НАЦІОНАЛЬНИЙ АЕРОКОСМІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АЕРОКОСМІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова праця
на правах рукопису

КАЛЮЖНИЙ ДМИТРО ОЛЕКСАНДРОВИЧ

УДК 342.9(043)

ДИСЕРТАЦІЯ

ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ВПРОВАДЖЕННЯ І ВИКОРИСТАННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ У ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

Спеціальність 081 Право
Галузь знань 08 Право

Подається на здобуття наукового ступеня доктора філософії

Дисертація містить результати власних досліджень.
Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело_____Д.О.КАЛЮЖНИЙ

Науковий керівник – Гуцу Світлана Федорівна, кандидат юрид. наук, доцент.

Харків – 2026

АНОТАЦІЯ

Калюжний Д.О. Теоретико-правові засади впровадження і використання інформаційно-комунікаційних технологій у діяльності правоохоронних органів – *Кваліфікаційна наукова праця на правах рукопису.*

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 081 «Право» – Національний аерокосмічний університет «Харківський авіаційний інститут», Харків, 2026.

Дисертаційне дослідження спрямоване на комплексний аналіз теоретико-правових засад впровадження і використання інформаційно-комунікаційних технологій у діяльності правоохоронних органів України. Особливу увагу приділено комплексному осмисленню теоретико-методологічних підходів використання технологій штучного інтелекту та інших інноваційних рішень у правоохоронній сфері. Їх упровадження розглядається крізь призму забезпечення належного захисту прав і законних інтересів громадян, підтримання громадського порядку, запровадження відповідальності для розробників прграмного забезпечення та працівників правоохоронних органів для зміцнення гарантій публічної безпеки. Водночас акцент зроблено на потенціалі таких технологій щодо підвищення інституційної ефективності правоохоронних органів, удосконалення професійної компетентності співробітників, посилення рівня їхньої безпеки та оптимізації результативності службової діяльності.

У дослідженні обґрунтовано, що цифровізація правоохоронної сфери зумовлює необхідність переосмислення традиційних підходів юридичної науки та формування комплексної методології, здатної поєднати правові, технологічні й соціальні виміри використання інформаційно-комунікаційних технологій. Методологію дослідження визначено як систему принципів, підходів і методів наукового пізнання, спрямовану на виявлення закономірностей формування та реалізації правових механізмів цифровізації правоохоронної діяльності. Розкрито зміст філософських, загальнонаукових і спеціально-юридичних

методів, зокрема діалектичного, метафізичного, системного, логічного, історико-правового та порівняльно-правового, обґрунтовано їх взаємозв'язок і значення для аналізу правового регулювання впровадження інформаційно-комунікаційних технологій. Доведено, що інтеграція різних рівнів пізнання забезпечує цілісне осмислення цифрової трансформації правоохоронної діяльності, дозволяє зберегти баланс між ефективністю технологій і дотриманням принципів верховенства права та захисту прав людини.

Здійснено комплексний теоретико-правовий аналіз поняття, сутності та завдань інформаційно-комунікаційних технологій у діяльності правоохоронних органів. Доведено, що відсутність уніфікованого понятійно-категоріального апарату щодо правоохоронної діяльності, правоохоронних органів та інформаційно-комунікаційних технологій зумовлює правову невизначеність у сфері цифровізації роботи органів правопорядку. Проаналізовано еволюцію понять «технологія», «інформаційна технологія» та «інформаційно-комунікаційні технології» у науковій доктрині й законодавстві України, з урахуванням нової редакції Закону України «Про Національну програму інформатизації». Запропоновано авторське визначення інформаційно-комунікаційних технологій у діяльності правоохоронних органів та визначено їх структурні елементи, функціональне призначення і класифікацію. Обґрунтовано, що завдання використання інформаційно-комунікаційних технологій у правоохоронній сфері полягають у забезпеченні інформаційної, аналітичної та інформаційно-технічної діяльності з метою підвищення ефективності роботи правоохоронців за умови дотримання конституційних прав і свобод людини.

У дослідженні проведено комплексний теоретико-правовий аналіз принципів використання інформаційно-комунікаційних технологій у діяльності правоохоронних органів як системоутворювальних засад правового регулювання цифровізації органів правопорядку. Узагальнено наукові підходи до розуміння змісту загальних принципів права та обґрунтовано їх значення для формування правових меж застосування інформаційно-комунікаційних технологій. Запропоновано авторське визначення принципів використання інформаційно-

комунікаційних технологій у діяльності правоохоронних органів як системи керівних ідей, що визначають зміст, спрямованість і допустимі межі впровадження, застосування та контролю цифрових технологій. Сформовано класифікацію галузевих принципів за рівнем і сферою дії. Обґрунтовано необхідність їх нормативної конкретизації з урахуванням національної правової доктрини, європейського законодавства та міжнародного досвіду.

У дослідженні здійснено комплексний науковий аналіз правової основи використання інформаційно-комунікаційних технологій у діяльності правоохоронних органів. Обґрунтовано відмінність між поняттями «правові засади» та «правова основа», визначено останню як структурно-нормативний рівень правового регулювання, що формує юридичний каркас цифровізації правоохоронної діяльності. Узагальнено доктринальні підходи до розуміння правової основи в різних напрямах правоохоронної та оперативно-розшукової діяльності, доведено її багатокомпонентний і системний характер. Проаналізовано національні та європейські нормативно-правові акти, що визначають стандарти захисту персональних даних, кібербезпеки та прав людини в цифровому середовищі. Запропоновано авторське визначення правової основи використання інформаційно-комунікаційних технологій у діяльності правоохоронних органів та здійснено систематизацію відповідного законодавства за ієрархічним, предметним, функціональним і спеціальним критеріями.

Осмислено концептуальні засади впровадження технології штучного інтелекту у правоохоронну сферу. Обґрунтовано, що штучний інтелект є міждисциплінарним явищем, яке поєднує технологічні, когнітивні, філософські та правові аспекти й потребує спеціального теоретико-правового осмислення у сфері реалізації владних повноважень держави. Визначено ключові юридичні виклики, пов’язані з використанням алгоритмічних систем у правоохоронній діяльності, зокрема ризики порушення прав людини, приватності, принципів законності та підзвітності. Сформульовано концептуальні підходи до правової легітимації застосування штучного інтелекту з урахуванням вимог верховенства

права, пропорційності, прозорості та верховенства інтересів людини, що створює методологічну основу для подальшого аналізу принципів, суб'єктного складу та механізмів контролю використання технологій штучного інтелекту у правоохоронній сфері. Запропоновано доповнити чинне законодавство нормами щодо обов'язкового моніторингу та контролю за законністю програмного забезпечення з елементами ШІ та передбачити відповідальність розробників і правоохоронців в разі порушення принципів запровадження і використання ШІ в процесі виконання службових повноважень.

Виявлено ключові проблеми правового регулювання невибіркового відеоспостереження з технологією відеоаналітики (FRT). Проведено порівняльний аналіз українського законодавства та стандартів ЄС (GDPR, Директива (ЄС) 2016/680), обґрунтовано необхідність цільового, обмеженого та контрольованого використання FRT як джерела інформації з обмеженим доступом, запровадження судового або адміністративного дозволу, сертифікації алгоритмів, визначення строків зберігання даних і юридичної відповідальності.

Проаналізовано можливості використання технологій штучного інтелекту в процесі автоматизованого формування протоколів, стенограм та аналітичних звітів на основі аудіо- й відеоданих, а також їх вплив на ефективність документування слідчих і службових дій. Особливу увагу приділено правовим аспектам допустимості документів, згенерованих за допомогою штучного інтелекту, зокрема вимогам до автентичності джерел даних, сертифікації алгоритмів, контролю похибок і відповідальності уповноважених посадових осіб. Обґрунтовується, що результати відеоаналітики та автоматичної транскрипції не можуть розглядатися як самостійні докази, а мають допоміжний характер і підлягають обов'язковій перевірці. Зроблено висновок про необхідність чіткого нормативного визначення правового статусу документів, створених із використанням штучного інтелекту, з метою забезпечення законності, процесуальних гарантій та пріоритету прав людини.

У дослідженні проаналізовано роль мережі Інтернет в інформаційно-аналітичній діяльності правоохоронних органів, як джерела доказової й

аналітичної інформації та інструменту організаційно-комунікаційної взаємодії з громадськістю. Розглянуто застосування сучасних технологій аналізу даних, зокрема OSINT і SOCMINT, а також програмних засобів аналізу зв'язків і соціальних мереж. Проаналізовано нормативно-правові засади моніторингу відкритих джерел і соціальних медіа з урахуванням принципів законності, доцільності та захисту прав людини.

У дисертації розглянуті можливості використання технологій штучного інтелекту у сфері безпеки та охорони праці працівників правоохоронних органів, виявлено їх потенціал для моніторингу фізичного стану поліцейських під час виконання службових обов'язків, а також досліджено умови належного нормативного та організаційного забезпечення таких процесів, зокрема необхідність запровадження чіткої й прозорої політики збирання, зберігання та обміну даними з метою гарантування конфіденційності, інформаційної безпеки та дотримання етичних стандартів. Обґрунтовано значення отримання поінформованої згоди й забезпечення взаємодії всіх залучених суб'єктів, а також визначено потенціал технологій ШІ для індивідуалізації професійного навчання, удосконалення тренувальних програм і впровадження систем об'єктивного зворотного зв'язку, що сприяє підвищенню ефективності службової діяльності та професійному зростанню правоохоронців.

Визначено європейські стандарти застосування інформаційно-комунікаційних технологій у правоохоронній діяльності та ключові принципи цифрової трансформації органів правопорядку в державах ЄС. Проаналізовано нормативно-правову базу ЄС, зокрема GDPR, Директиву (ЄС) 2016/680 (LED), Регламент про штучний інтелект (EU AI Act) та акти у сфері кібербезпеки, а також механізми міжнародного співробітництва, діяльність Європолу й системи контролю за високоризиковими ШІ-рішеннями. Підкреслено необхідність адаптації європейських практик для формування ефективної, безпечної та правомірної системи використання інформаційних технологій у правоохоронних органах України

Узагальнено міжнародний досвід упровадження новітніх технологій у правоохоронній діяльності в умовах глобалізації злочинності, зокрема протидії кіберзлочинам, тероризму та організованим формам кримінальної діяльності. Наведено приклади практик Інтерполу, США, Канади, Великої Британії, Німеччини, Франції та інших держав, що демонструють різні моделі правового й етичного регулювання інтелектуальних систем. Зроблено висновок, що ефективне використання цифрових технологій можливе лише за умови наявності системи контролю, яка гарантує прозорість, підзвітність і недискримінаційність алгоритмів, а для України адаптація міжнародного досвіду є важливою передумовою модернізації правоохоронної системи та інтеграції з міжнародними безпековими платформами.

Ключові слова: правове регулювання, правоохоронні органи, інформація, інформація з обмеженим доступом, інформаційно-комунікаційні технології, інформаційні технології, принципи використання ІКТ в правоохоронній діяльності, штучний інтелект, розробник програмного забезпечення, інформаційні права, інформаційна безпека, кібербезпека, відповідальність, європейське законодавство, зарубіжний досвід.

ABSTRACT

Kaliuzhnyi D.O. Theoretical and Legal Foundations of the Introduction and Use of Information and Communication Technologies in the Activities of Law Enforcement Agencies – *Qualification scientific work submitted as a manuscript.*

Dissertation for the degree of Doctor of Philosophy in specialty 081 “Law” – National Aerospace University “Kharkiv Aviation Institute”, Kharkiv, 2026.

The dissertation research is aimed at a comprehensive analysis of the theoretical and legal foundations for the implementation and use of information and communication technologies in the activities of law enforcement agencies in Ukraine. Particular attention is paid to a comprehensive understanding of the theoretical and methodological approaches to the use of artificial intelligence technologies and other innovative solutions in the law enforcement sphere.

Their implementation is considered through the prism of ensuring the proper protection of the rights and legitimate interests of citizens, maintaining public order, introducing liability for software developers and law enforcement officials to strengthen public safety guarantees. At the same time, emphasis is placed on the potential of such technologies to improve the institutional effectiveness of law enforcement agencies, improve the professional competence of employees, enhance their security, and optimise the effectiveness of their work.

The study argues that the digitalisation of law enforcement necessitates a rethinking of traditional approaches to legal science and the development of a comprehensive methodology capable of combining the legal, technological, and social dimensions of the use of information and communication technologies. The research methodology is defined as a system of principles, approaches, and methods of scientific knowledge aimed at identifying the patterns of formation and implementation of legal mechanisms for the digitalisation of law enforcement activities. The content of philosophical, general scientific, and special legal methods—in particular dialectical, metaphysical, systemic, logical, historical-legal, and comparative-legal methods—is revealed, and their interconnection and significance for the analysis of legal regulation of the implementation of information and communication technologies is substantiated. It is proven that the integration of different levels of knowledge provides a holistic understanding of the digital transformation of law enforcement activities and allows maintaining a balance between the effectiveness of technologies and compliance with the principles of the rule of law and human rights protection.

A comprehensive theoretical and legal analysis of the concept, essence, and tasks of information and communication technologies in the activities of law enforcement agencies has been carried out. It has been proven that the absence of a unified conceptual and categorical apparatus regarding law enforcement activities, law enforcement agencies, and information and communication technologies causes legal uncertainty in the field of digitalisation of the work of law enforcement agencies. The evolution of the concepts of “technology”, “information technology”, and “information and communication technologies” in the scientific doctrine and legislation of Ukraine

has been analysed, taking into account the new edition of the Law of Ukraine “On the National Informatisation Programme”. The author's definition of information and communication technologies in the activities of law enforcement agencies is proposed, and their structural elements, functional purpose, and classification are determined. It is substantiated that the tasks of using information and communication technologies in law enforcement consist in ensuring informational, analytical, and information-technical activities with the aim of improving the effectiveness of law enforcement agencies while respecting constitutional human rights and freedoms.

The study provides a comprehensive theoretical and legal analysis of the principles of using information and communication technologies in the activities of law enforcement agencies as the system-forming foundations of legal regulation of the digitalisation of law enforcement agencies. Scientific approaches to understanding the content of general principles of law are summarised, and their significance for the formation of legal boundaries for the application of information and communication technologies is substantiated. The author proposes a definition of the principles of using information and communication technologies in the activities of law enforcement agencies as a system of guiding ideas that determine the content, direction, and permissible limits of the introduction, application, and control of digital technologies. A classification of sectoral principles by level and scope of application has been developed. The necessity of their normative specification is justified, taking into account national legal doctrine, European legislation and international experience.

The study provides a comprehensive scientific analysis of the legal basis for the use of information and communication technologies in law enforcement activities. It substantiates the difference between the concepts of “legal principles” and “legal basis,” defining the latter as the structural and normative level of legal regulation that forms the legal framework for the digitalisation of law enforcement activities. It summarises doctrinal approaches to understanding the legal basis in various areas of law enforcement and operational-investigative activities and proves its multi-component and systematic nature. National and international regulatory and legal acts defining standards for the protection of personal data, cybersecurity, and human rights

in the digital environment are analysed. The author's definition of the legal basis for the use of information and communication technologies in the activities of law enforcement agencies is proposed, and the relevant legislation is systematised according to hierarchical, subject-matter, functional, and special criteria.

The conceptual foundations for the implementation of artificial intelligence technology in law enforcement have been comprehensively examined. It has been established that artificial intelligence is an interdisciplinary phenomenon that combines technological, cognitive, philosophical, and legal aspects and requires special theoretical and legal consideration in the sphere of the exercise of state authority. Key legal challenges associated with the use of algorithmic systems in law enforcement have been identified, in particular the risks of violating human rights, privacy, and the principles of legality and accountability. Conceptual approaches to the legal legitimisation of the use of artificial intelligence have been formulated, taking into account the requirements of the rule of law, proportionality, transparency, and the supremacy of human interests, which creates a methodological basis for further analysis of the principles, subject composition, and mechanisms for controlling the use of artificial intelligence technologies in law enforcement. It is proposed to supplement the current legislation with provisions on mandatory monitoring and control of the legality of software with AI elements and to provide for the liability of developers and law enforcement officials in case of violation of the principles of introduction and use of AI in the performance of official duties.

Key issues in the legal regulation of indiscriminate video surveillance using video analytics technology (FRT) have been identified. A comparative analysis of Ukrainian legislation and EU standards (GDPR, Directive (EU) 2016/680) was conducted, justified the need for targeted, limited and controlled use of FRT as a source of information with restricted access, the introduction of judicial or administrative authorisation, certification of algorithms, determination of data retention periods and legal liability.

The possibilities of using artificial intelligence technologies in the process of automated generation of protocols, transcripts, and analytical reports based on audio

and video data, as well as their impact on the effectiveness of documenting investigative and official actions, are analysed. Particular attention is paid to the legal aspects of the admissibility of documents generated using artificial intelligence, in particular the requirements for the authenticity of data sources, certification of algorithms, error control, and the responsibility of authorised officials. It is argued that the results of video analytics and automatic transcription cannot be considered independent evidence, but are of an auxiliary nature and are subject to mandatory verification. The study concludes that there is a need for a clear regulatory definition of the legal status of documents created using artificial intelligence in order to ensure legality, procedural guarantees, and the priority of human rights.

The study analyses the role of the Internet in the information and analytical activities of law enforcement agencies as a source of evidence and analytical information, and as a tool for organisational and communication interaction with the public. The application of modern data analysis technologies, in particular OSINT and SOCMINT, as well as software tools for analysing connections and social networks, is considered. The regulatory and legal framework for monitoring open sources and social media is analysed, taking into account the principles of legality, expediency, and the protection of human rights.

The dissertation examines the possibilities of using artificial intelligence technologies in the field of security and occupational safety of law enforcement officers, reveals their potential for monitoring the physical condition of police officers while performing their duties, and explores the conditions for proper regulatory and organisational support for such processes, in particular, the need to introduce a clear and transparent policy for the collection, storage, and exchange of data in order to ensure confidentiality, information security, and compliance with ethical standards. The importance of obtaining informed consent and ensuring the interaction of all involved parties was substantiated, and the potential of AI technologies for individualising professional training, improving training programmes, and introducing objective feedback systems was identified, which contributes to increasing the

effectiveness of official activities and the professional growth of law enforcement officers.

European standards for the use of information and communication technologies in law enforcement and key principles of digital transformation of law enforcement agencies in EU countries are identified. The EU regulatory framework, in particular the GDPR, Directive (EU) 2016/680 (LED), the Artificial Intelligence Regulation (EU AI Act), and cybersecurity acts, as well as mechanisms for international cooperation, Europol activities, and systems for controlling high-risk AI solutions, have been analysed. The need to adapt European practices for the formation of an effective, secure, and lawful system for the use of information technologies in law enforcement agencies in Ukraine is emphasised.

International experience in the implementation of the latest technologies in law enforcement activities in the context of globalised crime, in particular the fight against cybercrime, terrorism, and organised forms of criminal activity, is summarised. Examples of practices in Interpol, the United States, Canada, Great Britain, Germany, France, and other countries were given, demonstrating various models of legal and ethical regulation of intelligent systems. It is concluded that the effective use of digital technologies is only possible if there is a control system that guarantees the transparency, accountability, and non-discriminatory nature of algorithms, and that for Ukraine, the adaptation of international experience is an important prerequisite for the modernisation of the law enforcement system and integration with international security platforms.

Keywords: legal regulation, law enforcement agencies, information, restricted access information, information and communication technologies (ICT), information technologies, principles of ICT use in law enforcement activities, artificial intelligence, software developer, information rights, information security, cybersecurity, liability, European legislation, foreign experience.

Список публікацій здобувача

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Kalyuzhnyi D. Legal grounds for artificial intelligence use in law enforcement: international and foreign experience // Архів кримінології та судових наук. 2024. № 1 (9). С. 117–127. DOI: 10.32353/acfs.9.2024.08.

2. Калюжний Д. До питання правового статусу документів, згенерованих штучним інтелектом, в правоохоронній сфері // Науковий вісник Ужгородського національного університету. Серія: Право. 2025. Вип. 88, ч. 2. С. 399–404. DOI: 10.24144/2307-3322.2025.88.2.55.

3. Калюжний Д. Проблеми та перспективи штучного інтелекту в діяльності правоохоронних органів // Науковий вісник Дніпровського державного університету внутрішніх справ. 2025. № 1 (134). С. 281–287. DOI: 10.32782/2078-3566-2025-1-36.

4. Калюжний Д. Захист інформаційних прав особи в умовах цифровізації правоохоронної діяльності: теоретико-правовий аспект // Науковий вісник Ужгородського національного університету. Серія: Право. 2025. Вип. 90, ч. 3. С. 214–219. DOI: 10.24144/2307-3322.2025.90.3.30.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

1. Калюжний Д. Сучасні інформаційні технології в діяльності правоохоронних органів: проблеми і перспективи правового регулювання // Безпека та сталий розвиток критичної інфраструктури в умовах воєнного стану : тези доп. наук.-практ. конф., Харків, 8 листоп. 2023 р. / Нац. аерокосм. ун-т ім. М. Є. Жуковського «Харків. авіац. ін-т». Харків, 2023. С. 65–69. URL: http://library.khai.edu/library/fulltexts/doc/Bezpeka_Ta_Stalyy_Rozvytok.pdf (дата звернення: 30.01.2026).

