушень [1, с. 53], забезпечують якість та ефективність судового розгляду матеріалів кримінальних справ за європейськими стандартами [2, с. 73] тощо.

Слід мати на увазі, що у майбутньому з розвитком інформаційно-телекомунікаційних технологій буде змінюватися та розширюватися зміст багатьох основоположних понять, наприклад, власності, від її матеріального контексту до нематеріального, і є вірогідним, що деякі традиційні обов'язки правоохоронних органів можуть змінитися або навіть зникнути, а повна автоматизація мобільних засобів контролю за дотриманням правил дорожнього руху може вплинути на регулятивно-контрольну функцію поліції в цій сфері.

Метою статті є розгляд трансформації основних функцій правоохоронних органів та їх структури, зумовлених розвитком інформаційно-телекомунікаційних технологій та цифровізацією.

Стан опрацювання проблематики. Проблематика упровадження сучасних інформаційних технологій у діяльність правоохоронних органів є предметом досліджень багатьох вітчизняних науковців, зокрема О. Домашенка, І. Катеринчука, А. Колодіної, А. Кубаєнка, В. Кудінова, А. Мовчана, С. Пєткова, В. Пядишева, О. Радутного, А. Столітнього, В. Шевчука, В. Шепітька, К. Ярового та ін., залишивши відкритими для подальших наукових розвідок низку теоретичних та практичних питань застосування цифрових інновацій у зазначеній сфері.

Виклад основного матеріалу. У найближчій перспективі правоохоронні органи виконуватимуть функції та завдання, які вони виконували і до початку цифрової ери. Наприклад, ст. 2 Закону України «Про Національну поліцію», до завдань поліції відносить «забезпечення публічної безпеки і порядку; охорону прав і свобод людини, а також інтересів суспільства і держави; протидію злочинності; надання в межах, визначених законом, послуг з допомоги особам, які з особистих, економічних, соціальних причин або внаслідок надзвичайних ситуацій потребують такої допомоги», виконання яких, відповідно до ч. 3 ст. 13, покладено на такі її структурні підрозділи, як «кримінальна поліція, патрульна поліція, органи досудового розслідування, поліція охорони, спеціальна поліція та поліція особливого призначення» [3]. Поділяємо думку В. М. Шевчука, який зазначає, що, враховуючи реалії воєнного стану, однією з найважливіших тенденцій кримінально-процесуальної науки та криміналістики є інтеграція знань, створення та впровадження інноваційних розробок, широке використання цифрових технологій та штучного інтелекту, спрямованих на вирішення завдань протидії злочинності та формування доказової бази [4, с. 203].

Щодо трансформації змісту прогностичної та профілактичної функцій правоохоронних органів під впливом розвитку інформаційно-комунікаційних технологій, зокрема поліції, то вона буде ще більшою мірою покладатися на великі дані та алгоритми для прогнозування злочинів та поведінки злочинців, особистості злочинців або жертв злочинів, що допоможе більш ефективно

використовувати ресурси для стримування злочинності та швидкого реагування на загрози, що виникають. При цьому слід брати до уваги два моменти: з одного боку, превентивна поліцейська діяльність може запобігати злочинності ефективніше, ніж традиційні поліцейські методи, а з іншого боку, існують ризики, пов'язані з конфіденційністю, відсутністю прозорості та ін. Зокрема патрулювання як вид превентивної поліцейської діяльності може дедалі більше доповнюватись або навіть замінюватись можливостями розподіленого зондування та дистанційного спостереження, які передбачають використання технологічних досягнень у таких галузях, як відеоспостереження, розпізнавання осіб, БПЛА, що розширить можливості співробітників правоохоронних органів та дозволить оптимізувати розподіл кадрів. Наприклад, у деяких розумних містах датчики дозволяють реагувати на постріли та швидше спрямовувати поліцейських на місце події.

Очевидним є те, що наукові досягнення надавали і чинитимуть значний вплив на криміналістику та судову експертизу. Майбутнє реалізації правоохоронними органами функції з розслідування кримінальних правопорушень багато в чому визначатиметься розвитком нової підгалузі криміналістики – цифрової криміналістики, яка «зосереджена на кримінально-процесуальному праві та доказах щодо комп'ютерів та пов'язаних з ними пристроїв» [5, с. 29]. Вона також розглядається як «прикладна наука про розкриття злочинів, пов'язаних з комп'ютерною інформацією, про дослідження цифрових доказів [6, с. 176], що являє собою «сукупність заздалегідь визначених процесів або завдань, які використовуються під час кримінального розслідування, з деякими особливостями технічної реалізації, схожими з традиційною криміналістикою, для управління та збору інформації про цифрові докази» [7, с. 1280]. В.М. Шевчук до предмета цифрової криміналістики відносить «закономірності виявлення, обліку, попереднього розслідування, використання комп'ютерної інформації, цифрові сліди та засоби їх обробки для вирішення завдань; виявлення, розкриття, розслідування та запобігання кримінальним злочинам, а також розробки на основі цього знання особливостей технічних засобів, методів та методичні рекомендації, спрямовані на оптимізацію діяльності з боротьби з кримінальними правопорушеннями у цифровому просторі» [4, с. 204].

Використання складних інструментів та технологій для збирання, аналізу та складання звітів за цифровими доказами заощаджує час та зусилля та гарантує захист даних від несанкціонованого доступу та потенційного неправомірного використання. Цифрова криміналістика повинна постійно адаптуватися до технологічних розробок та досягнень, щоб бути ефективною. У цифровій криміналістиці з'являються нові напрямки, наприклад хмарна криміналістика. Метою хмарної цифрової криміналістики є відновлення цифрових доказів та відтворення подій шляхом збирання та вивчення даних з хмарних платформ. Можливості програмного забезпечення для цифрової криміналістики щодо отримання даних з хмари в майбутньому будуть удосконалюватися [8]. Очікується, що ринок цифрової криміналістики зросте з 4,49 млрд. доларів США у 2020 році до 8,21 млрд. доларів США до 2026 року [7, с. 1281].

Посилюватиметься вплив інновацій у сфері судової експертизи на виконання правоохоронними органами своїх функцій, наприклад, наукових досягнень у галузі молекулярної фотопідбірки та геотегування за допомогою ізотопного виявлення. Молекулярна фотодобірка, також відома як фенотипування ДНК, може дозволити експертам-криміналістам визначити зовнішній вигляд людини на основі ДНК, залишеної на місці злочину – свого роду «біологічного свідка». Використання мікроРНК може поліпшити аналіз рідин, допомагаючи, наприклад, визначити, чи є рідина менструальною кров'ю чи кров'ю з рани. Завдяки ізотопному виявленню судово-медичні експерти можуть отримати нові засоби геомаркування, тобто визначення, наприклад, географічного походження наркотиків. Слід враховувати, що у подальшому збільшуватиметься розрив між традиційними методами судової експертизи та швидкістю технологічних інновацій і розробкою ефективних методів судової експертизи. Слідчі мають докладати зусиль до опанування новими технологіями шифрування даних, емпіричними даними і розподіленим зберіганням даних [9].

У нових технологічних реаліях відбувається переосмислення правоохоронними органами «своєї місії у сенсі їх комунікації з громадськістю» [10, с. 405; 11, с. 407]. Нині технологічні досягнення створюють нові можливості позитивної взаємодії громадськості та поліції, зокрема шляхом розширення онлайн-платформ для контактів із онлайн-спільнотою. Багатоканальна комунікація, у тому числі повідомлення про кримінальні правопорушення за допомогою різноманітних додатків, може підвищити рівень участі громадян у забезпеченні правопорядку. Цифрова

взаємодія також може бути доповнена автоматизованими чат-ботами та інструментами штучного інтелекту, що дозволяє поліції швидше та якісніше надавати послуги громадянам.