2. Калюжний Д. Принципи використання інформаційних технологій правоохоронними органами // Протидія дезінформації в умовах російської агресії проти України: виклики і перспективи : тези доп. міжнар наук.-практ. конф., Харків, 12–13 груд. 2023 р. / НДІ публ. політики і соц. наук та ін. Харків, 2023. С. 221–224. URL: https://library.pp-

ss.pro/index.php/ndippsn_20231212/article/view/kaliuzhnyi/pdf (дата звернення: 30.01.2026).

3. Калюжний Д. Щодо питання правового визначення і особливостей ІКТ у правоохоронній діяльності // Сучасні проблеми розвитку авіаційно-космічної галузі України: інженерія, бізнес, право : тези доп. міждисциплінар. наук.-практ. конф., Харків, 5 листоп. 2024 р. / Нац. аерокосм. ун-т ім. М. Є. Жуковського «Харків. авіац. ін-т». Харків, 2024. С. 132–137. URL: http://library.khai.edu/library/fulltexts/Conf/Konf_SPR_2024.pdf (дата звернення: 30.01.2026).

4. Калюжний Д. Правові засади використання ІКТ в правоохоронній діяльності: європейський досвід // Міждисциплінарний дискурс: стійкість критичної інфраструктури : тези доп. наук.-практ. конф., Харків, 14 трав. 2024 р. / Нац. аерокосм. ун-т ім. М. Є. Жуковського «Харків. авіац. ін-т». Харків, 2024. С. 64–69. URL: https://library.khai.edu/library/fulltexts/Conf/Mizhdystsyplinarnyy_Dyskurs.pdf(дата звернення: 30.01.2026).

5. Калюжний Д. Проблеми правового регулювання використання систем відеоспостереження правоохоронними органами // Пропілеї права та безпеки. 2025. № 6/7: Захист та стійкість критичної інфраструктури : матеріали наук.-практ. конф., Харків, 14 трав. 2025 р. С. 65–67. DOI: 10.32620/pls.2025.67.16.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

Абревіатура	Розшифрування
АІС	автоматизована інформаційна система
ДБР	Державне бюро розслідувань
ДКП	Департамент кіберполіції Національної поліції України
ЄС	Європейський Союз
ІКТ	інформаційно-комунікаційні технології
ІТ	інформаційні технології
МВС	Міністерство внутрішніх справ України
Мінцифра	Міністерство цифрової трансформації України
НАБУ	Національне антикорупційне бюро України
НАЗК	Національне агентство з питань запобігання корупції
ООН	Організація Об’єднаних Націй
СБУ	Служба безпеки України
ШІ	штучний інтелект
ENISA	European Union Agency for Cybersecurity (Агентство Європейського Союзу з кібербезпеки)
ELOS	European Law of Security (Європейське право безпеки)
FRT	Facial Recognition Technology (технологія розпізнавання обличчя)
GDPR	General Data Protection Regulation (Загальний регламент про захист даних)
IEC	International Electrotechnical Commission (Міжнародна електротехнічна комісія)
IoT	Internet of Things (Інтернет речей)
ISO	International Organization for Standardization (Міжнародна організація зі стандартизації)
OECD	Organisation for Economic Co-operation and Development (Організація економічного співробітництва та розвитку)

ВСТУП

Обґрунтування вибору теми дослідження. У сучасних умовах цифрової трансформації суспільства та державного управління інформаційно-комунікаційні технології (ІКТ) набули стратегічного значення для забезпечення ефективного функціонування державних інституцій, зокрема правоохоронних органів. Їх упровадження сприяє підвищенню рівня оперативності, прозорості, координації, аналітичної спроможності та підзвітності правоохоронних структур, що є особливо важливим в умовах зростання складності викликів у сфері національної безпеки, охорони правопорядку та захисту прав і свобод людини.

Стрімке зростання обсягів і швидкості обігу інформації, розвиток технологій штучного інтелекту (ШІ), систем відеоаналітики, електронного документообігу, цифрової криміналістики, біометричних технологій і розширення кіберпростору зумовлюють необхідність переосмислення правових засад діяльності правоохоронних органів. Особливої актуальності ці питання набувають у контексті реалізації державної політики цифрової трансформації, розвитку електронного урядування та інтеграції України до європейського правового й інформаційного простору.

Водночас актуальність теми істотно посилюється в умовах триваючої збройної агресії проти України та ведення гібридної війни, що супроводжується масштабними інформаційними атаками, кібератаками, дезінформаційними кампаніями та використанням цифрових технологій як інструментів впливу на безпеку держави й суспільства. За таких умов інформаційно-комунікаційні технології набувають не лише допоміжного, а й системоутворювального значення у діяльності правоохоронних органів, забезпечуючи оперативне реагування на загрози, ефективну міжвідомчу взаємодію в межах сектору безпеки і оборони, фіксацію та розслідування воєнних злочинів, а також захист критичної інформаційної інфраструктури.

Разом із тим, інтенсивне, а подекуди прискорене, впровадження новітніх технологій у правоохоронну практику актуалізує низку складних теоретико-правових проблем, пов'язаних із визначенням меж їх допустимого використання, забезпеченням принципів законності, пропорційності та верховенства права, а також гарантуванням належного рівня захисту прав і свобод людини. Це зумовлює об'єктивну потребу у комплексному науковому осмисленні теоретико-правових засад впровадження та використання ІКТ у діяльності правоохоронних органів в умовах воєнної агресії.

Важливе методологічне та теоретичне підґрунтя для здійснення комплексного дослідження становлять праці українських і зарубіжних учених, присвячені проблематиці цифровізації публічного управління, використанню інформаційно-комунікаційних технологій у судочинстві та правоохоронній діяльності, а також питанням інформаційної безпеки й захисту прав людини в цифровому середовищі. Зокрема, окремі аспекти правоохоронної діяльності та правового статусу правоохоронних органів досліджували О. Бандурка, В. Гірич, Р. Калюжний, В. Ковальська, А. Кучук, О. Мартиненко, М. Мельник, В. Тацій, П. Хамула, А. Голубов, І. Казанчук та інші; правовий статус і роль штучного інтелекту аналізуються у працях Є. Тимошенко, А. Шевченка, О. Баранова та інших учених; застосування інформаційних технологій у кримінальному провадженні – у дослідженнях Є. Лук'янчикова, С. Лукашевича, М. Степанюка, В. Павликівського, В. Тіщенка, Н. Філіпенко, Д. Денищука, В. Шепітька, В. Шевчука, В. Юсупова; використання технологій штучного інтелекту в судочинстві з акцентом на автоматизації процедур, алгоритмізації правозастосування та відповідних правових ризиках досліджуються у працях В. Пенькова, В. Тація, О. Рєзніка, С. Холодника, К. Юдкової.

Праці вітчизняних учених у галузі теорії держави і права, зокрема Є. Харитонової, П. Рабіновича, М. Козюбри, О. Балинської, В. Ященка, О. Скакун та інших, мають фундаментальний характер і створюють концептуальне підґрунтя для осмислення правової природи, принципів і механізмів правового регулювання суспільних відносин, у тому числі пов'язаних із використанням

новітніх технологій. У дослідженні також використано праці зарубіжних науковців, зокрема S. A. Saxby, J. P. Barlow, L. Lessig, E. Poppel, H. L. Goldstein, J. McCarthy, у яких розкриваються концептуальні підходи до правового регулювання цифрового середовища, інформаційних прав, кібербезпеки, а також впливу новітніх технологій на трансформацію правової системи.

Разом із тим, сучасний стан наукової розробки теоретико-правових засад упровадження та використання інформаційно-комунікаційних технологій у діяльності правоохоронних органів, зокрема визначення їхніх правових ознак, принципів, механізмів функціонування, співвідношення із суміжними правовими категоріями, а також особливостей міжнародного, європейського й національного правового регулювання, ще не повною мірою відповідає потребам сучасної юридичної теорії та практики, особливо в умовах збройної агресії проти України, ведення гібридної війни та зростання масштабів і складності інформаційних атак. У вітчизняній юридичній науці наразі відсутні комплексні дослідження, присвячені системному визначенню теоретико-правових засад, принципів і механізмів правового регулювання застосування ІКТ у цій сфері. Це, своєю чергою, зумовлює наукову новизну, практичну актуальність і суспільну значущість обраної теми, а також потребу в поглибленому аналізі чинної нормативно-правової бази, оцінці інституційної спроможності правоохоронних органів до впровадження інновацій в умовах гібридної війни та визначенні ефективності реалізованих цифрових ініціатив у сфері протидії злочинності й інформаційним атакам.

Отже, дослідження проблематики теоретико-правових засад запровадження і використання інформаційно-комунікаційних технологій у діяльності правоохоронних органів України є своєчасним, науково обґрунтованим і має важливе значення для формування дієвих механізмів цифрового забезпечення правоохоронної діяльності, підвищення рівня правопорядку та зміцнення громадської безпеки.

Зв’язок роботи з науковими програмами, планами, темами. Тема дисертаційного дослідження затверджена Вченою радою Національного

аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут» 25.10.2023 (протокол № 3) зі змінами від 27.12.2023 (протокол № 5) та 22.10.2025 (протокол № 3). Тема дослідження відповідає основним науковим напрямам та найважливішим проблемам фундаментальних досліджень у галузі природничих, технічних, суспільних і гуманітарних наук Національної академії наук України на 2024–2028 роки, затвердженим постановою Президії НАН України від 10.01.2024 № 8, а саме підпунктам 3.5.5 (адміністративне право та процес, фінансове право) та 3.5.6 (інформаційне право), пріоритетним напрямам фундаментальних та прикладних наукових досліджень у галузі права, затвердженим Національною академією правових наук України, а також тематиці наукових досліджень кафедри права гуманітарно-правового факультету Національного аерокосмічного університету «Харківський авіаційний інститут» – «Правові засади стійкості та сталого розвитку критичної інфраструктури», затвердженій 23.04.2024 № 0124U002897. Тема також узгоджується з Концепцією Національної програми інформатизації (у редакції від 01.01.2022) та Концепцією Державної програми інформаційно-телекомунікаційного забезпечення правоохоронних органів, діяльність яких пов’язана з боротьбою зі злочинністю (від 19.09.2007).

Мета і завдання дослідження. *Метою* дисертаційного дослідження є всебічний аналіз теоретико-правових засад впровадження та використання інформаційно-комунікаційних технологій у діяльності правоохоронних органів, оцінка стану нормативно-правового регулювання у цій сфері, а також розроблення науково обґрунтованих пропозицій і рекомендацій щодо підвищення ефективності цифрової трансформації правоохоронної системи з урахуванням національної практики та міжнародного досвіду. Для досягнення поставленої мети були сформульовані такі завдання дослідження:

1. Проаналізувати методологічні підходи до дослідження теоретико-правових засад впровадження та використання інформаційно-комунікаційних технологій у діяльності правоохоронних органів.

2. Здійснити теоретико-правовий аналіз базової категорії дисертаційного дослідження – «інформаційно-комунікаційні технології в діяльності правоохоронних органів».

3. Дослідити принципи впровадження та використання інформаційно-комунікаційних технологій у діяльності правоохоронних органів, визначити їх зміст, класифікацію, роль та значення у забезпеченні законності, підзвітності та пропорційності.

4. Розкрити зміст, структуру та елементи правової основи застосування інформаційно-комунікаційних технологій правоохоронними органами.

5. Дослідити концептуальні засади впровадження та використання технологій штучного інтелекту у процесах збору, накопичення, обробки та аналізу інформації правоохоронними органами.

6. Визначити нормативно-правові засади використання можливостей мережі Інтернет під час здійснення правоохоронними органами функцій із розшуку осіб, запобігання та протидії правопорушенням, а також оцінити пов’язані з цим ризики для забезпечення прав людини та інформаційної безпеки.

7. Розкрити значення інформаційно-комунікаційних технологій у забезпеченні особистої безпеки працівників правоохоронних органів та у формуванні умов їх сталого професійного зростання, зокрема розвитку професійної, цифрової й аналітичної компетентності в умовах воєнних і гібридних безпекових загроз.

8. Дослідити Європейські норми та стандарти використання інформаційно-комунікаційних технологій у правоохоронній сфері, а також визначення можливостей їх імплементації у формування нормативної бази застосування ІКТ і ШІ в Україні.

9. Здійснити комплексний аналіз міжнародного досвіду застосування новітніх технологій у правоохоронній сфері та на його основі сформулювати науково обґрунтовані пропозиції щодо вдосконалення нормативно-правового регулювання впровадження, використання й контролю за застосуванням

інформаційно-комунікаційних технологій у діяльності правоохоронних органів України.

Об'єктом дослідження є суспільні відносини, що виникають у процесі впровадження і застосування інформаційно-комунікаційних технологій у діяльності правоохоронних органів.

Предметом дослідження виступають теоретико-правові засади впровадження і використання інформаційно-комунікаційних технологій у діяльності правоохоронних органів.

Методи дослідження обрано відповідно до мети та завдань дослідження, із урахуванням об'єкта й предмета дослідження. При підготовці дисертації використовувалися такі методи:

діалектичний (філософський) метод – для формулювання понять і визначень, тлумачення наукових термінів і приписів законодавства (підрозділи 1.1, 1.2, 1.3, 1.4, 2.1, 2.2);

аналізу та синтезу – дав можливість визначити ознаки, сутність і зміст поняття інформаційно-комунікаційної технології в діяльності правоохоронних органів (підрозділ 1.1);

системно-структурний застосовувався під час узагальнення історичного досвіду розвитку інформаційних відносин і застосування технологій в сфері юриспруденції і правозахисної діяльності (підрозділи 1.1, 1.2, 2.1, 3.1, 3.2);

системний підхід дав змогу сформулювати теоретичне обґрунтування необхідної діалектичної єдності загальної системи принципів використання ІКТ в діяльності правоохоронних органів (підрозділи 1.3, 2.1);

порівняльно-правовий метод – для узагальнення підходів щодо визначення змісту і ознак поняття «інформаційн-коммунікаційна технологія» (підрозділ 1.2) та правового регулювання використання окремих видів технологій в законодавстві зарубіжних країн (підрозділи 3.1, 3.2);

нормотворчості щодо вироблення пропозиції до законодавства в питанні використання ІКТ правоохоронними органами (підрозділ 1.3, 2.1, 2.2, 2.3).

Нормативно-правову базу дисертації становлять: Конституція України, закони України, укази Президента України, постанови Кабінету Міністрів України, міжнародно-правові акти, ратифіковані Україною, що визначають основи міжнародного співробітництва в інформаційній сфері.

Емпіричну базу дослідження становлять систематизовані матеріали офіційної статистичної звітності Вищого антикорупційного суду, Національної поліції України, Департаменту кіберполіції Національної поліції України, Державного центру кіберзахисту Держспецзв'язку, Державного бюро розслідувань, прокуратури України та Служби безпеки України опубліковані у відкритих джерелах, дані офіційного вебсайту Європейського Союзу, які містять рішення Європейського суду з прав людини.

Наукова новизна отриманих результатів полягає в тому, що дисертація є одним із перших в Україні комплексних самостійних наукових досліджень, присвячених визначенню теоретико-правових засад впровадження і використання інформаційно-комунікаційних технологій у діяльності правоохоронних органів. За її результатами сформульовано положення наукової новизни, що зводяться до такого:

вперше:

– сформульовано зміст поняття «правова основа застосування інформаційно-комунікаційних технологій у діяльності правоохоронних органів», під якою пропонується розуміти сукупність конституційних положень, міжнародно-правових стандартів, норм національного законодавства, підзаконних нормативно-правових актів і доктринальних положень, які визначають допустимі межі, порядок, форми та гарантії використання інформаційно-комунікаційних технологій правоохоронними органами з метою реалізації їхніх функцій за умови дотримання прав і свобод людини, забезпечення інформаційної безпеки та законності. Запропоновано розширити підходи до класифікації нормативних актів, що є правовою основою застосування інформаційно-комунікаційних технологій правоохоронцями за

предметом правового регулювання; за функціональним призначенням; за ступенем спеціалізації; за напрямом впливу;

– обґрунтовано доцільність внесення доповнень до законів України: «Про оперативно-розшукову діяльність», «Про Службу безпеки України», «Про Національну поліцію України», «Про захист персональних даних» щодо порядку і контролю (в тому числі громадського) використання інформаційно-комунікаційних технологій; а також щодо запровадження щорічного аудиту кібербезпеки та коректності функціонування інформаційних систем, що використовуються в оперативно-службовій діяльності відповідними правоохоронними органами;

– проведено класифікацію документів, створених із використанням технологій штучного інтелекту (ШІ), за критерієм ступеня автономності системи у процесі їх формування та визначено вимоги до документів, згенерованих або створених за допомогою ШІ. Зроблено висновок, що оскільки документи, створені автономними алгоритмічними системами, не мають автора у класичному праворозумінні, виникає необхідність нормативного визначення суб'єкта юридичної відповідальності за їх створення, перевірку і використання;

удосконалено:

– розуміння правової природи базової досліджуваної категорії – «інформаційно-комунікаційні технології в діяльності правоохоронних органів» як сукупності наукових, технічних, програмних і організаційних рішень, що використовуються для збирання, обробки, зберігання, передачі та аналізу інформації або створення нового інформаційного продукту з метою забезпечення законності, правопорядку, оперативного реагування на правопорушення, підтримки розслідувань і прийняття управлінських рішень у правоохоронних структурах.;

– визначення терміну «принципи використання інформаційно-комунікаційних технологій у діяльності правоохоронних органів» – це система керівних ідей, нормативно й доктринально обґрунтованих вимог, що визначають зміст, спрямованість та межі правового регулювання процесів упровадження,

застосування і контролю за використанням ІКТ у діяльності правоохоронних органів;

– перелік суб'єктів використання штучного інтелекту в правоохоронній діяльності за критерієм функціонального призначення: 1) правоохоронні органи, уповноважені законом здійснювати оперативно-розшукову, кримінально-процесуальну та іншу правоохоронну діяльність із використанням ІКТ і ШІ; 2) органи державного управління і регулювання, які формують державну політику, стандарти та нормативне забезпечення у сфері ШІ; 3) інституції контролю, нагляду та захисту прав людини; 4) розробники та технічні адміністратори систем ШІ; 5) громадяни, які виступають одночасно користувачами систем ШІ та суб'єктами, на яких впливають рішення, ухвалені з використанням алгоритмічних технологій;

дістали подальшого розвитку:

– наукові уявлення про визначення методології дослідження теоретико-правових засад впровадження і застосування інформаційно-комунікаційні технології в діяльності правоохоронних органів, як системи принципів, підходів, методів та засобів наукового пізнання, спрямованих на виявлення закономірностей формування, розвитку та реалізації правових механізмів використання інформаційно-комунікаційних технологій у діяльності правоохоронних органів;

– наукові напрацювання та теоретичні підходи до класифікації принципів використання інформаційно-комунікаційних технологій правоохоронними органами. Запропоновано класифікацію галузевих принципів використання ІКТ залежно від рівня та сфери їх дії (ступеня універсальності та спеціалізації);

– теоретико-правові засади впровадження і використання технологій штучного інтелекту правоохоронними органами. Обґрунтовано, що у вітчизняній і зарубіжній науковій літературі відсутня єдність підходів до визначення змісту та юридичної природи штучного інтелекту, що в умовах стрімкого розвитку цифрових технологій і зростання ролі алгоритмічних систем у процесах прийняття рішень актуалізує необхідність формування уніфікованих правових

стандартів, спрямованих на забезпечення ефективного, безпечного та етично виваженого застосування ШІ в діяльності правоохоронних органів;

– наукові положення про те, що мережа Інтернет у діяльності правоохоронних органів виконує подвійну функцію: як інструмент оперативно-розшукової та організаційно-комунікативної діяльності і як джерело доказової та аналітичної інформації, що зумовлює необхідність нормативного визначення підстав, процедур і меж її використання та чіткого розмежування спеціальних і загальнодоступних засобів правоохоронного моніторингу;

– наукові уявлення про роль штучного інтелекту як інструменту підтримки управлінських рішень у правоохоронних органах та забезпечення професійної безпеки правоохоронця, які доповнено цифровим і психофізіологічним виміром, що враховує вплив алгоритмічних систем підтримки прийняття рішень, автоматизованого моніторингу та інтелектуальних засобів навчання на умови проходження служби;

– наукові уявлення щодо принципів та підходів формування європейських стандартів використання ІКТ з елементами штучного інтелекту в правоохоронній сфері. Встановлено доцільність урахування відповідного європейського досвіду, зокрема щодо обмежень використання біометричних технологій, запровадження вимог до високоризикових систем та забезпечення багаторівневого контролю, у процесі формування нормативної бази застосування ІКТ і ШІ в діяльності правоохоронних органів України;

– пропозиції для України щодо імплементації зарубіжного досвіду впровадження інформаційно-комунікаційних технологій, які полягають у створенні незалежного Комітету з питань штучного інтелекту у правоохоронній сфері, який здійснюватиме експертно-наглядові функції щодо відповідності застосування ШІ міжнародним стандартам прав людини, а також у розробленні національних стандартів аудиту алгоритмів і систем ШІ, аналогічних американській моделі сертифікації безпеки, точності та захисту даних.