Розвиток технологій ставить на порядок денний появу нових концепцій функціонування правоохоронних органів, серед яких електронна поліція, віртуальна поліцейська ділянка та ін., як елементів електронного управління. У Конвенції про охорону нематеріальної культурної спадщини 2003 року зазначається, що загальною метою електронного управління є використання інформаційно-комунікаційних технологій для покращення надання послуг, сприяння громадянській активності та підвищення оперативності, послідовності та ефективності державного сектору [12]. Одним із досягнень у галузі електронного управління є електронна поліція – нова концепція інтернет-технологій, яка застосовується багатьма правоохоронними органами у багатьох країнах для покращення послуг з підтримки правопорядку, що надаються суспільству. Соціальні мережі є основним інструментом, який використовується правоохоронними органами для взаємодії з громадянами, зокрема у форматі 24/7. Наближення правоохоронних органів до громадськості за допомогою Інтернету та мобільних технологій надає багато переваг як правоохоронним органам, так і онлайн-спільноті.

Концепція електронної поліції – це використання технологій, які сприяють ефективній роботі поліції та моніторингу злочинності. Наприклад, система електронних ордерів – це система, де всі ордери на арешт документуються в електронному вигляді, щоб до них можна було отримати доступ через комп'ютери. Одним із проявів функціонування електронної поліції є практика подання заяв до поліції в онлайн-форматі, яка наразі є поширеною у багатьох країнах. Наприклад, система онлайн-подання заяв уже деякий час працює на Мальті, що стосується, здебільшого, кримінальних правопорушень невеликої тяжкості, які не потребують негайної присутності співробітника поліції. Однак, нею також можуть скористатися жертви серйозних злочинів, якщо вони бояться прийти до поліцейської дільниці. Співробітник поліції супроводжуватиме онлайн-заявника на кожному етапі та допоможе йому із правильним заповненням форм. Потім з ним зв'яжеться поліцейський через WhatsApp, Skype, Microsoft Teams, Google Meet або Facetime, аби уточнити деталі» [13].

Створення електронної поліції з точки зору ефективності та результативності має ґрунтуватися на етичних засадах, таких як повага до конфіденційності, підзвітність та прозорість. Щоб гарантувати, що програми електронної поліції реалізуються таким чином, щоб підтримувати цінності та принципи демократичного суспільства, політики та правоохоронні організації мають тісно співпрацювати з організаціями громадянського суспільства. Широке впровадження електронної поліцейської системи потребує забезпечення постійного навчання співробітників поліції. При цьому необхідно приділяти увагу питанням конфіденційності та безпеки, щоб гарантувати, що ці технології використовують таким чином, що сприяє зміцненню довіри та відкритості громадян.

Віртуальна поліцейська ділянка (VPS) – це інноваційна новаторська технологічна платформа, яка оптимізує діяльність правоохоронних органів, пов'язує громадськість та правоохоронні органи через інтуїтивно зрозумілу платформу для повідомлення про злочини та доступ до послуг та багато іншого. Це динамічне рішення посилює поліцейську діяльність у спільноті та сприяє спільному підходу до безпеки та захисту.

З точки зору ефективності та результативності, створення електронної поліції має ґрунтуватися на етичних засадах, таких як повага до конфіденційності, підзвітність та прозорість. Щоб гарантувати, що програми електронної поліції реалізуються саме таким чином, щоб підтримувати цінності та принципи демократичного суспільства, політики та правоохоронні організації мають тісно співпрацювати з організаціями громадянського суспільства. Широке упровадження електронної поліцейської системи потребує також забезпечення постійного навчання співробітників поліції, приділяючи особливу увагу питанням зміцненню довіри та відкритості громадян.