Практичне значення отриманих результатів полягає в тому, що основні положення, висновки та рекомендації дисертаційного дослідження можуть бути використані:

– *у науково-дослідній сфері* – для подальших наукових досліджень впровадження і використання ІКТ у правоохоронній діяльності;

– *у нормотворчості* – для вдосконалення нормативного регулювання застосування ІКТ правоохоронцями (Акт впровадження результатів дисертаційного дослідження у правотворчу діяльність Науково-дослідного інституту публічної політики і соціальних наук);

– *у правозастосовній діяльності* – для вдосконалення практики застосування ІКТ правоохоронними органами (Довідка про впровадження результатів дисертаційного дослідження у практичну діяльність Департаменту кіберполіції національної поліції України);

– *у навчальному процесі* – для підготовки навчально-методичних комплексів, підручників, навчальних посібників з дисциплін «Кримінально-процесуальне право», «Адміністративний процес», «Інформаційне право та інформаційна безпека об’єктів критичної інфраструктури» (Акт впровадження результатів дисертаційного дослідження в освітній процес Національного аерокосмічного університету «Харківський авіаційний інститут».

Апробація одержаних результатів дисертації. Одержані в ході дисертаційного дослідження висновки та узагальнення доповідалися та обговорювалися на міжнародних і всеукраїнських науково-практичних конференціях та круглих столах, а саме: «Безпека та сталий розвиток критичної інфраструктури в умовах воєнного стану» (м. Харків, 8 листопада 2023 р.); «Протидія дезінформації в умовах російської агресії проти України: виклики і перспективи» (м. Харків, 12–13 грудня 2023 р.); «Міждисциплінарний дискурс: стійкість критичної інфраструктури (м. Харків, 14 травня 2024 р.); Міждисциплінарна науково-практична конференція «Сучасні проблеми розвитку авіаційно-космічної галузі України: інженерія, бізнес, право» (м. Харків 5 листопада 2024 р.).

Публікації. Основні положення, висновки та пропозиції, сформульовані за результатами дисертаційної роботи, відображено у дев’яти наукових працях, зокрема у чотирьох наукових статтях (усі опубліковано у наукових виданнях України, визнаних фаховими з юридичних наук), а також у п’яти тезах наукових доповідей.

Структура та обсяг роботи. Дисертація складається зі вступу, трьох розділів, що містять 9 підрозділів, висновків, списку використаних джерел і двох додатків. Загальний обсяг дисертації становить 252 сторінки, з них основний текст – 202 сторінки, список використаних джерел (227 найменувань) – 27 сторінок.

РОЗДІЛ 1
ЗАГАЛЬНОТЕОРЕТИЧНІ ЗАСАДИ ВПРОВАДЖЕННЯ ТА ВИКОРИСТАННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ В ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

1.1 Методологія дослідження теоретико-правових засад впровадження і використання інформаційно-комунікаційних технологій в діяльності правоохоронних органів

Сучасна епоха характеризується глибокими трансформаційними процесами, що охоплюють усі сфери суспільного життя, у тому числі правоохоронну діяльність. Інформаційно-комунікаційні технології (ІКТ) стали одним із ключових чинників, які визначають ефективність, оперативність і прозорість функціонування правоохоронних органів. Їхнє впровадження сприяє підвищенню рівня аналітичного забезпечення, оптимізації управлінських процесів, зміцненню міжвідомчої взаємодії та забезпеченню належного рівня правопорядку в цифровому середовищі. Водночас використання ІКТ у сфері публічної безпеки створює низку нових викликів – від ризиків порушення прав людини до виникнення етичних та юридичних колізій, пов’язаних із застосуванням штучного інтелекту, автоматизованих систем ухвалення рішень чи обробки персональних даних. У цих умовах методологічне забезпечення дослідження впровадження ІКТ у діяльність правоохоронних органів набуває особливої ваги. Воно є не лише інструментом пізнання, а й концептуальною рамкою, що визначає логіку, напрям і теоретико-правову глибину всього дослідження.

Розвиток цифрових технологій зумовлює потребу в переосмисленні методології правознавства загалом, адже традиційні правові категорії (джерело права, доказ, суб’єкт правопорушення, публічна інформація тощо) набувають нових форм і змісту в електронному середовищі. Так, інформація, яка стає основним ресурсом діяльності правоохоронців, водночас перетворюється на

об’єкт правового захисту та доказову базу у кримінальному процесі. Це вимагає розроблення методології, здатної поєднати класичні правові доктрини з новими цифровими реаліями.

У цьому контексті особливого значення набуває узгодження методології правового аналізу ІКТ із державною політикою цифрової трансформації публічного управління, зокрема сектору безпеки і оборони, що реалізується відповідно до розпорядження Кабінету Міністрів України від 02.08.2024 № 735-р та актів, прийнятих на його виконання, за координації Міністерства цифрової трансформації України [1]. Цей документ передбачає створення єдиної цифрової екосистеми для правоохоронних органів, що підвищує актуальність методологічного осмислення правових аспектів її впровадження.

Треба зазначити, що розуміння дефініцій «методологія права» і «правові методи» не є однозначним. Власне, метод дослідження найчастіше розуміється як «шлях до чогось», процедура дослідження. Йдеться про певні дії, які спрямовані певними принципами на досягнення поставленої мети. Натомість поняття «методології» сприймається як наука про методи, вчення про способи пізнання. У широкому сенсі – це наука про обґрунтування наукових знань та побудови наукових систем. Методологія права є складовою юридичної науки, виходячи з того, що вона є системою знань, яка включена до певної пізнавальної системи [2].

Відповідно до вимог сучасної юридичної науки, методологія має забезпечити комплексне розуміння ІКТ у правоохоронній діяльності як правового, соціального та технологічного феномена, що трансформує систему правозастосування, характер правових відносин і механізми забезпечення безпеки особи. Як зазначають О. М. Балинська та В. А. Ященко: «Методологія сучасної юридичної науки є дуже складним і багатоплановим явищем. Ця обставина зумовлює велике розмаїття способів і підходів до інтерпретації її сутності. Очевидно, ця сутність розкривається через осягнення юридичної науки в контексті всієї системи соціально-гуманітарного знання, а також комунікативного характеру цієї системи, через розкриття особливого стилю

юриспруденції як складової правової культури та розгляд типів праворозуміння» [3, с. 20]. Своєю чергою, П. М. Рабінович дав таке визначення методології юридичної науки: «це система підходів, методів, і способів наукового дослідження, теоретичні засади яких використовуються при вивченні державно-правових явищ» [4, с. 168].

Український науковець М. Козюбра пропонує розглядати методологію правознавства у двох аспектах:

– як систему певних елементів, що має свою внутрішню будову, зумовлену предметом юридичної науки і пристосовану до нього;

– як елемент іншої системи (надсистеми), якою є юридична наука (в цьому аспекті методологію потрібно розглядати як сукупність знань, учень, теорій про пізнавальні й дослідницькі засоби юридичної науки та їх застосування; як складову юридичної науки, що належить до її теоретичної частини) [5].

У науковій юридичній літературі простежуються також спроби окреслити методологічні засади пізнання окремих галузей права, правових інститутів та явищ, з урахуванням їхньої специфіки та особливостей розвитку. Наприклад, Є. О. Харитонов, у межах методології юридичної науки визначає методологію цивілістики, що становить собою «систему підходів, методів і способів наукового дослідження, які є теоретично обґрунтованими» [6, с. 11]. У своїх наукових доробках О. М. Балинська та В. А. Ященко надають визначення методології оперативно-розшуковій діяльності (ОРД), яку пропонується розглядати у широкому та вузькому розумінні. В першому випадку – це система найбільш загальних підходів, що визначають її природу (походження), сутність та зміст (функції, закономірності), місце і роль оперативно-розшукової діяльності у суспільстві, державно-правовій сфері, правоохоронній діяльності й виконують функцію її регулятивного чинника. У вузькому ж розумінні методологія ОРД – це вчення про методи пізнання та здійснення оперативно-розшукової діяльності [3].

Враховуючи, наведений підхід щодо можливості звуження загальної методології правознавства до спеціальної методології галузевої юридичної науки, слід виокремлювати і методологію дослідження теоретико-правових засад

впровадження і застосування ІКТ у діяльності правоохоронних органів. Під такою методологією доцільно розуміти систему принципів, підходів, методів та засобів наукового пізнання, спрямовану на виявлення закономірностей формування, розвитку та реалізації правових механізмів легалізації й використання інформаційно-комунікаційних технологій у діяльності правоохоронних органів. Вона покликана забезпечити комплексний аналіз правових явищ, пов'язаних із цифровізацією правоохоронної сфери, їх філософське, загальнонаукове та спеціально-юридичне осмислення.

У теоретичному вимірі класифікація методів певної науки є свідченням її зрілості та сформованості власного пізнавального інструментарію. Методи наукового пізнання в юридичній науці класифікуються за різними критеріями, що зумовлено багатовимірністю правової реальності та складністю процесів її пізнання. Найбільш усталений підхід передбачає розмежування методів на філософські, загальнонаукові та конкретно-наукові (спеціальні) [7, с. 245]. У науковій літературі простежується також інший підхід, відповідно до якого методи поділяються за кількома додатковими ознаками:

– за рівнем пізнання – на теоретичні та практичні;

– за функціональним призначенням – на методи систематизації, пояснення й прогнозування;

– за предметною сферою застосування – на правові, статистичні, соціологічні, економічні тощо [8, с. 265].

Окремі дослідники пропонують розширену класифікацію, виділяючи філософські, загальнонаукові, приватнонаукові, дисциплінарні та міждисциплінарні методи [9, с. 24]. Така варіативність підходів свідчить про методологічний плюралізм сучасної юридичної науки та її відкритість до міжгалузевих форм пізнання. Саме через визнання цього плюралізму дослідники дедалі частіше відмовляються від жорсткої ієрархії методів та класичної вертикальної моделі їх поділу – на філософсько-світоглядні, загальнонаукові, спеціально-наукові та конкретно-наукові. Натомість ними пропонується «горизонтальний» підхід, за якого всі методи розглядаються як рівнозначні

інструменти дослідження, а їхнє використання визначається метою та логікою конкретного наукового пошуку [3].

Методологія дослідження теоретико-правових засад впровадження ІКТ у діяльність правоохоронних органів базується на єдності теоретичних і прикладних аспектів, що дозволяє не лише розкрити сутність правового регулювання цифрових процесів, а й визначити напрями його вдосконалення відповідно до принципів верховенства права, законності, пропорційності та поваги до прав людини. Вважаємо, що у межах цієї методології можуть застосовуватись як загальнотеоретичні підходи (діалектичний, системно-структурний, аксіологічний, герменевтичний, порівняльно-правовий, історико-правовий), так і спеціально-юридичні методи, що враховують особливості правового статусу суб'єктів правоохоронної діяльності, нормативно-правового забезпечення цифрових процесів, а також практику використання ІКТ у сфері запобігання, розслідування та протидії правопорушенням. Такий поділ забезпечує логічну впорядкованість методології, дозволяє визначити рівень наукової абстракції кожного методу та забезпечує цілісність і системність дослідження.

Як вже було зазначено, методологія дослідження теоретико-правових засад впровадження інформаційно-комунікаційних технологій в правоохоронну діяльність охоплює кілька взаємопов'язаних аспектів. По-перше, вона розглядається як вчення про процес пізнання та систему методів наукового дослідження, що визначають логіку та інструментарій наукового пошуку. По-друге, методологія виступає як практична основа здійснення наукової роботи, спрямованої на отримання нового знання у сфері цифровізації діяльності правоохоронних органів, що передбачає застосування конкретних засобів, прийомів і методів дослідження. По-третє, це сукупність методів, які використовуються у певному науковому дослідженні для досягнення поставленої мети та вирішення дослідницьких завдань.

Сутність методологічних засад полягає в інтеграції різних рівнів пізнання – філософського, загальнонаукового, спеціально-юридичного й

міждисциплінарного. Вона забезпечує перехід від абстрактного розуміння ролі технологій у праві до формування конкретних концептуальних положень щодо їхнього впровадження, регулювання та контролю в діяльності поліції, прокуратури, Державного бюро розслідувань (ДБР), Служби безпеки України (СБУ) та інших органів, уповноважених забезпечувати законність і правопорядок.

Для пізнання теоретико-правових засад упровадження та використання ІКТ у правоохоронній діяльності, на нашу думку, доцільно використовувати такий методологічний інструмент загального (філософського) рівня, як діалектичний метод. Метафізичний метод може застосовуватися як правомірний та обґрунтований за умови його виваженого й усвідомленого використання. У сукупності зазначені підходи формують світоглядно-методологічний фундамент наукового пізнання, зокрема в галузі юридичних досліджень. Загальнонаукові методи мають універсальний характер, оскільки охоплюють базові пізнавальні прийоми, зокрема аналіз, синтез, індукцію, дедукцію та класифікацію. Водночас конкретно-наукові (спеціальні) методи, зокрема порівняльно-правовий і історико-правовий, є визначальними на етапах опрацювання, тлумачення та впорядкування результатів наукового дослідження.

Провідну роль у структурі методології відіграє діалектичний метод, який забезпечує дослідження правових явищ у процесі їх змін, розвитку, внутрішніх суперечностей та взаємозумовленості. Саме діалектика виступає аксіоматичною засадою наукового пізнання, визначаючи теоретичну основу та категоріальний апарат методологічної свідомості сучасного науковця [10, с. 219]. Саме тому вона виступає методологічним стрижнем дослідження процесів інформатизації в системі правоохоронних органів, даючи змогу поєднати правові, технологічні та соціальні аспекти цього складного явища.

Діалектичний метод дозволяє розглядати право не як застиглу систему норм, а як динамічне явище, що розвивається у взаємодії з технологічним, економічним і соціальним середовищем. У цьому контексті застосування діалектики означає:

– аналіз взаємозв’язку між розвитком цифрових технологій та еволюцією правового регулювання правоохоронної діяльності;

– виявлення внутрішніх суперечностей між інтересами безпеки держави та правами людини у цифровому просторі (наприклад, між потребою у відеоспостереженні та правом на приватність);

– розгляд правових норм як результату постійного діалогу між старими (традиційними) і новими (цифровими) формами правоохоронної діяльності.

Правоохоронна діяльність у цифрову добу характеризується наявністю об’єктивних суперечностей, наприклад: між ефективністю контролю та дотриманням прав людини; між автоматизацією процесів (ШІ, аналітика, відеоспостереження) та необхідністю людського контролю; між технічними можливостями ІКТ і нормативними обмеженнями чинного законодавства. Застосування діалектичного методу дає змогу проаналізувати ці суперечності не як проблему, а як рушійну силу розвитку права, що стимулює формування нових теоретичних концепцій (наприклад, «цифрового правопорядку») і вдосконалення законодавства.

У межах діалектичного підходу важливо досліджувати категоріальний апарат теми в розвитку. Це означає, що такі поняття, як: «інформаційно-комунікаційні технології», «правоохоронний орган», «інформаційна безпека», «інформаційні права громадян» розглядаються не як сталі визначення, а як поняття, що еволюціонують унаслідок розвитку техніки, зміни суспільних відносин і трансформації правових принципів. Категорії діалектики є універсальними логічними формами мислення, в яких відображені ті загальні властивості, відношення і зв’язки, які існують в об’єктивній реальності. Без понять і категорій, як стверджує М. В. Костицький, пізнання дійсності було б неможливим [11]. Таким чином, діалектичний метод дає змогу осмислити перехід від традиційної правоохоронної діяльності до цифрової як закономірний етап розвитку правової системи.

Метафізичний метод у правознавстві традиційно розглядається як такий, що ґрунтується на аналізі явищ у статиці, тобто в їхньому відносно сталому стані,

без урахування постійного розвитку чи змін. На відміну від діалектичного підходу, який досліджує право як динамічне, мінливе явище, метафізичний метод зосереджується на виявленні сутнісних, незмінних властивостей правових категорій, закономірностей і структур, що визначають стабільність правової системи.

У контексті дослідження теоретико-правових засад впровадження і використання інформаційно-комунікаційних технологій у правоохоронній діяльності, застосування метафізичного методу має важливе значення. Він дозволяє:

– виділити базові, незмінні принципи функціонування правоохоронної системи, які повинні залишатися сталими незалежно від технічного прогресу (наприклад, принцип законності, верховенства права, забезпечення прав людини);

– проаналізувати структуру правового регулювання ІКТ, визначивши його основні елементи – суб'єкти, об'єкти, механізми правового впливу, – у їхньому нормативному, логічно впорядкованому стані;

– оцінити межі правового втручання у сферу цифровізації правоохоронної діяльності, встановити сталі юридичні категорії (такі як «інформаційно-комунікаційні технології в діяльності правоохоронних органів», «принципи використання інформаційно-комунікаційних технологій у діяльності правоохоронних органів», «правова основа інформаційно-комунікаційних технологій в діяльності правоохоронних органів») як системоутворюючі елементи;

– сформулювати логічно завершену модель правового регулювання використання ІКТ, яка базується на системі незмінних засад, що гарантують узгодженість, стабільність і передбачуваність діяльності правоохоронних органів.

Отже, метафізичний метод дає можливість розглядати ІКТ не лише як технологічний феномен, а як елемент сталого правопорядку, що підпорядковується основоположним юридичним принципам. Його застосування

сприяє чіткому окресленню категоріального апарату дослідження, формулюванню чітких юридичних дефініцій і забезпеченню логічної узгодженості теоретико-правових конструкцій, що стосуються цифровізації правоохоронної діяльності [3]. Діалектичний і метафізичний методи виступають не кожен окремо, а в єдності, у певному зв'язку.

Специфіка загальнонаукового рівня методології полягає в тому, що саме на філософському рівні формулюються найбільш узагальнені способи наукового пізнання досліджуваних явищ, зокрема діалектичний та метафізичний методи. Зазначені методи виступають універсальним методологічним інструментарієм, який забезпечує комплексний, системний і логічно впорядкований аналіз правових процесів

Загальнонаукові методи застосовуються для обробки, узагальнення й інтерпретації наукових даних. До них належать аналіз, синтез, індукція, дедукція, класифікація, порівняльний і історичний методи. Вони сприяють виявленню закономірностей розвитку правових категорій, встановленню зв'язків між елементами системи правового регулювання використання ІКТ у діяльності правоохоронних органів.

Логічний метод посідає одне з провідних місць серед загальнонаукових методів пізнання, оскільки забезпечує послідовність, аргументованість і внутрішню узгодженість наукового дослідження. Його застосування дозволяє будувати систему доказів, формулювати поняття, усувати суперечності та логічно обґрунтовувати висновки, що є необхідним для будь-якого теоретико-правового аналізу [3]. У межах дослідження теоретико-правових засад використання інформаційно-комунікаційних технологій у правоохоронній діяльності логічний метод виступає універсальним інструментом, який супроводжує виклад матеріалу на всіх етапах – від формування категоріального апарату до побудови узагальнених висновків. Його зміст полягає у застосуванні логічних прийомів і процедур, серед яких: *аналіз* – для розчленування досліджуваних правових явищ на окремі елементи, зокрема для вивчення структури інформаційно-правових відносин, елементів правового статусу суб'єктів у сфері ІКТ, а також складових

інформаційної безпеки; *синтез* – для узагальнення отриманих результатів і формування цілісного уявлення про право як систему норм, що регулює цифрові процеси у правоохоронній сфері; *індукція* – для виведення загальних закономірностей на основі аналізу окремих прикладів правозастосовної практики; *дедукція* – для застосування загальних теоретичних положень до конкретних аспектів використання ІКТ у діяльності правоохоронних органів; *аналогія* – для встановлення подібності між окремими правовими явищами (наприклад, між традиційними та цифровими формами пошуку доказів).

Таким чином, логічний метод забезпечує внутрішню цілісність дослідження, надає можливість побудувати аргументовану систему понять і висновків, сприяє обґрунтованому формулюванню наукових положень і розкриттю сутності правових явищ у сфері цифровізації діяльності правоохоронних органів.

Дедукція передбачає логічний процес, у межах якого нові знання отримуються на основі вже відомих положень загального характеру. Іншими словами, це рух думки від загального до часткового, коли окремі правові явища пояснюються через загальні закономірності, принципи чи концепти, сформульовані на попередніх етапах наукового пізнання [12, с. 274].

В процесі дослідження теоретико-правових засад впровадження і використання інформаційно-комунікаційних технологій у правоохоронній діяльності, дедуктивний метод відіграє особливу роль. Він дозволяє виводити понятійний апарат даної проблематики із загальних теоретичних положень про сутність права, його функції та принципи правового регулювання. Крім того, за допомогою дедукції ми маємо змогу застосовувати фундаментальні засади теорії держави і права (зокрема, принципи законності, верховенства права, правової визначеності, пропорційності) до аналізу конкретних питань цифровізації правоохоронної сфери, а також логічно впорядковувати систему понять і категорій, пов’язаних із ІКТ у правоохоронній діяльності, визначаючи їх місце в загальній структурі правових інститутів;

Таким чином, дедуктивний метод є інструментом, який забезпечує послідовність, системність і логічну обґрунтованість наукового аналізу правових аспектів упровадження ІКТ у діяльність правоохоронних органів. Саме завдяки цьому методу можливо виявити, як загальні закономірності розвитку права реалізуються в специфічній сфері – цифровому забезпеченні реалізації правоохоронної функції держави.

Методи аналізу та синтезу посідають важливе місце серед загальнонаукових інструментів пізнання, оскільки забезпечують логічну послідовність, глибину та системність наукового дослідження. Їх застосування дозволяє не лише розчленувати складне правове явище на окремі елементи, а й об’єднати їх у цілісну теоретико-правову конструкцію.

Метод аналізу передбачає розподіл складного об’єкта на складові частини з метою їх самостійного дослідження. У межах теми використання ІКТ у діяльності правоохоронних органів цей метод дає змогу виокремити окремі елементи правового регулювання цифрових технологій – нормативні акти, принципи, інститути, правовідносини. Досліджується взаємозв’язок між правовими нормами, що регламентують використання ІКТ у різних правоохоронних органах (поліції, прокуратурі, СБУ тощо). Метод аналізу дозволяє з’ясувати зміст основних понять – «інформаційно-комунікаційні технології», «правоохоронні органи», «принципи ІКТ в правоохоронній діяльності», «штучний інтелект» тощо, а також визначити проблемні аспекти чинного законодавства у сфері цифровізації правоохоронної сфери.

Метод синтезу, у свою чергу, полягає в об’єднанні проаналізованих елементів у єдину систему. За його допомогою можливо узагальнити результати аналізу правових норм та практики їх застосування, сформувати цілісне уявлення про механізм правового забезпечення використання ІКТ правоохоронцями і виробити теоретичну модель ефективного впровадження ІКТ у діяльність органів правопорядку.

У поєднанні ці методи дозволяють поетапно досліджувати об’єкт від часткового до загального: аналіз забезпечує глибину та деталізацію, а синтез –

цілісність і системність теоретичного пізнання. Така взаємодія надає можливість сформулювати узагальнені висновки про закономірності правового регулювання цифрових технологій у правоохоронній сфері та розробити науково обґрунтовані пропозиції щодо вдосконалення законодавства України у цій галузі [13].

Застосування історичного (історико-правового) методу має особливе значення для вивчення процесів формування та розвитку правового регулювання використання інформаційно-комунікаційних технологій у діяльності правоохоронних органів. Сутність цього методу полягає у тому, що будь-яке правове явище розвивається у часовій послідовності, характеризується наступністю, незворотністю та наявністю внутрішніх суперечностей, які стають джерелом його подальшої еволюції [14, с. 23]. Історичний метод дозволяє відстежити розвиток правового регулювання інформаційних процесів у сфері правоохоронної діяльності – від перших нормативних актів, що встановлювали порядок обліку та збереження інформації, до сучасного законодавства щодо кібербезпеки, електронних доказів, захисту персональних даних та цифрових інструментів в оперативно-розшуковій роботі. Використання цього методу сприяє глибшому усвідомленню закономірностей формування правового статусу інформаційно-комунікаційних технологій у діяльності правоохоронних органів, а також дає змогу виявити ключові етапи, тенденції та фактори, що впливали на створення сучасної правової моделі їх застосування. Історико-правовий метод є невід’ємною складовою методології, виконуючи функцію історичного аналізу та критичного дослідження права, що дозволяє подолати застаріле й непродуктивне протиставлення «сучасної» та «традиційної» юридичної науки [15].

Використання історичного методу у дослідженні теоретико-правових засад використання ІКТ у діяльності правоохоронних органів дає змогу: розкрити еволюцію підходів до визначення дефініцій – від «технологія» до «інформаційно-комунікаційна технологія»; виявити закономірності розвитку правового регулювання у сфері інформаційної безпеки, електронного документообігу, використання баз даних і відеоаналітики; зрозуміти історичну взаємодію між технологічними досягненнями та правовими обмеженнями, що виникали у

процесі їх впровадження; визначити досвід зарубіжних держав у правовому врегулюванні цифрових інновацій в правоохоронній сфері та можливість його імплементації у національне законодавство.

Таким чином, історичний метод є не лише засобом ретроспективного аналізу, а й важливою методологічною основою для формування концептуальних положень подальшої цифрової трансформації правоохоронної діяльності. Його використання дає змогу дослідити генезу правового регулювання інформаційно-комунікаційних технологій у правоохоронній сфері, простежити розвиток наукових підходів, правових понять і категорій, а також виявити закономірності еволюції нормативної бази та практики її реалізації. Завдяки цьому можна обґрунтувати тяглість і спадкоємність правових процесів, окреслити провідні тенденції та чинники, що визначали становлення сучасного стану правового забезпечення застосування ІКТ у діяльності правоохоронних структур.

Необхідно також зазначити, що право становить для дослідників складну систему. У цьому зв’язку доречно вказати на необхідність відповідного системного пізнання, що дозволяє визначити природу та характер взаємозв’язків його елементів, розкрити функціональне призначення та ефективність дії кожного з компонентів та охарактеризувати право в цілому [16, с. 38]. Представники сучасної вітчизняної юридичної науки тлумачать системний метод як підхід, за якого всі державно-правові явища розглядаються у взаємозв’язку – як елементи єдиної системи. У цьому контексті держава, право та їхні інституційні складові постають як відкриті системи, що включають підсистеми нижчого рівня та водночас входять до ширших соціально-правових утворень. Застосування системного методу дає змогу всебічно простежити взаємодію держави й права як складного багаторівневого процесу, виявити внутрішні й зовнішні закономірності їх розвитку, а також з’ясувати причинно-наслідкові зв’язки між окремими державно-правовими явищами [13, с. 15]. Застосування системного методу передбачає розгляд правових явищ не ізольовано, а як структурні компоненти цілісної правової системи, де кожен елемент має своє місце, функцію та взаємодіє з іншими. У контексті теми даного дослідження,

системний метод дозволяє розглядати ІКТ як елемент єдиної системи інформаційно-технічного забезпечення правоохоронній діяльності, а також виявляти взаємозв'язок між технологічними, організаційними та правовими її компонентами, визначаючи, як зміни в одній підсистемі (наприклад, технологічній) впливають на інші (нормативну або інституційну).

Порівняльно-правовий метод є одним із найважливіших спеціальних методів юридичного пізнання, що дає можливість досліджувати правові явища шляхом зіставлення різних правових систем, інститутів і підходів до правового регулювання певних суспільних відносин. У контексті нашого дослідження цей метод має особливе значення. Він допомагає виявити спільні та відмінні риси правового регулювання ІКТ у правоохоронній сфері різних держав, визначити загальні закономірності цифрової трансформації правоохоронних органів, а також з'ясувати, які підходи зарубіжного досвіду можуть бути ефективно імплементовані у вітчизняну практику. Особливого значення цей метод набуває в умовах інтеграції України в Європейський безпековий простір, адаптації вітчизняного законодавства до законодавства Європейського Союзу, а також використання окремих елементів позитивного досвіду з урахуванням національних традицій та особливостей. Наприклад, шляхом порівняння можна встановити тенденції розвитку правового забезпечення цифровізації правоохоронних систем у провідних державах світу (США, Канада, Німеччина, Франція тощо) та зіставити їх із національною моделлю. Таким чином, створюються передумови для гармонізації українського законодавства із правом Європейського Союзу, з урахуванням міжнародних стандартів у сфері захисту персональних даних, цифрової безпеки та прав людини, а також виявляються потенційні ризики та колізії, які можуть виникнути під час запозичення іноземного досвіду без урахування національної правової традиції. Порівняльно-правовий метод дає змогу не лише описати іноземний досвід, а й глибше осмислити природу вітчизняного правового регулювання ІКТ, визначити його сильні та слабкі сторони, сформулювати пропозиції щодо вдосконалення національної нормативної бази.

На підставі вищенаведеного можна дійти висновку, що методологічна основа цього дослідження включає систему підходів, принципів і методів, які дають змогу дослідити використання ІКТ не лише з технічної чи організаційної точки зору, а передусім – у контексті правової легітимності, етичності та відповідності демократичним стандартам. Особливої значущості набуває розуміння методології як засобу забезпечення єдності теорії й практики. Теоретико-правові положення, що розробляються у процесі дослідження, мають бути перевірені через аналіз реального нормативного масиву, практики його застосування та наслідків цифровізації для забезпечення правопорядку і громадської безпеки. У цьому аспекті методологічні засади виконують функцію своєрідного «містка» між науковим осмисленням і практичною реалізацією ІКТ у діяльності правоохоронних органів.

Таким чином, методологічні засади впровадження і використання ІКТ в діяльність правоохоронних органів – це не просто набір методів і прийомів, а цілісна система наукових орієнтирів, спрямованих на розкриття закономірностей цифровізації правоохоронної діяльності, з урахуванням її теоретико-правових, етичних, соціальних і безпекових аспектів. Вони визначають структуру дослідження, логіку формулювання висновків і практичних рекомендацій, забезпечуючи наукову новизну й обґрунтованість отриманих результатів.

1.2 Поняття, зміст та завдання інформаційно-комунікаційних технологій у діяльності правоохоронних органів

Розвиток правової системи сучасної держави дедалі більше зумовлюється впливом цифрових технологій, які трансформують як механізми державного управління, так і способи забезпечення правопорядку. Інформаційні та комунікаційні технології стали не лише інструментом підвищення ефективності протидії злочинності, а й важливим чинником у забезпеченні дотримання прав і свобод людини. Правоохоронні органи, традиційно перебуваючи в авангарді

впровадження новітніх технологічних рішень, відіграють визначальну роль у гарантуванні державної та громадської безпеки.

У цьому контексті, цифровізація правоохоронної діяльності вимагає не лише технічного, а й системного оновлення правового регулювання. Відсутність чітко визначеної нормативно-правової основи застосування ІКТ у роботі органів правопорядку, разом із неврегульованістю базових понять і термінів у законодавстві, породжує стан правової невизначеності. Це, у свою чергу, становить загрозу для реалізації принципу верховенства права, адже технологічні інновації розвиваються швидше, ніж їх належне правове осмислення та контроль. У зв'язку з цим особливої ваги набуває формування цілісної правової політики цифровізації правоохоронного сектору, яка має охоплювати не лише технічні аспекти впровадження ІКТ, а й питання етичної відповідальності, захисту даних, безпеки та незалежного нагляду за їх використанням.

Наприкінці минулого століття цифрові технології стали настільки поширеними, що у 1990-х роках правознавці почали говорити про появу наступного покоління прав людини, так званих «цифрових прав», а на початку 2000-х років – розробляти перші концепції щодо цієї правової проблеми. Насамперед це відображено в працях зарубіжних науковців, таких як: S. A. Saxby [17], J. P. Barlow [18], L. Lessig [19]. Водночас, увагу фахівців почали привертати не лише переваги, а й загрози, які несе використання цифрових технологій. Зазначені застереження ґрунтувалися на практиці протидії злочинності, у межах якої злочинні угруповання почали активно використовувати технології у своїй протиправній діяльності. Наукова думка тих років сформувала переконання щодо небезпеки неконтрольованого використання цифрових технологій, у зв'язку з чим значна кількість досліджень була присвячена боротьбі з цифровою злочинністю в Інтернеті [20], [21], [22].

У сучасній науковій літературі, присвяченій розвитку цифрових технологій у сфері права, виокремлюється кілька основних напрямів дослідження, що відображають різні аспекти цифрових трансформацій: вплив цифрових технологій на функціонування сучасних держав; їхній вплив на еволюцію

правової системи; а також вплив процесів цифровізації на правотворчу та правозастосовну діяльність у публічній і приватно-правовій сферах. На сучасному етапі результативність діяльності правоохоронних органів значною мірою залежить від рівня інформаційного забезпечення та технічної оснащеності. Застосування ІКТ у цій сфері характеризується низкою специфічних рис і особливостей. У зв'язку з цим видається доцільним насамперед уточнити зміст понять «правоохоронна діяльність» і «правоохоронний орган» у межах даного дисертаційного дослідження.

Окремі аспекти правоохоронної діяльності та правового статусу правоохоронних органів були предметом наукових досліджень низки вітчизняних учених і практиків, зокрема О. М. Бандурки, В. В. Ковальської, Р. А. Калюжного, М. Гірича, А. М. Кучука, О. А. Мартиненка, М. І. Мельника, В. В. Нагорної, В. Я. Тація, П. І. Хамули та інших. Водночас, попри наявність значного масиву наукових публікацій і сталий інтерес до зазначеної проблематики, низка ключових питань і дотепер залишається недостатньо розробленою та дискусійною.

Методологічні та правові проблеми у вивченні правоохоронної діяльності та правоохоронних органів пов'язані насамперед з відсутністю однакового розуміння та тлумачення основних понять і термінів, а також неоднозначністю законодавчого закріплення вищезазначених категорій.

Так, для одних авторів правоохоронна діяльність – це будь-яка діяльність, пов'язана з охороною та забезпеченням права; для інших – це діяльність компетентних державних органів у сфері боротьби зі злочинами та правопорушеннями; для третіх – це діяльність з охорони громадського порядку. Відповідно, неоднозначно розв'язується питання і про систему органів, які здійснюють в Україні правоохоронну діяльність. Керуючись критеріями обсягу предмета та сфери дії, традиційно виділяють вузький та широкий підходи до розуміння зазначеного поняття [23]. У юридичній літературі правоохоронна діяльність у вузькому значенні визначається як діяльність спеціально уповноважених органів (державних та недержавних) з метою охорони прав і

свобод громадян, правопорядку та забезпечення законності, що реалізується в установленій законом формі та в межах повноважень, наданих цим органам. Представниця цього підходу В. В. Ковальська визначає правоохоронну діяльність як безперервну, узгоджену діяльність державних і недержавних органів і організацій, спрямовану на створення максимально сприятливих умов для безперешкодної реалізації правових норм, суб'єктивних прав і свобод, профілактику та виявлення правопорушень з метою попередження, припинення, ліквідації їх наслідків, поновлення прав, відшкодування збитків, покарання винних [24].

У широкому значенні правоохоронна діяльність – це діяльність всіх державних органів та недержавних організацій щодо забезпечення дотримання прав і свобод громадян, їх реалізації, забезпечення законності та правопорядку. Наприклад, у «Юридичній енциклопедії» за редакцією Ю. С. Шемшученка поняття правоохоронної діяльності визначено у широкому розумінні, а саме як система заходів, спрямованих на забезпечення виконання Конституції України, законів та інших нормативно-правових актів держави [25].

На підставі викладеного ми вважаємо за доцільне зауважити, що одним із напрямів правоохоронної діяльності є захист прав і свобод людини й громадянина, забезпечення автономності особи як суб'єкта громадянського суспільства. Правоохоронні органи захищають права і свободи людини й громадянина шляхом здійснення конкретних слідчих, оперативно-розшукових та інших дій. Такого роду дії є елементами правоохоронної діяльності та спрямовані: з одного боку, на припинення, профілактику правопорушень у сфері прав і свобод людини й громадянина, а з іншого – на відновлення порушеного права протиправними посяганнями і притягнення до юридичної відповідальності правопорушника [26]. Отже, правоохоронна діяльність є ширшим поняттям, оскільки охоплює всю діяльність із забезпечення правопорядку та захисту прав і свобод, яку можуть здійснювати різні суб'єкти. Діяльність правоохоронних органів є вужчим поняттям і стосується реалізації відповідних функцій конкретними правоохоронними інституціями в межах їхніх повноважень.

Чинне законодавство також не надає однозначної і чіткої відповіді на питання про те, який орган публічної влади слід вважати правоохоронним, що, своєю чергою, породжує дискусії щодо сутнісних ознак поняття і, відповідно, його змісту.

Так Закон України «Про державний захист працівників суду і правоохоронних органів» надає наступний перелік: «Правоохоронні органи – органи прокуратури, Національної поліції, Служби безпеки України, Військової служби правопорядку у Збройних Силах України, Національне антикорупційне бюро України, органи охорони державного кордону, Бюро економічної безпеки України, органи і установи виконання покарань, слідчі ізолятори, органи державного фінансового контролю, рибоохорони, державної лісової охорони, інші органи, які здійснюють правозастосовні або правоохоронні функції.» [27]. В свою чергу, Закон України «Про контррозвідувальну діяльність» [28], у частині 4 статті 5 зазначає: «правоохоронні та інші органи державної влади, органи місцевого самоврядування, підприємства, установи та організації України, незалежно від форми власності, в межах, визначених законами України та іншими нормативно-правовими актами, сприяють органам і підрозділам Служби безпеки України у проведенні контррозвідувальної діяльності в інтересах забезпечення державної безпеки».

До 2018 року тлумачення терміну «правоохоронні органи» можна було віднайти в Законі України «Про основи національної безпеки України» (втратив чинність 08.07.2018): «правоохоронні органи – органи державної влади, на які Конституцією і законами України покладено здійснення правоохоронних функцій». Водночас, Порядок проведення інспектування Державною аудиторською службою, її міжрегіональними територіальними органами, затверджений Постановою Кабінету Міністрів України від 20 квітня 2006 р. № 550 містить таке визначення: «правоохоронні органи – органи прокуратури, служби безпеки, Національної поліції, Бюро економічної безпеки, Національне антикорупційне бюро, інші утворені відповідно до законодавства органи, які здійснюють правоохоронні функції» [29]. Отже, аналіз вітчизняного

законодавства, дає підстави стверджувати, що законодавець відносить правоохоронні органи до державних органів, що здійснюють правоохоронні чи правозастосовні функції [30, с. 53], тоді як науковці схильні використовувати більш розширений зміст цього терміну.

Як свідчить аналіз наукової літератури найчастіше поняття правоохоронного органу фахівці пов'язують із поняттям правоохоронної діяльності. Деякі науковці до правоохоронних органів відносять лише ті, які ведуть боротьбу зі злочинністю та правопорушеннями, результатами якої є юридична відповідальність у межах кримінально-процесуального й адміністративного законодавства (М. І. Мельник та М. І. Хавронюк) [31, с. 31]. Також є думка, що до правоохоронних слід відносити лише ті органи, службовці яких займаються професійною діяльністю, що спрямована на виконання спеціальних завдань (О. М. Бандурка). Натомість у межах широкого розуміння правоохоронними визнаються всі органи держави, органи місцевого самоврядування та самоорганізації населення, які здійснюють правоохоронну діяльність, тим чи іншим чином реалізують чи сприяють реалізації правоохоронної функції [23]. Отже, класифікація суб'єктів правоохоронної діяльності здебільшого здійснюється за критерієм наявності/відсутності владних повноважень. За цим критерієм суб'єкти правоохоронної діяльності поділяються на суб'єктів правоохоронної діяльності, які наділені владними повноваженнями – правоохоронні органи (поліція, Служба безпеки України, прокуратура та інші) та суб'єктів правоохоронної діяльності, які владних повноважень не мають – правоохоронні організації (адвокатура, Асоціація юристів та інші).

Вагомий внесок у порівняльний аналіз та наукову розробку понять «правоохоронні органи», «правозахисні органи», «органи охорони правопорядку» було зроблено членами Комісії з питань правоохоронної діяльності Конституційної Асамблеї (Комісія) під керівництвом академіка НАН України В. Я. Тація. Науковець зазначав, що поняття «правоохоронні органи» є одним із найбільш невизначених в українському правознавстві, внутрішньо суперечливим і надмірним за обсягом. Внаслідок такої невизначеності цього

поняття у Конституції та законах України, а також відсутності визначеного суб'єктного складу, виникає певна конкурентність термінів – «правоохоронні органи», «правозахисні органи», «органи кримінальної юстиції» тощо. Як результат, до системи правоохоронних органів належать різні за своїм статусом та функціональним призначенням органи, що унеможливлює чітке визначення їх системи [32]. У Доповіді Комісії відмічалося, що критерієм виокремлення правоохоронних органів не може бути виконання лише правоохоронних функцій, які так чи інакше здійснюють усі державні органи, насамперед, виконавчої влади. Внаслідок широкого тлумачення правоохоронної функції як визначальної ознаки правоохоронних органів, до них почасти включаються майже всі органи виконавчої влади, які тією чи іншою мірою займаються виконанням цих функцій або займаються правоохоронною діяльністю. З метою усунення цієї термінологічної колізії та правової невизначеності, Комісією було запропоновано збереження та застосування поняття «правоохоронні органи» лише як узагальнюючого та наукового. Натомість, у законодавчому й правозастосовному процесах – відмовитися від терміну «правоохоронні органи», здійснити поділ цієї системи органів, використовуючи як основні критерії для виокремлення певних класифікаційних груп конкретні функції, які вони виконують, та їх призначення в механізмі охорони права [32]. У зв'язку з цим, було запропоновано виділити із правоохоронних органів в окрему інституційну групу органи охорони правопорядку, оскільки, на відміну від інших органів виконавчої влади, для них: а) правоохоронна функція є основною і такі органи безпосередньо здійснюють повноваження, спрямовані на захист прав і свобод людини та охорону правопорядку; б) внаслідок цього органи охорони правопорядку мають право легального застосування сили та примусу; в) у своєму складі вони мають відповідні озброєні формування [33].

Ми погоджуємось з позицією науковців, які вважають що право завжди пов'язане з примусом, впливом, хоча і є за своєю сутністю мірилом рівності та справедливості. А тому мають існувати інституції, що будуть охороняти право (у тому числі ще з додержавницького періоду розвитку суспільства, а також в

протодержаві). Зазначене дає підстави для висновку, що не лише держава, але й саме суспільство може здійснювати охорону права [34].