Віртуальна поліцейська ділянка (VPS) – це інноваційна новаторська технологічна платформа, яка оптимізує діяльність правоохоронних органів. Вона пов'язує громадськість та правоохоронні органи через інтуїтивно зрозумілу платформу для повідомлення про кримінальні правопорушення, шляхом доступу до послуг, що надаються поліцією, тощо. Віртуальні поліцейські дільниці вже існують у багатьох країнах, наприклад, у Швеції перша така ділянка була відкрита у 2000 році.

Наразі одним з найбільш обговорюваних напрямів впливу інформаційно-телекомунікаційних технологій на правову сферу загалом, та правоохоронну зокрема, є використання технології штучного інтелекту. Технології ШІ значною мірою перетворюють правоохоронну діяльність,

профілактику та виявлення кримінальних правопорушень. По суті, прийняття та використання ШІ правоохоронними органами – це не просто використання технологій, це переосмислення роботи поліції в цифрову епоху з чітким акцентом на підвищення суспільної безпеки за дотримання принципів справедливості та неупередженості, що лежать в основі функціонування демократичного суспільства.

Інтелектуальні алгоритми можуть аналізувати величезні обсяги даних, виявляючи закономірності та тенденції, які можуть спрямовувати дії правоохоронних органів, виявляти потенційні осередки злочинності та спільноти, що перебувають у зоні ризику, і навіть типи злочинів, найпоширеніших у певних сферах. Більше того, предиктивна поліція – одна з найефективніших додатків ШІ у правоохоронній діяльності, використовує можливість аналізу даних для прогнозування потенційних злочинних дій до того, як вони відбудуться. Як зазначає В. Г. Пядишев, «на відміну від традиційних методів, штучний інтелект пропонує динамічний підхід до розкриття кримінальних правопорушень використовуючи можливості аналізу даних, машинного навчання та розпізнавання образів, а здатність систем ШІ швидко обробляти величезні обсяги інформації, дозволяє правоохоронним органам виявляти закономірності, виявляти потенційних підозрюваних та активно запобігати злочинам» [10, с. 409]. Такі заходи можуть допомогти правоохоронним органам стати більш ефективними, зосередивши свої ресурси там, де вони найбільше потрібні. Виклики, з якими стикається українська правоохоронна та судова системи у воєнний час, зокрема «блокування чи ускладнення роботи установ на деокупованих та прифронтових територіях, нестача кадрів, велика кількість справ та ін.», значним чином підвищують ймовірність використання штучного інтелекту в Україні, при цьому сферу кримінальної юстиції «називають найменш перспективною для імплементації ШІ» [14, с. 33].

Перспективним інструментом для правоохоронних органів стає технологія безпілотних літальних апаратів зі штучним інтелектом, пропонуючи практичну та економічно ефективну альтернативу традиційним методам спостереження, таким як гелікоптери. Ці безпілотники забезпечують огляд потенційно нестабільних ситуацій із висоти пташиного польоту, допомагаючи правоохоронним органам приймати обґрунтовані рішення та відповідним чином реагувати. Однак використання такої технології не позбавлене протиріч, зокрема щодо порушення конфіденційності. Також наголошується на неконтрольованому використанні програмного забезпечення ШІ співробітниками поліції для моніторингу соціальних мереж громадян, що викликає ще більше занепокоєння з приводу конфіденційності.

Правоохоронні органи для прискорення розслідувань та потенційного запобігання кримінальним правопорушення дедалі частіше використовують системи розпізнавання осіб на базі штучного інтелекту та біометрію. Наприклад, ідентифікуючи людину, яка залишила відбиток пальця на місці злочину, поліція може швидко знайти підозрюваного та притягнути його до відповідальності. Однак поряд із очевидними перевагами ці технології також містять значні ризики, оскільки відсутність контролю людини за процесами прийняття рішень на технології ШІ порушує питання відповідальності. Наприклад, якщо ШІ дасть збій або прийме невірне рішення, залишається незрозумілим, хто за це відповідатиме – правоохоронні органи, черговий офіцер чи виробник таких програм?