Однак, в рамках цього дисертаційного дослідження ми будемо вживати термін «правоохоронні органи» в контексті його вузького розуміння, а саме: спеціально уповноважені державні органи, наділені державно-владними повноваженнями, які на професійній основі, на підставі та відповідно до вимог законодавства, а у випадках, прямо передбачених законом, – у встановленій процесуальній формі із застосуванням правових засобів, здійснюють діяльність, спрямовану на забезпечення охорони прав і свобод людини та громадянина, законності й правопорядку, а також усіх суспільних відносин, врегульованих нормами права.

Варто зазначити, що для ефективного дослідження змісту та значення ІКТ в діяльності правоохоронних органів, необхідно розуміти також суть і правову природу базових понять: «технологія», «інформаційна технологія» та «інформаційно-комунікаційні технології». На жаль, сучасна юридична наука і національне законодавство не мають єдності у визначенні понятійно-категоріального апарату в інформаційному праві, зокрема у тлумаченні зазначених термінів. Як влучно зазначає К. В. Юдкова: «Це призводить до неоднозначного, подвійного тлумачення понять. А в тих випадках, коли поняття, терміни є визначальними не тільки для позначення сфери чи зони правового регулювання, а й для виокремлення з-поміж інших специфічного об’єкта правового регулювання, – недостатня чіткість визначення призводить до плутанини на етапі правозастосування» [35].

Незважаючи на своє порівняно недавнє походження поняття «технологія» міцно увійшло в терміносистему різних областей знань і напрямів людської діяльності. Поява цього терміну і його еволюція яскраво ілюструє розвиток людського суспільства. Термін «технологія» є комбінацією двох грецьких слів: technë – мистецтво, майстерність, уміння + logia – наука. До початку XX ст. термін «технологія» набув широкого поширення у багатьох розвинених країнах і включав в себе все зростаючу кількість процесів, а також знаряддя і машини.

Часто ототожнювалися поняття «техніка» і «технологія». У вітчизняній науковій традиції склалися поняття техніки як комплексу матеріальних речей і технології – як сукупність методів, прийомів, способів. Техніка розглядалася як матеріальний носій технології. В Україні з кінця XVII ст. з'явилося досить багато перекладної іноземної літератури, яка вплинула на наукову термінологію, але в наукову літературу цей термін був введений тільки на початку XIX ст. У сучасному розумінні *технологія* – це сукупність засобів, процесів, операцій, методів, прийомів, режим роботи, за допомогою яких елементи, які входять у виробництво, перетворюються у вихідні; вона охоплює машини, механізми та інструменти, навички і знання [36].

Перше використання терміну «інформаційна технологія» датується кінцем 1970-х рр., і до цього часу в різних джерелах має доволі широке трактування. Багато авторів ототожнюють поняття «комп'ютерна технологія» і «інформаційна технологія». Інші шукають відмінності і намагаються визначити ці дефініції через мету і сферу застосування. За визначенням H. L. Poppel та B. Goldstein інформаційні технології – це використання обчислювальної техніки та систем зв'язку для створення, збору, передачі, зберігання та обробки інформації для всіх сфер суспільного життя [37]. Вітчизняний науковець В. Ю. Триняк визначає інформаційні технології як «конкретні способи й механізми оперування інформацією, які мають безпосередньо культурогенний, гносеогенний та автогенеративний характер». При цьому автор в своїх працях ототожнює це поняття з поняттям ІКТ [38].

Науковець В. А. Баженов пропонує під інформаційними технологіями розуміти «методи та способи, що використовують комп'ютерні програмно-технічні засоби, окремі або сукупні інформаційні процеси та операції для досягнення поставленої мети» [39]. Своєю чергою О. О. Берназюк використовує термін «цифрові технології», визначаючи їх як: «законодавчо урегульований та організований процес застосування державними органами та органами місцевого самоврядування, іншими суб'єктами публічного управління засобів комп'ютерної та іншої електронно-обчислювальної техніки, програмного

забезпечення, інформаційно-комунікаційних мереж та інших цифрових засобів з метою збирання, фіксації, обробки, зберігання та поширення правової інформації, а також створення документів в електронній формі» [40].

Інші автори під інформаційними технологіями розуміють «сукупність територіально розрізнених кінцевих систем, об'єднаних інформаційною мережею, за допомогою якої забезпечується взаємодія прикладних процесів, активізованих у кінцевих системах, та їх колективний доступ до ресурсів мережі» [41]. Наприклад, К. В. Юдкова пропонує розуміти під інформаційними технологіями «цілеспрямовану сукупність інформаційних процесів та методів створення, пошуку, отримання, передачі, збору, обробки, накопичення, зберігання, розповсюдження, використання та захисту інформації» [35]. На думку О. В. Синєокого, «інформаційна технологія – це процес, що використовує сукупність засобів і методів збирання, оброблення і передавання даних (первинної інформації) для одержання інформації нової якості про стан об'єкта, процесу або явища (інформаційного продукту)» [42].

Отже, в науковій літературі широко використовуються терміни: «інформаційні технології», «інформаційно-комунікаційні технології», «комп'ютерні технології», «цифрові технології», «мережні технології», «новітні технології» тощо. Але, переважним чином, ними позначають однакові соціально-економічні явища. До прийняття нової редакції Закону України «Про Національну програму інформатизації» від 01.12.2022, який ввів термін «Інформаційно комунікаційна технологія», у правовому полі тривалий час існував лише термін «інформаційна технологія», роль якої науковці пов'язували з кількома основними напрямами. Зокрема, інформаційні технології розглядалися як галузь матеріального виробництва, орієнтована на розвиток процесів виробництва, розподілу та споживання, а також як каталізатор розвитку інформаційного суспільства й економіки. Водночас вони трактувалися як елемент загальної правової терміносистеми та як самостійний об'єкт правового регулювання, до якого застосовуються норми цивільного права. Крім того, інформаційні технології визнавалися основою перетворення й накопичення

інформаційних ресурсів, забезпечення інформаційної безпеки та формування національного й глобального інформаційного простору [35].

Наприкінці 90-х років минулого століття в міжнародних документах, присвячених регулюванню інформаційних відносин, з'являється термін «комунікація», що означає передачу повідомлення за допомогою мови та інших знакових систем. Так, Організація економічного співробітництва і розвитку (OECD) у 1998 р. дала визначення терміну інформаційних і комунікаційних технологій як: «технологій, що використовують засоби мікроелектроніки для збору, зберігання, обробки, пошуку, передачі і представлення даних, текстів, образів, звуку» [43].

ЮНЕСКО у документі «Керівництво з вимірювання інформаційно-комунікаційних технологій (ІКТ) в освіті» (2009 р.) визначає ІКТ як різноманітний набір технологічних засобів і ресурсів, які використовуються для передачі, зберігання, створення, спільного використання або обміну інформацією. Ці технологічні інструменти та ресурси включають комп'ютери, Інтернет (веб-сайти, блоги та електронні листи), технології прямого мовлення (радіо, телебачення та веб-мовлення), технології записаного мовлення (подкастинг, аудіо- та відеопрогравачі та пристрої зберігання даних) і телефонію (стаціонарну або мобільну), супутник, відео/відеоконференції тощо) [44]. Виходячи з цього, слід констатувати, що зміст поняття ІКТ включає сукупність методів і процесів, призначених для виконання операцій, пов'язаних з інформацією.

У вітчизняному законодавстві визначення терміну «інформаційні технології» містилось в Закону України «Про Національну програму інформатизації» від 04.02.1998 (втратив чинність) в такій редакції: «інформаційна технологія – цілеспрямована організована сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування». Як бачимо, тут поняття інформаційної технології визначається

через інформаційні процеси, тобто сукупності дій, пов'язаних із створенням, обробкою, передачею, зберіганням і знищенням інформації. На сьогодні в Україні діє новий Закон України «Про Національну програму інформатизації» від 01.12.2022. У новій редакції застаріле поняття «інформаційна технологія» замінено на термін *«інформаційно-комунікаційні технології»*, які визначаються як «результат інтелектуальної діяльності, сукупність систематизованих наукових знань, технічних, організаційних та інших рішень про перелік та послідовність виконання операцій для збирання, обробки, накопичення та використання інформаційної продукції, надання інформаційних послуг». Отже, на відміну від першого варіанту терміну, ІКТ це вже результат певної інтелектуальної діяльності, а не тільки процес роботи з інформацією. Крім того, документ доповнено поняттям «цифрова технологія», якою є «…сукупність систематизованих правових, науково-технічних, організаційних рішень, спрямованих на застосування комп'ютерної та іншої електронно-обчислювальної техніки, програмного забезпечення та інших засобів для зменшення участі користувача інформаційно-комунікаційних систем і засобів інформатизації під час збирання, приймання, обробки, передавання інформації чи трудомісткості виконуваних операцій» [45].

Треба зазначити, що низка сучасних науковців віддають перевагу термінам «цифрові технології», «комп'ютерні технології», «нові інформаційні технології», а не терміну «інформаційно-комунікаційні технології», зазначаючи, що цифрові технології є найбільш динамічними та швидко розвиваються технологіями у сфері телекомунікацій. та інформатизації суспільства. Але, цифрові і інформаційно-комунікаційні технології не є ідентичними поняттями. Вони співвідносяться як загальне і окреме, де ІКТ виступає більш широким за своїм змістом явищем, а цифрові технології – його складовою, оскільки термін «інформаційно-комунікаційні технології», на відміну від цифрових технологій, включає й інші технології, призначення яких полягає у виконанні інформаційних операцій.

З огляду на вищесказане та враховуючи оновлене і розширене визначення Законом України «Про Національну програму інформатизації» термінології, вважаємо за доцільне використовувати у цьому дослідженні саме термін «інформаційно-комунікаційні технології (ІКТ)» для позначення процесів роботи з інформацією за допомогою електронних технічних засобів.

У сучасну інформаційну епоху модернізація нормативного забезпечення інформаційних відносин має ґрунтуватися на визначенні пріоритетності розвитку інформаційних технологій. З огляду на це, подальше правове регулювання ІКТ в юридичній діяльності, в тому числі і правоохоронній сфері має бути спрямовано на дотримання конституційних прав людини [46, с.216], а саме:

– вільно збирати, зберігати, використовувати і поширювати інформацію (ст. 34 Конституції України);

– право на доступ до публічної інформації та здійснення громадського контролю громадянами і громадськими організаціями за діяльністю органів державної влади (ст.38,40 Конституції України);

– захист авторських прав і прав майнової власності на інформаційні технології, інформаційні ресурси, продукти і послуги, технічні та інші засоби забезпечення інформаційної безпеки (ст. 54 Конституції України);

– формування рівних умов для усіх суб’єктів інформаційної діяльності (незалежно від форми власності) шляхом створення національного ринку інформаційних технологій, продуктів і послуг, конкурентного середовища та проведення ефективної антимонопольної політики (ст.42 Конституції України) [47];

– забезпечення відповідальності суб’єктів єдиного інформаційного простору за правопорушення при створенні інформаційних технологій, продуктів і послуг, формуванні інформаційних ресурсів та їх використанні;

– розвиток систем міжнародної і колективної інформаційної безпеки та інформаційного обміну в системі міжнародного співробітництва [48].

Виходячи з законодавчого визначення ІКТ як результату інтелектуальної діяльності, сукупності систематизованих наукових знань, технічних, організаційних та інших рішень, можна зробити висновок, що основними об'єктами застосування ІКТ є: первинна інформація (придатна для автоматизованої обробки); новостворений інформаційний продукт; відповідне програмне забезпечення; засоби збирання, накопичення, поширення, доступу до інформації та її зберігання, незалежно від місця її розташування.

У наукових джерелах прийнято розрізняти дві основні складові сучасних інформаційно-комунікаційних технологій: інфраструктура, яка забезпечує процеси збору, обробки, накопичення, розосередження, зберігання, пошуку і поширення інформації; та інформаційні відносини, які виникають під час застосування цих технологій [48]. Таким чином, інформаційно-комунікаційна технологія не може існувати і функціонувати сама по собі, а лише в сукупності з інформацією (будь-якими даними) та відповідною інфраструктурою, яка визначається специфікою діяльності її суб'єктів, від яких залежить виготовлення та постачання інформаційного продукту, а також його обіг за допомогою інформаційної технології.

У контексті правоохоронної діяльності ці взаємозв'язки набувають особливої специфіки: роль суб'єкта інформаційної діяльності виконують правоохоронні органи, робота яких спрямована на забезпечення публічної безпеки, протидію злочинності, захист прав і свобод громадян. Саме тому структура, функції та зміст ІКТ у правоохоронній сфері визначаються потребами цієї діяльності. Таким чином, функціональне призначення інформаційно-комунікаційних технологій у діяльності правоохоронних органів полягає у цілеспрямованому та ефективному використанні цифрових інструментів для підвищення результативності, оперативності, точності прийняття рішень, а також рівня прозорості та підзвітності правоохоронних органів у сучасному цифровому середовищі.

Велика різноманітність технологій потребує певної систематизації для подальшого визначення їх правового режиму. У науковій літературі існують

спроби класифікації ІКТ за різними критеріями. Так, К. В. Юдкова пропонує враховувати те, на вирішення яких задач спрямовані інформаційні технології:

– інформаційні технології глобального типу, які об'єднують собою методи і способи формалізації інформаційних ресурсів та використовуються суспільством;

– інформаційні технології, які є платформою для подальшого використання конкретних інформаційних технологій або використовуються в окремих галузях виробництва, науки тощо;

– спеціальні інформаційні технології, що спрямовані на вирішенні конкретних завдань, зокрема планування, облік, аналіз на базі «платформних» інформаційних технологій [49].

Українські вчені Д. В. Риндюк та В. А. Пешко поділяють ІКТ за типом інформації на: текстові, табличні, графічні, звукові, відео та мультимедійні дані. Залежно від видів використовуваних мереж інформаційні технології поділяють на: локальні, регіональні, корпоративні, національні, міжнаціональні (міжнародні), однорангові, багаторівневі, розподілені та інші [36].

На наш погляд усі інформаційно-комунікаційні технології, що застосовуються правоохоронними органами, можна поділити на: *загальні (базові чи універсальні)*, які можуть використовуватися практично у будь-якій сфері діяльності людини (наприклад, офісне програмне забезпечення (текстові редактори, електронні таблиці, бази даних); електронна пошта, месенджери та корпоративні комунікаційні платформи (Teams, Zoom, Slack); хмарні сервіси для зберігання та обміну інформацією (Google Drive, OneDrive); Інтернет та локальні мережі для обміну інформацією та доступу до ресурсів), а також *спеціальні* інформаційні технології, розроблені безпосередньо для застосування у правоохоронній діяльності з урахуванням її специфіки. Наприклад:

1) автоматизовані інформаційні системи (АІС), такі, як: Єдиний реєстр досудових розслідувань (ЄРДР), бази ДНК та відбитків пальців для криміналістики, реєстри обліку зброї, автотранспорту та правопорушників;

2) системи електронного документообігу для внутрішніх процесів органів правопорядку;

3) експертні системи на основі штучного інтелекту для підтримки слідства та прогнозування злочинів;

4) системи відеоспостереження та розпізнавання облич (FRT, CCTV, системи аналітики відеопотоку);

5) телекомунікаційні системи та засоби контролю за мережевою інформацією (моніторинг Інтернету, перехоплення комунікацій у межах закону);

6) платформи для кримінальної аналітики та прогнозування (Big Data Analytics для правоохоронних задач) тощо.

Завдання використання інформаційно-комунікаційних технологій у діяльності правоохоронних органів випливають із загальної логіки функціонування держави в умовах цифрової трансформації, а також із нормативно-правових засад, що визначають повноваження та обов'язки правоохоронних органів. Водночас формування таких завдань відбувається з урахуванням міжнародних стандартів і рекомендацій ООН, Ради Європи, Інтерполу, Європолу, а також вимог інформаційної безпеки, закріплених у стандартах ISO/IEC (International Organization for Standardization – Міжнародна організація зі стандартизації; International Electrotechnical Commission – Міжнародна електротехнічна комісія).

Виходячи з цього, вважаємо, основними завданнями використання інформаційно-комунікаційних технологій правоохоронними органами є забезпечення:

1. *інформаційної діяльності* як процесу збирання, обробки та зберігання інформації. Реалізація цього завдання передбачає формування єдиних підходів до збирання, обробки й зберігання даних, а також впровадження сучасних інструментів автоматичного моніторингу інформаційних ресурсів, зокрема відкритих джерел, для своєчасного виявлення потенційних загроз і правопорушень;

2. *аналітичної діяльності* як процесу встановлення причинно-наслідкових зв'язків, логічної побудови та виявлення тенденцій розвитку досліджуваного явища. У межах цієї діяльності особливого значення набуває створення спеціалізованих аналітичних підрозділів, здатних опрацьовувати складні інформаційні масиви, розробляти єдині методики кримінально-аналітичного аналізу та забезпечувати підготовку фахівців у сфері цифрової аналітики й кіберрозвідки;

3. *інформаційно-технічного забезпечення* як сукупності автоматизованих систем обробки інформації, програмно-апаратних комплексів і програмно-технічних засобів. Йдеться про розробку комплексних механізмів кіберзахисту, проведення аудиту інформаційних потоків, упровадження блокчейн-технологій, створення єдиної платформи відомчих баз даних, що гарантуватиме узгодженість і достовірність інформації. Важливо також передбачити належний державний контроль за сертифікацією програмно-технічних засобів, які використовуються у правоохоронній діяльності.

Комплексна реалізація цих напрямів сприятиме формуванню сучасної моделі цифрової трансформації правоохоронної системи, яка забезпечить її відкритість, безпеку та здатність ефективно реагувати на виклики інформаційного суспільства.

Отже, узагальнюючи викладене, пропонуємо визначити термін «*інформаційно-комунікаційні технології в діяльності правоохоронних органів»* як сукупність наукових, технічних, програмних і організаційних рішень, що використовуються для збирання, обробки, зберігання, передачі та аналізу інформації або створення нового інформаційного продукту з метою забезпечення законності, правопорядку, оперативного реагування на правопорушення, підтримки розслідувань і прийняття управлінських рішень у правоохоронних структурах.

Визначене поняття дозволяє не лише окреслити загальні риси інформаційно-комунікаційних технологій, а й виокремити основні складові їхньої структури, що безпосередньо забезпечують виконання завдань органів

правопорядку. Зміст ІКТ у цій сфері розкривається через сукупність практичних інструментів, систем і програмних рішень, які застосовуються у процесі реалізації правоохоронних функцій.

1.3 Принципи використання інформаційно-комунікаційних технологій правоохоронними органами

У загальній теорії права принципи розглядаються як першоджерела, основоположні ціннісні орієнтири, вихідні положення, що характеризують зміст права, його сутність і призначення в регулюванні суспільних відносин. Як зазначав М. Козюбра: «Принципи права утворюють своєрідний фундамент, на якому тримається право, і у цій якості виступають в ролі джерел права. Вони пронизують собою правову матерію, всі процеси, що протікають у правовій сфері та так чи інакше пов'язані з правом. Принципи виражають сутність права, визначають його зміст і загальний характер правового регулювання суспільних відносин. Поняття «принципи права» є однією з базових юридичних категорій. Вони згадуються майже у кожному монографічному правовому дослідженні, у численних навчальних посібниках і підручниках із будь-яких галузей правового знання» [50, с. 142]. Принципи права виступають системоутворюючим правовим елементом. Ними вноситься єдність до всієї системи правових положень; надання внутрішньої узгодженості юридичному регулюванню відносин в суспільстві постає конструкцією, довкола котрої здійснюється формування його норм, інститутів, галузей і всієї правової системи загалом [51, с. 124]. Сучасними дослідниками справедливо зазначено, що питанню стосовно принципів права в науці присвячено велику кількість якісної літератури, однак це досі не допомогло його загальноприйнятному вирішенню. Це можна пояснити тим, що «будь-які принципи, у тому числі і принципи права, є продуктом людської діяльності, результатом якої вони виступають й інтереси якої вони задовольняють. Принципи є соціальними явищами, як за джерелом виникнення, так і за змістом: їх виникнення зумовлюється потребами суспільного розвитку і в них

відображаються закономірності суспільного життя» [52, с. 42]. Аналіз наукових підходів до досліджуваної проблематики показує, що в юридичній науці сформувалися три основні напрями розуміння принципів права – широкий, вузький (нормативний) та доктринальний. У широкому підході право трактується як комплексне соціальне явище, що охоплює не лише норми, а й інші елементи правової системи: правосвідомість, правовідносини, суб'єктивні права, акти застосування норм, правопорядок тощо. Відповідно, і принципи права розглядаються у розширеному значенні [53, с. 11]. Наприклад, український вчений А. М. Колодій у рамках власної монографії визначає поняття «принцип права» через категорію відправних ідей існування права, що реалізують вираження найважливіших закономірностей та підвалин цього різновиду держави та права, постає однопорядковим із сутністю права та становить його основні характерні ознаки, відрізняється універсальністю, імперативністю вищого класу та суспільною значимістю, відповідає об'єктивній потребі побудування та зміцнення відповідного ладу в суспільстві [52, с. 27]. В свою чергу С. Шатрава, Д. Денищук та О. Погорілець під принципами розуміють основоположні засади діяльності, які виступають критеріями правильності прийняття і оцінки управлінських (адміністративних) рішень [54, с. 379].

Інші вітчизняні вчені, наприклад О. Ф. Скакун [13, с. 221] та П. М. Рабінович [4, с. 91], принципи права визначають через поняття керівних ідей, об'єктивно властивих праву відправних початків, незаперечних вимог (позитивних зобов'язань), що ставлять до суб'єктів відносин у суспільстві заради ефективного об'єднання інтересів індивідуального, групового та громадського характеру й реалізують визначення змісту та спрямованості юридичного регулювання, відображають найістотніші закономірності формації соціально-економічного типу.

Прибічники доктринального розуміння принципів права вважають, що принципи права мають виключно доктринальний характер і їм не властива імперативність. Так, О. О. Уварова визначає принципи права як систему вимог до належної і можливої поведінки людей, які відображають визнані у суспільстві

цінності і утворюють спрямовану на регулювання суспільних відносин ієрархічну єдність [55, с. 55].

Натомість вузький (нормативний) підхід зводить право до закону або інших визнаних джерел, у межах яких принципи можуть існувати лише як складова частина нормативних положень. Наприклад, О. М. Макеєва вважає, що: «Принципи – це вихідні положення, які закріплюють об'єктивні закономірності суспільного життя. Їх провідна роль забезпечується прямим чи непрямим їхнім закріпленням у нормах права» [56, с. 48].

Попри розбіжності у наукових підходах до розуміння сутності принципів права, юридична наука в різні історичні періоди виявляла єдність у визнанні певних положень і засад як основоположних принципів правової системи. Іншими словами, принципи права становлять ті фундаментальні правові явища, які безпосередньо поєднують зміст права із закономірностями суспільного розвитку, що зумовлюють його природу та функціонування. Саме цей зв'язок визначає характер правотворчості, впливає на формування змісту правових норм, а також визначає способи, засоби й механізми реалізації права в конкретних соціально-історичних умовах.

Звертаючись до осмислення змісту принципів впровадження і застосування інформаційно-комунікаційних технологій у діяльності правоохоронних органів, насамперед необхідно врахувати комплекс специфічних чинників, які зумовили їх формування [57, с. 222]. Ці принципи не виникли ізольовано – вони є результатом взаємодії загальнотеоретичних положень правової науки, сучасних тенденцій цифровізації публічного управління та практичних потреб правоохоронної системи. З огляду на зазначене, можна запропонувати наступне визначення змісту терміна «*принципи використання інформаційно-комунікаційних технологій у діяльності правоохоронних органів*» –це система керівних ідей, нормативно й доктринально обґрунтованих вимог, що визначають зміст, спрямованість та межі правового регулювання процесів упровадження, застосування і контролю за використанням ІКТ у діяльності правоохоронних

органів. Таким чином, принципи ІКТ у правоохоронній сфері мають комплексний характер, поєднуючи в собі елементи різних правових систем і доктрин.

У цьому контексті важливо підкреслити, що принципи ІКТ виступають сполучною ланкою між правом і технологіями, забезпечуючи баланс між ефективністю правоохоронних механізмів і дотриманням прав та свобод особи. Крім того, вони ґрунтуються на конституційних положеннях, що гарантують інформаційні права та свободи, визначають межі допустимого державного втручання у сферу приватного життя й комунікацій. Такі принципи забезпечують реалізацію права на доступ до інформації, її захист від неправомірного використання, а також створюють правові умови для безпечного застосування ІКТ у процесах запобігання, розслідування та розкриття правопорушень.

Водночас на їх зміст впливають правові властивості інформації як особливого об’єкта правових відносин – її нематеріальність, динамічність, багатоаспектність і технологічна залежність. Саме ці характеристики зумовлюють необхідність гнучкого, системного підходу до формування принципів, які мають поєднувати правові, етичні та технічні аспекти, забезпечуючи належний баланс між публічними інтересами держави і приватними правами громадян.

Принципи права забезпечують однорідність і внутрішню узгодженість системи юридичних норм, надають правовому регулюванню цілісного характеру, виступаючи своєрідним «цементуючим» елементом усієї правової конструкції. Саме тому дослідження логічної структури та системи принципів права є необхідною передумовою для подальшого аналізу специфіки окремого їх різновиду – принципів застосування інформаційно-комунікаційних технологій у діяльності правоохоронних органів, що формують важливий сегмент сучасної юридичної надбудови.

Слід зазначити, що класифікація принципів права має як теоретичне, так і практичне значення. Вона сприяє глибшому розумінню їхньої юридичної природи, дозволяє виявити вертикальні та горизонтальні зв’язки між різними групами чи видами принципів у межах єдиної системи, визначити місце кожного

з них у структурно-ієрархічній побудові права, а також розробити науково обґрунтовані рекомендації щодо підвищення їхньої регулятивної ефективності.

Як і у багатьох інших питаннях, що стосуються принципів права, в підходах до їхньої класифікації відсутня єдність поглядів. Найбільш поширеним є їх поділ за сферою дії на загальні, міжгалузеві, галузеві принципи та принципи інститутів права. У більш широкому контексті залежно від рівня суспільних відносин, що регулюються правом, розглядає принципи права О. Ф. Скакун. Вона виокремлює такі види: загальнолюдські (міжнародні, загальноцивілізаційні), регіонально-континентальні та національні (внутрішньодержавні). Останні, зі свого боку, поділяються на загальноправові (загальні, основні), міжгалузеві, галузеві, підгалузеві, інституційні [13]. Своєю чергою М. Козюба пропонує визначати класифікацію принципів права за сферою їхньої дії: а) універсальні (загальнолюдські) принципи права, тобто основоположні, базові правові засади, сформульовані в процесі багатовікової історії прогресивного розвитку права, притаманні всім правовим системам; б) цивілізаційні принципи права, характерні для певних правових культур і традицій, що уособлюють відповідні їм цивілізації; в) правосімейні принципи права, тобто принципи, притаманні окремим правовим сім'ям (навіть у межах однієї цивілізації); г) національні принципи права, тобто принципи, що сформульовані і діють у межах певної національної правової системи, відображаючи її особливості [50, с. 152].

Олена Уварова пропонує покласти в основу побудови системи принципів права їх функціональне призначення, що дозволить здійснити умовний поділ принципів права на дві ієрархічні підсистеми, які перебувають у тісному взаємозв'язку. Першу підсистему становлять принципи, зміст яких складають вимоги до процесу праворегулювання. Другу – вимоги, які застосовуються безпосередньо до відносин, які потребують врегулювання, відображають їх змістовні зв'язки [55, с. 58].

Анатолій Колодій вважає, що слід виділяти: 1) принципи правосвідомості; 2) принципи правоутворення; 3) принципи правотворчості, а серед них законотворчості і нормотворчості; 4) принципи системи права:

а) загальноправові (основні); б) міжгалузеві; в) галузеві; г) принципи інститутів права; 5) принципи структури права: а) загальносоціального і юридичного; б) публічного і приватного; в) регулятивного й охоронного; г) матеріального і процесуального; д) об'єктивного і суб'єктивного; 6) принципи правореалізації, а серед них принципи правозастосування; 7) правоохоронні принципи, а серед них, особливо, принципи правосуддя й юридичної відповідальності. Принципи системи і структури права, що змінюються у принципи правоутворення, правореалізації і правоохоронні, можна назвати принципами правового регулювання, визнаючи при цьому особливу роль загальноправових (основних) принципів [52, с. 44].

З огляду на специфіку сфер застосування законів і відмінності в їхній юридичній силі, Д. Денищук пропонує здійснювати класифікацію правових «принципів», поділяючи їх на такі групи: 1) «конституційні принципи» (діють у всіх галузях права та мають найвищу юридичну силу); 2) «спеціальні принципи» (діють в межах, визначених спеціальним законом де мають вищу юридичну силу); 3) «особливі принципи» (мають обмежену сферу застосування, в якій користуються юридичною силою спеціального закону, в якому вони закріплені); 4) «загальні принципи» (в сфері визначеній законом упорядковують всю діяльність, поступаючись в пріоритеті правовим нормам спеціального закону) [54, с. 380].

Вважаємо, що використання ІКТ у діяльності правоохоронних органів спирається на поєднання *базових (загальноправових)* принципів, *галузевих* принципів, притаманних інформаційному й адміністративному праву та *інституційних* принципів здійснення правоохоронної діяльності. Останні мають подвійну природу – з одного боку, вони відображають вплив загальних принципів права, які визначають фундаментальні засади функціонування правової системи в цілому; з іншого – формуються з урахуванням специфіки цілей, завдань і функцій правоохоронної діяльності, де цифрові технології стають не лише інструментом, а й правовим середовищем.

Загальні принципи права притаманні праву загалом і діють у межах усіх галузей й інститутів права. Вони визначають якісні особливості всіх правових норм національної правової системи незалежно від специфіки регульованих ними суспільних відносин [58, с. 6]. У теорії права до загальноправових принципів прийнято відносити: принципи верховенства права і законності; принцип правової визначеності; принцип рівності і недискримінації; дотримання прав і свобод людини тощо.

Розглянемо зміст і особливості реалізації зазначених принципів в контексті здійснення правоохоронної діяльності із використанням засобів ІКТ.

Принцип верховенства права.. Принцип верховенства права, як стверджують науковці, – свого роду мегапринцип, оскільки змістовно включає в себе, виражає низку інших принципів права, зокрема, основоположних та процедур. Його закріплено в ст. 8 Конституції України, але змістовні характеристики його в цій статті не розкрито. Проте відображенням змісту цього принципу є низка інших принципів та положень, закріплених в чинній Конституції України. Мова йде про визнання людини, її життя, здоров'я, честь, гідність, безпеку, недоторканність, що є найвищою соціальною цінністю в Україні (ч.1 ст. 3). Верховенство права як мегапринцип включає в себе змістовно такі принципи та положення, як: авторитетність суду, незалежність його, принцип його доступності, принцип правової визначеності, що передбачає правову якість закону, принцип пропорційності, відповідно до якого в нормотворчості та правозастосовній діяльності необхідно дотримуватися балансу приватного інтересу та суспільного, принцип передбачуваності, принцип субсидіарності тощо. Отже, «верховенство права можна трактувати як панування права українського народу, втіленого та вираженого чинною Конституцією України як волеустановленим актом нашого народу. Очевидно, важливою в плані верховенства права є ідея первинності і визначальності людини і народу та їх права стосовно державної влади з її писаним, державним правом» [59, с. 14]. Верховенство права – концепт, що відображає найбільш важливі аспекти демократичного способу життя. Конституційний Суд України у Рішенні від 02.11.2004 трактує верховенство

права як панування права в суспільстві [60]. Верховенство права як мегапринцип не виключає принципу законності. Водночас верховенство права не є аналогією верховенства закону, а принцип верховенства права – ширший і глибший за принцип законності. В юридичній літературі пропонується визначати *принцип законності*, як один зі складових елементів принципу верховенства права, і розглядати його як систему вихідних засад, реалізація яких спрямована на досягнення кінцевої мети та завдань при здійсненні правотворчості та правозастосування, з суворим дотриманням конституційних норм та законів України [61, с. 112].

Надаючи оцінку законності в діях суб'єктів владних повноважень та їх посадових осіб, дотримання останніми відповідного принципу, Верховний Суд України вказує на необхідність врахування чинності редакції законодавчого акту, на норми якого спиралися посадовці на момент вчинення дії (постанова від 26 жовтня 2023 року, справа № 380/4680/21, Верховний Суд України) [62]. Також Верховний Суд України наголошує, що принцип законності вимагає, щоб органи державної влади мали дозвіл на вчинення певних дій та в подальшому діяли в межах повноважень та у спосіб, що визначено Конституцією України та законами України.

Як і будь-яка інша діяльність, яку правоохоронні органи здійснюють у рамках своєї місії із запобігання, виявлення та розслідування злочинів, їхня взаємодія із системами ІКТ має бути законною. Це означає, що під час проєктування, розробки та використання інформаційних технологій і систем штучного інтелекту необхідно додержуватися законів і правил. Тому законність, як принцип діяльності правоохоронних органів вказує на необхідність дотримання правового режиму добування, перевірки та використання інформації. Усе використання ІКТ має відповідати чинним законам, стандартам та регламентам. Повага до прав людини також є важливою частиною законності. Правоохоронні органи несуть загальний обов'язок захищати людську гідність і безпеку. Таким чином, впровадження ІКТ у правоохоронних органах має мінімізувати будь-яку шкоду або негативний вплив, які ця технологія може спричинити правам будь-

якої людини незалежно від її статусу: жертва злочину, підозрюваний, злочинець, працівник правоохоронних органів, представник населення загалом. Сюди входять права, визнані та встановлені в міжнародному праві, яке містить базові та адаптовані стандарти захисту прав людини, а також права, зазначені в національному законодавстві. Тому у контексті законності правові норми можуть уповноважувати, зобов'язувати або забороняти правоохоронцям здійснювати ті чи інші гласні або негласні заходи, використовувати оперативно-технічні засоби чи ІКТ, а також вимагають дотримання правового порядку їх застосування, встановлюють судовий та відомчий контроль, прокурорський нагляд за їх здійсненням.

Принцип правової визначеності. Під «правовою визначеністю», як правило, в юридичній літературі розуміють принцип правової системи за яким людині гарантується можливість планувати та вчиняти дії з упевненістю, що їй відомо (або може бути відомо) про правові наслідки таких дій. У контексті цифрової автоматизації та профілювання в правоохоронній діяльності принцип правової визначеності є поняттям, зміст якого активно обговорюється.

У висновках Європейської комісії за демократію через право (Венеціанська комісія) неодноразово визначалися ключові елементи принципу правової визначеності. Так, при аналізі одного з законів Угорщини, Комісія зазначає: «Будь-яке обмеження свободи вираження має бути «передбачено законом». З цього висловлювання випливають дві вимоги: 1) Закон повинен бути достатньо доступним: громадянин повинен мати можливість отримати достатню вказівку на правові норми, що застосовуються в даних обставинах; 2) Закон повинен бути передбачуваним: норма не може вважатися «законом», якщо вона не сформульована з достатньою точністю, щоб дозволити громадянинові регулювати свою поведінку: він/вона повинен мати можливість «при необхідності з відповідною консультацією передбачати, розумною мірою даних обставин, наслідки, які можуть спричинити дану дію». Як наголошує Комітет ООН з прав людини, «закони повинні надавати достатні керівництва тим, хто відповідає за їх виконання, щоб вони могли визначити, які форми висловлювання

можуть бути належним чином обмежені, а які – ні» і вони повинні відповідати недискримінаційним положенням Пакту про недискримінацію [63].

Доктрина українського права в цілому солідарна у питанні про те, що правова визначеність стає все більш значущим чинником поточного правотворчого і правозастосовного процесу у державі та суспільстві. Однак, у юридичній літературі не досягнуто єдиного розуміння щодо видової належності та сутності цієї засади. Так, У. Б. Андрусів та С. Є. Федик пропонують розглядати принцип юридичної визначеності в широкому розумінні, як сукупність вимог до організації та функціонування правової системи з метою забезпечення стабільного правового становища особи та її захисту від можливих проявів свавілля, шляхом вдосконалення процесів правотворчості та правозастосування [64, с. 19].

З визначеністю тісно пов'язана вимога стабільності законів. Сталість можна розглядати як таку, що має два ключові аспекти. По-перше, це тривалість часу, протягом якого набір правових норм залишається працездатним з точки зору досягнення цілей політики в середовищі, в якому вони діють. По-друге, можливість примусового виконання правил щодо забороненої поведінки (особливо в кіберпросторі, де діють численні та суперечливі юрисдикції). Нездатність забезпечити виконання вимог закону підриває цінність будь-якого набору правових норм. Таким чином, принцип правової визначеності надає можливість правоохоронним органам визначитися з правовими процедурами і варіантами допустимої поведінки при виконанні своїх службових обов'язків.

Принцип забезпечення прав людини правоохоронними органами передбачає, що держава гарантує забезпечення прав і свобод людини відповідно до принципів та стандартів, встановлених у внутрішніх та міжнародних нормативних актах. Так, П. М. Рабінович визначає, що забезпечення прав людини включає три елементи (напрями) діяльності держави для створення умов для здійснення прав і свобод людини: «1) сприяння реалізації прав і свобод (шляхом позитивного впливу на формування їх загальних соціальних гарантій); 2) захист прав і свобод (здійснення заходів, зокрема правових, щоб запобігти порушенням

прав і свобод); 3) захист прав і свобод людини (відновлення порушень правового стану, притягнення порушників до юридичної відповідальності)» [4, с. 87].

Така позиція випливає із змісту положень Конституції України, згідно з якими: особа, її життя та здоров'я, гідність і честь, недоторканність і безпека визнаються найвищою соціальною цінністю в Україні. Права і свободи людини та їх гарантії визначають зміст і напрям діяльності держави. Держава несе відповідальність перед народом за свою діяльність. Утвердження та забезпечення прав і свобод людини є головним обов'язком держави (стаття 3); Органи державної влади та органи місцевого самоврядування, їх посадові особи зобов'язані діяти лише на підставі, в межах повноважень і спосіб, встановлений Конституцією та законами України (стаття 19); Усі люди є вільними і рівними у своїй гідності та правах. Права і свободи людини невід'ємні і недоторканні (стаття 21); Ніхто не може бути підданий катуванню, жорстокому, нелюдському чи принижувальному поводженню чи покаранню (стаття 28); Ніхто не може бути заарештований або утриманий під вартою, крім як за обґрунтованого судового рішення та тільки з підстав і в порядку, встановлених законом (стаття 29); Усім гарантується право на оскарження в суді рішень, дій або бездіяльності органів державної влади, органів місцевого самоврядування, посадових осіб та працівників цих органів [47].

Принцип забезпечення прав людини правоохоронними органами випливає також із Конвенції про захист прав людини і основоположних свобод (з протоколами) (Європейська конвенція з прав людини) від 4 листопада 1950 року, яка має на меті забезпечити загальне та ефективне визнання і дотримання положень проголошених у ній прав правоохоронними органами, а саме: обов'язок поважати права людини; право на життя; заборона катувань; право на свободу та особисту недоторканність; право на справедливий судовий розгляд; жодного покарання без закону; право на ефективний засіб правового захисту [65].

Принцип рівності і недискримінації. Принципи рівності та недискримінації є складовими засад верховенства права, закріпленого у статті 8 Конституції України. Повага до рівності та відсутність дискримінації, у тому числі при

використанні алгоритмів штучного інтелекту в діяльності правоохоронних органів, означає забезпечення рівного ставлення та можливостей для всіх зацікавлених сторін і утримання від будь-якої невиправданої дискримінації окремих осіб або соціальних груп.

Рівність і недискримінація набувають особливої ваги у контексті відповідальних інновацій у правоохоронній сфері. По-перше, справедливе ставлення до людей є ключовим елементом принципової поліцейської діяльності та безпосередньо пов'язане з правами людини на рівність і недискримінацію, які правоохоронні органи зобов'язані поважати відповідно до статті 24 Конституції України, що гарантує рівність громадян перед законом та забороняє будь-які привілеї чи обмеження за ознаками раси, статі, етнічного чи соціального походження, майнового стану, місця проживання, мови або іншими ознаками.

Цей принцип також конкретизовано в Законі України «Про засади запобігання та протидії дискримінації в Україні» від 06.09.2012, який визначає правові механізми запобігання дискримінації у всіх сферах суспільних відносин [66].

Наприклад, правоохоронний орган, який запроваджує чат-бот на основі штучного інтелекту для взаємодії з громадськістю, має забезпечити альтернативні канали комунікації для осіб, які мають обмежений доступ до цифрових технологій. Це узгоджується із положеннями Закону України «Про Національну поліцію» [67] (ст. 11), який покладає на поліцію обов'язок поважати права і свободи людини та громадянина, не допускати дискримінаційних дій чи рішень.

По-друге, дискримінація в правоохоронному контексті становить значну загрозу для окремих осіб і суспільства загалом. Вона може призвести до неправомірного переслідування чи необґрунтованого покарання окремих осіб, залишаючи без уваги реальних правопорушників. Крім того, використання окремих інформаційно-комунікаційних технологій, зокрема технологій розпізнавання облич, може підсилювати ризик упередженості. Такі системи потребують оцінки впливу на права людини відповідно до принципів Конвенції про захист прав людини і основоположних свобод [65] (ст. 14) та

Протоколу№ 12 до неї, а також у світлі Загальної декларації прав людини [68] (ст. 7) та Міжнародного пакту про громадянські і політичні права [69] (ст. 26), які закріплюють право на рівний захист від дискримінації у будь-якій формі.

Отже, дотримання принципу рівності і недискримінації в умовах цифровізації діяльності правоохоронних органів має бути невід'ємним елементом правомірного, етичного та соціально відповідального використання ІКТ, спрямованого на зміцнення довіри громадян до державних інституцій.

Для того, щоб окреслити галузеві та інституційні принципи використання ІКТ в діяльності правоохоронних органів, необхідно також звернути увагу на чинне вітчизняне законодавство, яке регулює роботу правоохоронних органів. Аналіз окремих норм чинного національного законодавства України, що визначає засади організації та функціонування правоохоронних органів, свідчить, по-перше, про відсутність системного уніфікованого підходу до визначення принципів їх існування; по-друге, про спробу врахування особливостей формування та професійної діяльності кожного окремо взятого органу, підтвердженням чого є як різна кількість таких принципів, так і обсяг змісту у відповідних нормативно-правових приписах.