Отже, інформаційно-телекомунікаційні технології сприяють удосконаленню роботи правоохоронних органів, однак вони містять багато ризиків, на що звертають увагу дослідники цієї проблематики.. Зокрема О. Е. Радутний, із посиланням на зарубіжних дослідників, звертає увагу на небезпеку критичних зловживань при «диктатурі» великих даних» у правоохоронній діяльності [15, с. 96]. Так, Ендрю Фергюсон наголошує, що «предиктивна поліція, спираючись на кореляції та алгоритми для прогнозування ймовірних місць скоєння злочинів, може бути як ефективною, так і проблематичною: з одного боку, вона є здатною допомогти правоохоронним органам більш ефективно розподіляти ресурси і потенційно запобігати правопорушенням, але з іншого боку, може підсилити упередження та дискримінацію, що має наслідком надмірний поліцейський нагляд в одних громадах і нестачу ресурсів в інших, вимагає підсилення прозорості, підзвітності та спирання на етичні міркування в кримінальному правосудді» [16]. Б. Гаркорт застерігає від того, що «використання великих даних у правоохоронній діяльності увічнює та посилює існуючу соціальну нерівність, замість того, щоб вирішувати її, піддає маргіналізовані групи підвищеному нагляду та дискримінації» [17]. До ризиків широкого використання технологій нагляду та прийняття рішень, в основу яких покладено великі данні, що може «загрожувати приватному життю та громадянським свободам, стати приводом для поглиблення расової та соціальної нерів-

ності, посилить існуючі упередження та дискримінації у зв'язку з їх недостатньою прозорістю та підзвітністю» [18], а також «призведе до посилення он-лайн переслідувань і злочинів на ґрунті ненависті» [19]. Отже, безконтрольне використання ШІ в правоохоронних та судових системах може мати негативні наслідки, зокрема містить загрозу безпеці даних, етичні та юридичні проблеми, підриває фундаментальні права людини, такі як право на недискримінацію, право на захист особистих даних та конфіденційність, право на свободу вираження поглядів та право на справедливий судовий розгляд. До найбільших ризиків застосування ШІ у межах кримінального провадження відносять непередбачуваність результатів, відповідальність за помилки, заміщення людської праці, етичні моменти» [14, с. 33].

Висновки. У підсумку зазначимо наступне. Поява та розвиток інформаційних технологій багато в чому визначає виконання покладених на правоохоронні органи традиційних функцій, а також впливає на появу нових функцій. Зокрема, впровадження комп'ютерних систем, програмних додатків, технології штучного інтелекту, використання великих даних, інтелектуальний аналіз даних, інструменти цифрової криміналістики, впровадження електронного поліцейського та інші технологічні інновації зробили революцію в традиційних методах правоохоронної діяльності та сприяють появі нових стратегій прогнозування кримінальних правопорушень. Використання цифрових технологій та інформаційних систем підвищує ефективність правоохоронних органів та відкриває нові можливості запобігання злочинності, сприяє консультуванню та покращенню операційної ефективності, зокрема шляхом автоматизації слідчих процедур.