Так, у розділі ІІ Закону України «Про Національну поліцію» закріплені такі основні принципи: 1) верховенства права; 2) дотримання прав і свобод людини; 3) законності; 4) відкритості та прозорості; 5) політичної нейтральності; 6) взаємодії з населенням на засадах партнерства; 7) безперервності [67].

Відповідно до Закону України «Про Службу безпеки України» організація і діяльність СБУ базується на принципах законності, поваги до прав і гідності особи, позапартійності і відповідальності перед народом України [70]. А в ст. 4 Закону України «Про оперативно-розшукову діяльність» [71] (далі Закон про ОРД) вказано, що оперативно-розшукова діяльність ґрунтується на принципах верховенства права, законності, дотримання прав і свобод людини.

В свою чергу принципи діяльності Прокуратури в Україні мають більш широкий перелік. Так ст. 3 Закону України «Про прокуратуру» встановлює, що: «Діяльність прокуратури ґрунтується на засадах:

1) верховенства права та визнання людини, її життя і здоров'я, честі і гідності, недоторканності і безпеки найвищою соціальною цінністю;

2) законності, справедливості, неупередженості та об'єктивності;

3) територіальності;

4) презумпції невинуватості;

5) незалежності прокурорів, що передбачає існування гарантій від незаконного політичного, матеріального чи іншого впливу на прокурора щодо прийняття ним рішень при виконанні службових обов'язків;

6) політичної нейтральності прокуратури;

7) недопустимості незаконного втручання прокуратури в діяльність органів законодавчої, виконавчої і судової влади;

8) поваги до незалежності суддів, що передбачає заборону публічного висловлювання сумнівів щодо правосудності судових рішень поза межами процедури їх оскарження у порядку, передбаченому процесуальним законом;

9) прозорості діяльності прокуратури, що забезпечується відкритим і конкурсним зайняттям посади прокурора, вільним доступом до інформації довідкового характеру, наданням на запити інформації, якщо законом не встановлено обмежень щодо її надання;

10) неухильного дотримання вимог професійної етики та поведінки» [72].

Аналіз вищенаведених нормативних актів показує, що нормативно закріплені принципи визначають основні орієнтири організації роботи та взаємодії правоохоронців із громадянами, забезпечують законність, дотримання прав і свобод людини та ефективність функціонування правоохоронних органів. Водночас формулювання принципів у законодавчих актах носить базовий характер і не завжди деталізує їх взаємозв'язки чи ієрархію. Тому для більш глибокого розуміння сутності принципів впровадження і використання ІКТ у діяльності правоохоронних органів нами були проаналізовані наукові джерела, де принципи класифікуються, систематизуються та розкривають своє значення в теоретичному контексті. Це дозволило дослідити їх специфіку, виділити характерні ознаки і особливості реалізації, що забезпечило комплексний підхід

до визначення системи принципів використання інформаційно-комунікаційних технологій правоохоронними органами.

Так, вітчизняна науковиця Д. С. Тихонова зазначає, що «принципи правоохоронної системи існують у вигляді вихідних засад правових теорій і концепцій, що виступають правовими орієнтирами суб'єктів правоохоронної діяльності. Принципи на яких ґрунтується правоохоронна діяльність, складають цілісну систему, до якої, враховуючи вище викладене, потрібно віднести такі принципи: 1) спеціальні – узагальнюють засади формування та існування власне правоохоронної системи як специфічного соціального явища; 2) загальноспеціальні – відображають систему цінностей, що притаманні певному суспільству, і мають чи повинні мати правову форму вираження і забезпечення» [73, с. 225].

Своєю чергою, Ю. Холодник виділяє такі спеціальні принципи правоохоронної діяльності, як: принцип забезпечення довіри; принцип забезпечення прав людини; принцип забезпечення доступу до інформаційних технологій; принцип забезпечення конфіденційності інформації [74, с. 100].

Аналізуючи діяльність Національної поліції, В. В. Сокуренко [75, с. 118], наводить такий перелік галузевих (спеціальних) принципів: відкритість і прозорість, політична нейтральність, взаємодія з населенням на засадах партнерства, безперервність. На думку І. А. Григоренко, усі принципи правоохоронної діяльності можна поділити на такі групи: 1) загальносоціальні, що відображають систему цінностей, притаманних певному типу суспільства, мають правову форму закріплення та гарантії забезпечення (гуманізм, демократизм, соціальна справедливість); 2) спеціальні, які втілюють засади формування та існування власне правоохоронної системи як специфічного соціального явища (верховенство права; законність; добропорядність громадян; рівність усіх перед законом; гласність; взаємодія з органами державної влади, органами місцевого самоврядування, об’єднаннями громадян, населенням; професіоналізм і компетентність; незалежність суб’єктів правоохоронної діяльності) [76, с. 25].

З огляду на вищенаведене, вважаємо доцільним запропонувати поділ галузевих принципів застосування ІКТ у діяльності правоохоронних органів залежно від рівня та сфери їх дії (ступеня універсальності та спеціалізації) на:

1. *Універсальні принципи*, які є фундаментом для регулювання відносин щодо застосування ІКТ у всіх, без винятку, формах діяльності правоохоронних структур і мають загальний, всеохоплюючий універсальний характер. Це принцип прозорості, принцип відповідальності, принципи підзвітності, необхідності і пропорційності, надійності тощо.

2. *Спеціальні* – характеризують закономірності роботи з окремими елементами ІКТ або дії окремих суб'єктів при застосуванні ІКТ. Це принципи: конфіденційності, оспорюваності і відшкодування, верховенство інтересів людини, (людського контролю).

Розглянемо докладніше суть та форми реалізації вказаних принципів у національному законодавстві.

Прозорість і відкритість у діяльності правоохоронних органів є необхідними умовами для боротьби з корупцією, забезпечення довіри громадськості та підвищення якості самої правоохоронної діяльності. Поряд з цим важливо знайти оптимальний баланс між вимогами прозорості та необхідністю збереження конфіденційності для забезпечення ефективного функціонування правоохоронних органів у сучасному правовому середовищі [77, с. 99]. Принцип прозорості використання ІКТ правоохоронними органами означає відкритість, зрозумілість і передбачуваність процесів, пов'язаних із застосуванням цифрових технологій у правоохоронній діяльності. Його сутність полягає в тому, що впровадження, функціонування та результати використання ІКТ повинні бути зрозумілими як для суспільства в цілому, так і для осіб, щодо яких здійснюються правоохоронні заходи. Тобто як громадськість, так і кожна окрема особа повинні бути належним чином поінформовані про використання правоохоронними органами тих чи інших технологічних засобів (зокрема систем відеоспостереження, аудіо- чи відеофіксації) під час збирання, обробки та використання інформації про людину. Ця теза знаходить своє відображення,

наприклад, в Законі України «Про захист персональних даних» [78], де в статті 8 зазначається, що: «суб'єкт персональних даних має право: …знати механізм автоматичної обробки персональних даних; …на захист від автоматизованого рішення, яке має для нього правові наслідки». Законодавство має чітко визначати умови, порядок та межі застосування таких технологій у правоохоронній сфері. Водночас відомості про впровадження та функціонування інформаційних систем і реєстрів, їхнє призначення, мету та завдання повинні бути загальнодоступними. Якщо ж оперативні або безпекові потреби об’єктивно обмежують можливість розкриття окремих механізмів чи алгоритмів їх роботи, законність і обґрунтованість використання відповідних технологій повинна підлягати перевірці незалежними контролюючими чи експертними інституціями.

Принципи підзвітності та відповідальності є взаємопов’язаними та взаємодоповнюючими, адже саме через їх реалізацію забезпечується належне, законне та етичне використання інформаційно-комунікаційних технологій у правоохоронній діяльності. Застосування технологій та інформаційних систем правоохоронними органами має здійснюватися в межах чітко визначеної відповідальності кожного суб’єкта, залученого до цього процесу. Кожен структурний підрозділ повинен мати призначену особу, відповідальну за функціонування відповідних інформаційних систем, їхні результати та наслідки використання. Всі посадові особи та кінцеві користувачі ІКТ зобов’язані пройти належну підготовку й навчання, що гарантує їхню компетентність і усвідомлення потенційних ризиків, пов’язаних із технологічними рішеннями. Реалізація цього принципу здійснюється, наприклад, у тексті Положення «Про інформаційно-комунікаційну систему «Інформаційний портал Національної поліції України» (ІПНП), затвердженого Наказом Міністерства внутрішніх справ України від 03.08.2017 № 676 [79]. Документ визначає перелік суб'єктів данної системи, їх повноваження та порядок доступу і роботи в системі.

Використання ІКТ у поліції та інших правоохоронних органах має підлягати належному управлінню, моніторингу та контролю на відповідному організаційному рівні. Так, стаття 27 Закону України «Про Національну поліцію»

визначає вимоги до використання поліцією інформаційних ресурсів: «Інформація про доступ до бази (банку) даних повинна фіксуватися та зберігатися в автоматизованій системі обробки даних, включно з інформацією про поліцейського, який отримав доступ, та про обсяг даних, доступ до яких було отримано. Кожна дія поліцейського щодо отримання інформації з інформаційних ресурсів, передбачених статтями 26, 27 цього Закону, фіксується у спеціальному електронному архіві, ведення якого покладається на службу інформаційних технологій Міністерства внутрішніх справ України. В електронному архіві фіксуються прізвище, ім'я, по батькові та номер спеціального жетона поліцейського, вид отриманої інформації, реєстр, з якого отримувалася інформація, час отримання інформації та інші дані, необхідні для ідентифікації поліцейського, який отримував інформацію з реєстрів». А стаття 28 цього Закону визначає, що «Поліцейські та особи, які відповідно до цього Закону мають доступ до інформаційних ресурсів єдиної інформаційної системи Міністерства внутрішніх справ України та інших інформаційно-комунікаційних систем (інформаційних ресурсів), несуть персональну дисциплінарну, адміністративну та кримінальну відповідальність за вчинені ними діяння, що призвели до порушень прав і свобод людини, пов'язаних з обробкою інформації».

З огляду на наведене, доцільним видається внесення аналогічних доповнень до інших законодавчих актів, які визначають правові засади діяльності інших правоохоронних органів. Так, пропонуємо доповнити Закон України «Про Службу безпеки України» статтею 26-1 такого змісту: «Стаття 26-1. Порядок використання інформаційно-комунікаційних технологій у діяльності Служби безпеки України.

Служба безпеки України у своїй діяльності має право використовувати інформаційно-комунікаційні технології з метою забезпечення національної безпеки, захисту державного суверенітету, територіальної цілісності, конституційного ладу України, а також для запобігання, виявлення, припинення та розслідування злочинів, віднесених до її компетенції.

Застосування інформаційно-комунікаційних технологій у діяльності Служби безпеки України не може бути спрямоване на неправомірне втручання в приватне життя особи, обмеження її прав чи свобод, крім випадків, прямо передбачених законом і санкціонованих у встановленому порядку.

Кожне втручання в інформаційний простір, що пов'язане з персональними даними або електронною ідентичністю особи, підлягає обов'язковій фіксації та контролю з боку визначених уповноважених підрозділів Служби безпеки України. Відомості про такі дії зберігаються у захищених журналах обліку в порядку, визначеному відомчими нормативно-правовими актами.

Служба безпеки України впроваджує щорічний аудит кібербезпеки та функціонування інформаційних систем, що використовуються в оперативно-службовій діяльності.

Контроль за дотриманням законності під час використання інформаційно-комунікаційних технологій у діяльності Служби безпеки України здійснюється Верховною Радою України, Уповноваженим Верховної Ради України з прав людини, а також у межах компетенції — іншими державними органами».

В свою чергу Закон України «Про оперативно-розшукову діяльність» містить ст. 9 в якій п.11 зазначає, що: «Підрозділи, що використовують автоматизовані інформаційні системи в оперативно-розшуковій діяльності, повинні забезпечити можливість видавати дані про особу на запит органів досудового розслідування, прокуратури, суду. В місцях зберігання інформації повинна бути гарантована її достовірність та надійність охорони». Пропонуємо доповнити цю частину новим абзацом такого змісту: *«Кожне використання таких систем повинно бути зафіксовано в електронному журналі, що підлягає внутрішньому та зовнішньому контролю. Доступ до цифрових матеріалів здійснюється за індивідуальним цифровим ідентифікатором з обов'язковим протоколюванням усіх дій. Оперативні підрозділи мають право застосовувати програмно-апаратні засоби, бази даних, системи штучного інтелекту, аналітичні платформи тощо – виключно на підставі та в порядку, визначених законом».*

На наш погляд, такі доповнення сприятимуть гармонізації та узгодженості положень відповідних нормативно-правових актів, а також забезпечать більш ефективну реалізацію принципів підзвітності та відповідальності в діяльності зазначених органів. Правоохоронні органи, будучи наділеними широкими владними повноваженнями, перебувають у потенційно асиметричних відносинах влади та контролю з суспільством. Упровадження складних цифрових технологій, зокрема штучного інтелекту, може посилити цей дисбаланс, особливо за умов недостатньої обізнаності громадян щодо мети та механізмів їх використання. Саме тому забезпечення прозорої підзвітності та персональної відповідальності є ключовими умовами легітимності цифрової трансформації правоохоронної діяльності.

Принципи необхідності та пропорційності у використанні ІКТ правоохоронними органами. Застосування інформаційно-комунікаційних технологій у діяльності правоохоронних органів може істотно впливати на реалізацію прав і свобод людини – як громадян, так і працівників самих органів, потерпілих, підозрюваних, засуджених чи інших осіб. Тому впровадження, використання або вдосконалення цифрових систем повинно відбуватися на основі принципів легітимності, необхідності та пропорційності, які становлять універсальні правові орієнтири при будь-якому обмеженні прав людини.

Відповідно до статей 8 і 19 Конституції України, діяльність органів державної влади має ґрунтуватися на принципі верховенства права і здійснюватися виключно на підставі, у межах повноважень та у спосіб, передбачений законом. Принцип необхідності вимагає, щоб втручання у права людини відбувалося лише тоді, коли досягнення законної мети неможливе без застосування відповідних технологічних засобів. Це положення узгоджується зі ст. 11 Закону України «Про Національну поліцію», де передбачено, що поліція застосовує технічні засоби виключно в обсязі, необхідному для виконання своїх повноважень.

Принцип пропорційності передбачає досягнення балансу між втручанням у права людини та суспільною потребою, яка обґрунтовує це втручання.

Правоохоронні органи повинні обирати найменш інвазивний із можливих способів досягнення цілей, передбачених законом, а наслідки такого втручання мають бути співмірними із переслідуваною метою. Цей принцип закріплений у практиці Європейського суду з прав людини (рішення у справах S. and Marper v. the United Kingdom, 2008; Roman Zakharov v. Russia, 2015 [80]) та імплементований у національне законодавство через вимоги щодо обмеження доступу до персональних даних (ст. 7, 10 Закону «Про захист персональних даних»).

Таким чином, необхідність і пропорційність утворюють єдину систему правових критеріїв, які мають оцінюватися до ухвалення рішення про впровадження ІКТ або технологій штучного інтелекту у правоохоронну практику. Наприклад, перед запровадженням системи автоматизованого аналізу електронних пристроїв підозрюваних має бути проведено попередню оцінку впливу на права людини або оцінку впливу на захист даних. Водночас відповідність цим принципам повинна забезпечуватися на всіх етапах життєвого циклу технології – від розробки до її практичного використання, включаючи регулярну переоцінку доцільності застосування. Якщо, наприклад, мета розслідування вже досягнута, подальше використання зібраних даних або повторне сканування пристроїв є недопустимим, оскільки перестає відповідати вимогам необхідності та пропорційності.

Принцип надійності та безпеки використання ІКТ у діяльності правоохоронних органів передбачає, що технологічні системи повинні функціонувати стабільно, забезпечувати узгодженість у різних умовах та бути захищеними від зовнішніх і внутрішніх загроз. Надійність означає здатність системи штучного інтелекту або іншої ІКТ адекватно й послідовно виконувати свої функції незалежно від зміни вхідних даних або контексту застосування. Вона передбачає також відповідність технологій стандартам якості, що гарантують сталість результатів та зниження рівня технічних збоїв.

Безпека ІКТ охоплює запобігання будь-яким ризикам заподіяння шкоди фізичному, психічному чи матеріальному добробуту осіб, а також

навколишньому середовищу. У цьому контексті правоохоронні органи зобов'язані впроваджувати технології, які відповідають вимогам безпеки, передбаченим міжнародними актами – зокрема, Конвенцією Ради Європи про кіберзлочинність (Будапештська конвенція, 2001 р.) [81], Рекомендацією Комітету Міністрів Ради Європи щодо впливу алгоритмічних систем на права людини (CM/Rec (2020)1) [82], а також Керівними принципами Організації економічного співробітництва та розвитку щодо штучного інтелекту (OECD AI Principles, 2019 р.), де прямо зазначено, що надійність і безпечність є обов'язковими умовами етичного використання технологій [83].

Відповідно до Регламенту Європейського парламенту і Ради 2016/679 (GDPR) [84], принцип безпеки оброблення даних вимагає запровадження належних технічних та організаційних заходів для гарантування конфіденційності, цілісності та доступності інформації. У правоохоронному контексті ці положення конкретизуються в Директиві ЄС 2016/680, що регулює обробку персональних даних компетентними органами для запобігання злочинам, розслідування та виконання покарань.

В Україні принципи надійності та безпеки ІКТ знаходять своє відображення у національному законодавстві, зокрема Законі України «Про основні засади забезпечення кібербезпеки України» [85], який визначає забезпечення цілісності, стійкості та безперебійності функціонування інформаційних систем як стратегічне завдання держави. В свою чергу Закон України «Про захист персональних даних» встановлює обов'язок володільців баз даних уживати технічних і організаційних заходів для захисту даних від незаконної обробки, втрати або знищення (ст. 24). В контексті реалізаццііі данного принципу цікавим є текст Концепції розвитку цифрової економіки та суспільства України (Розпорядження КМУ № 67-р від 17.01.2018), яка передбачає створення безпечного цифрового середовища на основі принципів надійності, стійкості та довіри до ІКТ: «Використання цифрових технологій повинно запровадити новий рівень координації діяльності оперативних, чергових, диспетчерських та муніципальних служб, відповідальних за громадську безпеку та повсякденну

життєдіяльність місцевих громад, а також запровадити механізми швидкого реагування відповідних служб з метою усунення наслідків правопорушень та надзвичайних ситуацій»[86]. А також Стратегії розвитку системи Міністерства внутрішніх справ України до 2030 року (Наказ МВС № 547 від 22.06.2023) [87], де визначено пріоритет цифрової трансформації правоохоронної діяльності з дотриманням вимог безпеки інформаційних систем та захисту даних.

Таким чином, надійність і безпека ІКТ є системоутворювальними принципами, які вимагають від правоохоронних органів не лише попередньої технічної перевірки технологій, але й регулярного моніторингу їхньої ефективності протягом усього життєвого циклу системи. Дотримання цих принципів сприяє підвищенню довіри суспільства до використання цифрових інструментів у правоохоронній сфері та узгоджує національну практику з міжнародними стандартами належного управління ІКТ.

Друга група галузевих принципів – *спеціальні принципи* визначають закономірності роботи з конкретними інформаційними технологіями, системами або окремих суб'єктів правоохоронної діяльності. Наприклад, при впровадженні і використанні систем штучного інтелекту діють принципи конфіденційності, оспорюваності і відшкодування, верховенства інтересів людини, (людського контролю) тощо. Так, А. В. Мовчан серед спеціальних принципів інформаційно-аналітичної роботи в оперативно-розшукової діяльності називає: безперервність накопичення інформації, системність, узгодженість, варіантність, верифікованість, ефективність тощо [88, с. 40].

Зміст даної групи принципів випливає з обґрунтованих ознак, якими має характеризуватись будь-яка наукова та практична технологія, а також з обґрунтованих критеріїв, яким ця технологія має відповідати. В усі принципи повинно бути закладено об'єктивне прагнення забезпечити оптимальну чи близьку до оптимальної динаміку розвитку процесу інформаційно-технічного забезпечення правоохоронної діяльності. Реалізація цих принципів дозволяє визначити раціональні межі вимог до персоналу, що діятиме за даною інформаційною технологією на кожному етапі управлінського процесу.

В свою чергу інституційні принципи – це фундаментальні керівні засади діяльності конкретних інститутів або органів влади, які визначають їхню внутрішню організацію, порядок функціонування та спосіб реалізації повноважень. Правовою основою для їх реалізації є відомчі накази, регламенти, внутрішні інструкції, положення про інформаційні системи тощо, а метою – забезпечення ефективності, безпеки та відповідності внутрішньої роботи конкретного правоохоронного органу. До інституційних принципів можна віднести: принцип довіри до правоохоронного органу; принцип оперативності (використання ІКТ для швидкого реагування на правопорушення); принцип спеціалізації (ІКТ застосовуються відповідно до функцій органу (розвідка, розслідування); принцип внутрішнього контролю (державний і громадський аудит, контроль доступу, внутрішні процедури безпеки); принцип інтеграції (забезпечення взаємодії між інформаційними системами різних відомств).

Отже, чітке окреслення принципів використання ІКТ в діяльності правоохоронних органів сприяє визначенню правових рамок їх компетенції, стандарту діяльності посадових осіб, а також засобів забезпечення реалізації законних прав, міжнародних і європейських принципів і стандартів у національній правовій системі як основного чинника подальшого розвитку і систематизації законодавства.