Сучасні інформаційно-комунікаційні технології пропонують правоохоронним органам інструменти для оптимізації слідчих процесів, підвищення ефективності забезпечення ними громадської безпеки тощо. Однак поряд з перевагами є ризики, серед яких порушення безпеки даних, етичні проблеми, технологічна залежність та ін. Стратегічне прогнозування, пов'язане з визначенням перспектив досудового розслідування і судового розгляду, моделювання наслідків процесуальних рішень, що приймаються з використанням цифрових технологій, і планування заходів щодо сучасного процесу доказування.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Домашенко О.М. Проблемні питання використання цифрових доказів у криміналістиці. *Інноваційні методи та цифрові технології в криміналістиці, судовій експертизі та юридичній практиці*: матеріали міжнар. круглого столу (м. Харків, 12 груд. 2019 р.). Харків, 2019. С. 52–55.
2. Konovalova V.O., Shevchuk V.M. Digital criminalistics as a strategic direction of formation of criminalistic knowledge. *Advanced discoveries innovations, of modern, science experience, approaches and innovations: collection of scientific papers*: III International Scientific and Theoretical Conference (Amsterdam, Netherlands, 2023, January 20). Amsterdam, 2023. P. 73–77.
3. Про Національну поліцію: Закон України від 11.04.2015 № 580-VIII у ред. від 16.07.2024. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text.
4. Shevchuk V. Development trends in criminalistics in the era of digitalization**.** *Modern Knowledge: Research and Discoveries*: Proceedings of the 1st International Scientific and Practical Conference (Vancouver, Canada, May 19–20, 2023). P. 198–219. DOI 10.51582/interconf.19-20.05.2023.019.
5. Maras M.-.H. Computer forensics: cybercriminals, laws, and evidence. 2nd ed.. Burlington : Jones & Bartlett Learning, 2014. 372 p.
6. Колодіна А.С., Федорова Т.С. Цифрова криміналістика: проблеми теорії і практики. *Київський часопис права*. 2022. № 1. С. 176–180. DOI: 10.32782/klj/2022.1.27.
7. An Algorithm for Crime Detection in Digital Forensics / A. Singh, S.K. Singh, N. Singh, Sandeep K. Nayak. *Journal of Survey in Fisheries Sciences*. 2023. Vol. 10. P. 1281–1290. DOI 10.17762/sfs.v10i3S.136.
8. Deepak Thakkar. The Future of Digital Forensics: Trends and Emerging Technologies. 2024. Apr 12. URL: https://medium.com/@deepak_94375/the-future-of-digital-forensics-trends-and-emerging-technologies-567483f778d6.
9. Nelufule N., Masango Mf., Singano T. The Future of Digital Forensic Investigations: Keeping the Pace with Technological Advancements. *Conference: 2024 47th MIPRO ICT and Electronics Convention (MIPRO)*. 2024. DOI 10.1109/MIPRO60963.2024.10569461.

10. Пядишев В.Г. Перспективи розвитку проактивної діяльності поліції: зарубіжний погляд. *Право і суспільство*. 2024. № 1, т. 2. С. 403–412. DOI 10.32842/2078-3736/2024.1.2.61.
11. Проневич О.С. Проактивна діяльність поліції (міліції) як складова сучасної парадигми охорони правопорядку. *Форум права*. 2011. № 3. С. 639–643.
12. Convention for the Safeguarding of the Intangible Cultural Heritage MISC/2003/CLT/CH/14/ UNESCO. 2003. URL: https://unesdoc.unesco.org/ark:/48223/ pf0000132540.
13. Заяву в поліцію тепер можна подати онлайн на Мальті. *Закон і бізнес*. 2024. 13 серпня. URL: https://zib.com.ua/ua/print/162668.html.
14. Малачівська-Данчак М. Інтеграція штучного інтелекту в кримінальний процес: чи готова Україна до цього? *Юридичний вісник України*. 2024. 16–30 квіт. (№ 16–17). С. 33.
15. Радутний О.Е. Великі дані: кореляція та причинність (кримінально-правовий аспект). *Інформація і право*. 2023. № 2. С. 94–112. DOI 10.37750/2616-6798.2023.2(45).282328.
16. Ferguson A.G. The rise of big data policing: Surveillance, race, and the future of law enforcement. New York : NYU Press, 2017. 272 p.
17. Harcourt B.E. The counterrevolution: How our government went to war against its own citizens. Basic Books, Feb 27, 2018. 336 p.
18. Angwin J. Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance. New York: Times Books, 2014. 304 p.
19. Citron D.K. Hate Crimes in Cyberspace. Harvard University Press, 2014. 352 p.