1.4 Правова основа використання інформаційно-комунікаційних технологій у діяльності правоохоронних органів

Дослідження правових основ є необхідним для оцінки ефективності правового регулювання, з’ясування рівня узгодженості національної нормативної бази із міжнародними стандартами Ради Європи, Європейського Союзу та ООН у сфері безпеки, захисту персональних даних і забезпечення прав людини в цифровому середовищі. Такий аналіз дозволяє не лише виявити прогалини чи колізії у законодавстві, а й обґрунтувати напрямки його вдосконалення відповідно до принципів верховенства права, законності,

пропорційності та підзвітності. На сьогодні у наукових дослідженнях, присвячених цій правовій тематиці не має єдиної точки зору на зміст категорії «правова основа». Наприклад С. Г. Серьогіна визначає даний термін як сукупність нормативно-правових актів, що визначають, регулюють або встановлюють правові межі, порядок, правила, права й обов'язки у певній сфері суспільних відносин [89, с. 77]. С. П. Поляк, під «правовою основою» розуміє систему нормативних актів, що визначають функції, компетенцію, форми і методи діяльності органів державної влади і місцевого самоврядування, а також їх структурних підрозділів [90, с. 174]. Своєю чергою В. Копейчиков вважає, що правова основа є формою вираження правового регулювання, що визначає «юридичну конструкцію діяльності суб'єктів та систему норм, які встановлюють механізми реалізації функцій у межах законності» [91].

Необхідно відрізняти термін «правова основа» від терміну «правові засади» (або «засади права») під яким найчастіше розуміють сукупність основоположних правових елементів, які визначають нормативну, ідейну та організаційну основу певної сфери суспільних відносин, виду діяльності або інституту. Вони окреслюють як, на підставі чого і в яких межах здійснюється відповідна діяльність. Це філософсько-ціннісний рівень права – своєрідна «ідеологічна база» або «духовний фундамент» правового регулювання. Своєю чергою термін «правові основи» – це структурно-нормативний рівень – тобто «юридичний каркас», який формують закони, підзаконні акти, міжнародні договори тощо.

Наприклад, у преамбулі Закону України «Про Національну поліцію» говориться, що: «Цей Закон визначає правові засади організації та діяльності Національної поліції України..». Водночас стаття 3 цього Закону має назву «Правова основа діяльності поліції» і містить перелік нормативно-правових актів, якими у своїй діяльності керується поліція. Подібна фраза міститься і в тексті Закону України «Про прокуратуру», де стаття 3 визначає *засади* діяльності прокуратури, і, здебільшого, перераховує її принципи. У Законі України «Про Службу безпеки України» також стаття 3 встановлює, що: «Діяльність Служби безпеки України, її органів і співробітників ґрунтується на *засадах* законності,

поваги до прав і гідності особи, позапартійності та відповідальності перед народом України», а стаття 4 закріплює, що «Правову основу діяльності Служби безпеки України становлять Конституція України, цей Закон та інші акти законодавства України, відповідні міжнародні правові акти, визнані Україною…».

Отже, поняття «правова основа» можна розглядати як законодавчу базу, на яку спирається певна діяльність (правоохоронна, оперативно-розшукова, адміністративна, інформаційно-аналітична тощо), і яка: визначає повноваження суб'єктів цієї діяльності; регламентує процедури і механізми реалізації функцій; установлює обмеження і відповідальність; гарантує правовий захист прав і свобод людини в межах цієї діяльності. У галузі організації й діяльності органів публічної влади під правовою основою розуміють систему нормативних актів, що визначають функції, компетенцію, форми і методи діяльності органів державної влади і місцевого самоврядування, а також їх структурних підрозділів [92, с. 174].

Аналізуючи різні аспекти правоохоронної діяльності, дослідники наголошують на багатокомпонентному характері її правового забезпечення та окреслюють низку ключових підходів до розуміння правових основ окремих її напрямів. Зокрема, в юридичній літературі містяться наступні визначення:

1) А. Є. Голубов – правова основа провадження у справах щодо злочинів неповнолітніх розглядається як цілісне системне утворення, що об'єднує нормативно-правові акти різної юридичної сили, правової природи та змісту, однак об'єднані спільним призначенням – регулюванням правозастосовної діяльності в межах відповідного провадження [93, с. 141];

2) А. В. Лапкін – правова основа діяльності органів прокуратури визначається як сукупність правових норм, які закріплюють засади організації та функціонування прокуратури України, встановлюють правовий статус її працівників, регулюють відносини, що є об'єктом прокурорського нагляду, а також визначають порядок, методи й засоби здійснення прокурорської діяльності [94, с. 18];

3) К. Л. Бугайчук – правову основу діяльності Національної поліції України можна визначити як сукупність правових норм, що закріплюються у національних та міжнародних нормативно-правових актах і регулюють суспільні відносини, які виникають у процесі її діяльності з надання поліцейських послуг в сферах забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки і порядку, надання послуг з допомоги особам, які її потребують, а також у сферах публічного адміністрування та взаємодії з іншими органами державної влади, місцевого самоврядування та громадськістю [95, с. 126];

4) С. П. Поляк – правова основа оперативно-розшукової діяльності щодо протидії втягненню неповнолітніх у злочинну діяльність трактується як сукупність науково обґрунтованих і нормативно закріплених положень, що мають правовий, організаційний та тактичний характер. Ці положення визначають межі легальної діяльності оперативних підрозділів правоохоронних органів і створюють умови для реалізації завдань оперативно-розшукової діяльності та кримінального судочинства [90, с. 92].

Для даного наукового дослідження аналіз правових основ застосування інформаційно-комунікаційних технологій у діяльності правоохоронних органів, має принципове значення для розкриття сутності предмета дослідження. Саме правові основи визначають нормативно-інституційне підґрунтя, в межах якого реалізуються теоретичні положення щодо цифровізації діяльності правоохоронних органів. Вони забезпечують практичний вимір теоретико-правових концепцій, демонструючи, як ідеї, принципи та доктринальні підходи відображаються у чинному законодавстві та правозастосовній практиці.

Правова основа впровадження та застосування новітніх технологій у діяльності органів правопорядку наразі не має універсально сформованої концепції. Ані правова доктрина, ані чинне законодавство поки що не містять визначення терміну «правова основа використання інформаційно-комунікаційних технологій у правоохоронній діяльності». Водночас у наукових дослідженнях зустрічаються спроби визначити близькі за змістом поняття, такі

як: «правова основа цифровізації правоохоронних органів» та «правова основа інформаційно-аналітичного забезпечення органів внутрішніх справ». В узагальненому вигляді названа правова категорія характеризується як сукупність нормативно-правових актів, що опосередковано або безпосередньо регламентують організаційно-управлінські та організаційно-тактичні заходи (функції), що здійснюються у зазначеній сфері оперативно-розшукової діяльності [96], [97]. Таким чином, правова основа є складовим елементом правового забезпечення певної сфери діяльності; вона повинна бути системною, логічно узгодженою і стабільною. Її аналіз виступає важливою передумовою ефективного правозастосування.

Науковці відзначають, що розвиток правової системи сучасної держави дедалі більше зумовлюється впливом процесів цифровізації. Як підкреслює В. М. Василенко: «цифрова трансформація у сфері правопорядку охоплює широке коло змін – від переходу до електронного документообігу і створення інформаційно-аналітичних платформ до запровадження електронного обліку правопорушень, цифрових систем спостереження, автоматизованих реєстрів та комунікацій між органами досудового розслідування… Окремої уваги потребує правова складова цифрової трансформації, адже впровадження нових інструментів має відповідати конституційним принципам, не порушувати прав і свобод громадян, а також бути контрольованим з боку судових та наглядових органів» [98, с. 950]. Цю точку зору поділяють Д. А. Зінченко та О. П. Макарова які вважають, що: «суттєвим викликом є недосконаліть нормативного регулювання цифрових процедур у сфері правозастосування. Законодавство України ще не повною мірою адаптоване до специфіки роботи з цифровими доказами, механізмами електронного документообігу, віддаленим слідством та міжнародним обміном цифровою інформацією» [99]. М. Р. Каліман заявляє, що: «наявна фрагментарність правових актів, відсутність єдиного стандарту цифрової доказової бази, а також неоднозначність тлумачень електронних процедур у судовій практиці створюють простір для правової невизначеності та зловживань. У таких умовах важко забезпечити однаковість застосування закону,

що знижує ефективність правоохоронної системи і ставить під сумнів її авторитет у суспільстві» [100].

Слід відзначити, що швидкий розвиток технологій значно випереджає адаптаційні можливості законодавства. Це призводить до правових прогалин та невідповідностей у нормативній базі, що створює ризики неоднозначного тлумачення прав і обов'язків як з боку суб'єктів владних повноважень, так і громадян. Таким чином, удосконалення правової основи використання ІКТ у правоохоронній діяльності має стати не лише техніко-юридичним інструментом, але й гарантією реалізації принципу верховенства права, правової визначеності та ефективного захисту прав людини у цифровому вимірі.

Як соціальний інститут, право змушене реагувати на динаміку цифрових трансформацій у суспільстві. Сучасне право стає не лише інструментом, який забезпечує впровадження ІКТ у різні сфери державного управління та правоохоронної діяльності, але й самим об'єктом цифровізації – змінюється його форма, зміст, механізми реалізації та тлумачення. Як слушно зазначає І. І. Онищук: «правова цифровізація – це інтегральний метод формалізації права, активного системного оперування нормативно-правовими масивами, що трансформуються або відображаються за допомогою комп'ютерних програмних кодувань. З метою оптимізації правовідносин, а також створення нової цифрової реальності правова цифровізація також вимагає правового регулювання або присутності уповноваженого державою регулятора. Вплив технологічного фактора призводить до трансформації традиційного права. Втім, впровадження правової цифровізації у правотворчий процес сприятиме покращенню системи права в контексті її упорядкування, систематизації, усунення прогалин і суперечностей» [101].

Однак ні правова доктрина, ні юридична практика ще не виробили загальновизнаної концепції напрямів і закономірностей цих трансформацій у правоохоронній сфері. Основною проблемою сучасного етапу є неможливість повного нормативного охоплення всіх нових видів суспільних відносин, що виникають у цифровому середовищі. Надмірна спроба законодавця

«зарегулювати» цифрові процеси може позбавити правове поле гнучкості та стримувати технологічний розвиток. Іншою важливою проблемою є відносність юрисдикційних меж держави в умовах глобалізованих інформаційних потоків. Це створює потребу у посиленні ролі міжнародних правових механізмів, зокрема імплементації принципів, закріплених у таких документах: Регламент (ЄС) 2016/679 (GDPR) та Європейська стратегія з даних (2020) [102], що задають стандарти відповідальної цифрової взаємодії; Окінавська Хартія глобального інформаційного суспільства (визначає розвиток та ефективне функціонування електронної ідентифікації, електронного підпису, криптографії та інших засобів забезпечення безпеки та достовірності операцій) [103]; Резолюція Генеральної Асамблеї «Створення глобальної культури кібербезпеки та оцінка національних зусиль щодо захисту найважливіших інформаційних інфраструктур» [104], тощо. Основні ідеї цих документів виражають прагнення до більш безпечного, стабільного, відкритого глобального інформаційного простору.

В межах національного права слід згадати наступні документи:

Закон України «Про Національну програму інформатизації» від 01.12.2022 [45] включає правоохоронні органи до переліку суб’єктів Програми і визначає серед основних її напрямів розробку, впровадження та застосування інформаційно-комунікаційних технологій у державному управлінні, місцевому самоврядуванні та суспільному житті.

Закон України «Про захист інформації в інформаційно-комунікаційних системах» [105], що визначає об'єктами захисту інформацію, що обробляється в системі, та програмне забезпечення, яке призначено для обробки цієї інформації. Також документ регулює питання доступу до інформації в системі, умови її обробки і захисту, відносини між суб’єктами, повноваження державних органів влади у сфері захисту інформації в системах.

Отже, правове регулювання використання ІКТ у діяльності правоохоронних органів є багаторівневою системою, що поєднує міжнародні та національні норми. Правове регулювання визначає межі правомірного застосування цифрових інструментів у діяльності органів публічної влади та забезпечує баланс

між ефективністю і дотриманням прав людини. Його розвиток має ґрунтуватися на принципах верховенства права, правової визначеності, пропорційності та недискримінації, а також передбачати гнучкість у реагуванні на технологічні зміни. На підставі аналізу наукових праць та національної законодавчої бази, пропонуємо під *правовою основою застосування інформаційно-комунікаційних технологій у діяльності правоохоронних органів* розуміти сукупність конституційних положень, міжнародно-правових стандартів, норм національного законодавства, підзаконних нормативних актів і доктринальних положень, які визначають допустимі межі, порядок, форми та гарантії використання інформаційно-комунікаційних технологій правоохоронними органами з метою реалізації їхніх функцій за умови дотримання прав і свобод людини, забезпечення інформаційної безпеки та законності.

В цьому контексті вважаємо, що необхідною передумовою побудови ефективного правового механізму цифрової трансформації публічної безпеки є систематизація законодавства у сфері застосування інформаційно-комунікаційних технологій правоохоронними органами. У науковій літературі пропонуються різні підходи до класифікації нормативно-правових актів, що регулюють цю сферу. Більшість науковців поділяють їх за юридичною силою (О. Ф. Скакун [13], К. Л. Бугайчук [95, с. 126], Л. Я. Масьюк [106, с. 547]). Своєю чергою В. В. Горбонос пропонує систематизацію нормативно-правових актів за критеріями: юридична сила; суб'єкт нормотворчості; рівень регулювання; галузева належність; сфера дії; напрям регулювання [107, с. 77]. Іншого критерію дотримується В. Р. Біла, яка у своїх дослідженнях пропонує поділ за компетенцією суб'єктів, що видають документи: загальні; відомчі; міжвідомчі; місцеві регуляторні акти.[108, с. 73].

На наш погляд, ієрархічний критерій систематизації законодавства дозволяє виявити співвідношення між нормативними актами різного рівня та встановити пріоритетність норм у випадку колізій. В сфері застосування інформаційно-комунікаційних технологій правоохоронними органами за юридичною силою виокремлюють такі групи нормативно-правових актів:

– акти конституційного рівня – Конституція України (ст. 3, 32, 92, 106);

– закони України, які визначають правові засади інформаційної і правоохоронної діяльності, серед яких: Закон України «Про Національну поліцію», Закон України «Про інформацію», Закон України «Про захист персональних даних», Закон України «Про електронні комунікації» тощо;

– міжнародно-правові акти, які встановлюють стандарти у сфері цифрових прав і захисту даних – Європейська конвенція з прав людини (1950), Конвенція Ради Європи № 108+ (2018), Регламент (ЄС) 2016/679 (GDPR);

– підзаконні нормативні акти, включно з указами Президента України, постановами Кабінету Міністрів України, відомчими нормативними актами (наприклад, Наказ МВС України № 747 від 08.09.2017 «Про затвердження Положення про інформаційно-аналітичну систему Національної поліції України») та міжвідомчими угодами про інформаційну взаємодію між різними правоохоронними структурами. А також Розпорядження Кабінету Міністрів України «Про схвалення Концепції розвитку штучного інтелекту в Україні», в якому наголошується, що: «Застосування технологій штучного інтелекту в забезпеченні інформаційної безпеки є одним із факторів, що сприятиме забезпеченню національних інтересів. Зокрема, моніторинг соціальних мереж та інтернет-ресурсів електронних медіа з використанням технологій штучного інтелекту дає можливість виявляти системні тренди і проблематику, діяти на випередження, аналізувати цільову аудиторію» [109].

Як було зазначено раніше, систематизація нормативних актів, що регулюють використання інформаційно-комунікаційних технологій у діяльності правоохоронних органів, є ключовою передумовою створення ефективного правового механізму забезпечення цифрової трансформації сфери публічної безпеки. Ґрунтовний аналіз чинної нормативно-правової бази дає можливість не лише визначити її структурні особливості, а й розширити підходи до класифікації відповідних актів, виокремивши такі критерії:

1. Залежно від сфери правовідносин, які регулюють відповідні норми (за предметом правового регулювання), можна виділити:

– інформаційно-правові акти, що визначають порядок обробки, зберігання та передачі даних (Закон «Про інформацію», Закон «Про доступ до публічної інформації»);

– організаційно-правові акти, що регламентують діяльність правоохоронних органів у частині застосування ІКТ (Закон «Про Національну поліцію», Закон «Про оперативно-розшукову діяльність»);

– техніко-правові акти, що встановлюють стандарти, вимоги та безпекові протоколи при роботі з інформаційними системами (ДСТУ ISO/IEC 27001:2015 — «Інформаційні технології. Методи захисту інформації. Системи управління безпекою інформації»);

– кримінально-правові норми, що встановлюють відповідальність за кіберзлочини (Розділ XVI Кримінального кодексу України «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів)»).

2. За функціональним призначенням:

– регулятивні, які встановлюють порядок функціонування інформаційних систем у правоохоронних органах (наприклад, Постанова КМУ № 835 від 21.10.2015 «Про затвердження Положення про єдину інформаційну систему МВС»);

– охоронні, що визначають заходи захисту прав громадян під час використання ІКТ (Закон «Про захист персональних даних», Закон «Про електронні довірчі послуги»);

– забезпечувальні, які регулюють питання фінансування, навчання кадрів, впровадження стандартів кібербезпеки (Закон «Про основні засади забезпечення кібербезпеки України»).

3. За ступенем спеціалізації:

– загальне законодавство – регулює відносини у сфері інформації, зв'язку, захисту персональних даних. Наприклад, Закон України «Про основні засади забезпечення кібербезпеки України» визначає, що: «правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина,

суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки» [85]. Серед суб'єктів, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки названі правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності;

– спеціальне законодавство – регламентує діяльність конкретних правоохоронних структур (МВС, СБУ, ДБР, Прокуратури) з використанням ІКТ. Так, на законодавчому рівні найбільш повно сьогодні регламентовані питання інформаційно-аналітичного забезпечення Національної поліції України. Зокрема, ст. 25 Закону України «Про Національну поліцію» визначено повноваження поліції у сфері інформаційно-аналітичного забезпечення. Визначено, що поліція здійснює інформаційно-аналітичну діяльність виключно для реалізації своїх повноважень у таких напрямах: 1) формує бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України; 2) користується базами (банками) даних Міністерства внутрішніх справ України та інших органів державної влади; 3) здійснює інформаційно-пошукову та інформаційно-аналітичну роботу; 4) здійснює інформаційну взаємодію з іншими органами державної влади України, органами правопорядку іноземних держав та міжнародними організаціями; 5) надає до Єдиного державного реєстру призовників, військовозобов'язаних та резервістів. Поліція може створювати власні бази даних, необхідні для забезпечення щоденної діяльності органів (закладів, установ) поліції у сфері трудових, фінансових, управлінських відносин, відносин документообігу, а також міжвідомчі інформаційно-аналітичні системи, необхідні для виконання покладених на неї повноважень.

– відомче законодавство – внутрішні накази, інструкції, положення про інформаційні системи, які діють в системі правоохоронних органів. Зокрема, слід виділити такі відомчі нормативно-правові акти МВС та Національної поліції

України, як. Положення про автоматизовану інформаційну систему оперативного призначення єдиної інформаційної системи МВС, затверджене Наказом Міністерства внутрішніх справ України від 20.10.2017 № 870; Положення про інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України», затверджене Наказом Міністерства внутрішніх справ України від 28 серпня 2017 року № 1059/30927; Наказ Національного агентства з питань запобігання корупції від 21 червня 2024 року № 161/24 «Про затвердження Порядку проведення логічного та арифметичного контролю декларації особи, уповноваженої на виконання функцій держави або місцевого самоврядування».

4. За напрямом впливу (сфера дії норм):

– внутрішньо-організаційні акти, які регламентують порядок збору, аналізу, зберігання та передачі службової інформації (наприклад, накази МВС про ведення баз даних);

– зовнішні акти, які визначають порядок доступу громадян, обміну інформацією між державними органами та міжнародне співробітництво у сфері ІКТ (зокрема, Будапештська конвенція про кіберзлочинність (2001)).

Отже, формування правової основи впровадження та використання інформаційно-комунікаційних технологій у діяльності правоохоронних органів має бути спрямоване на створення комплексних передумов для ефективного, безпечного та правомірного функціонування цифрових інструментів у цій сфері. Реалізація цього завдання вимагає комплексного вдосконалення правового регулювання на кількох рівнях, кожен із яких має власну сферу дії, механізми впливу та правові інструменти, що забезпечують узгоджене функціонування цифрових технологій у межах правової системи, а саме:

1. Конституційний рівень. Застосування ІКТ має здійснюватися з урахуванням конституційних гарантій прав і свобод людини, зокрема права на приватність, недоторканність особистого життя та захист персональних даних (статті 3, 32 Конституції України).

2. Законодавчий рівень. Потребує оновлення система профільних законів, зокрема Законів України «Про оперативно-розшукову діяльність», «Про

Національну поліцію», «Про Службу безпеки України», «Про захист персональних даних» *(Додаток Б*), а також положень Кримінального процесуального кодексу України, в яких необхідно чітко визначити:

– право правоохоронного органу використовувати сучасні інформаційно-комунікаційні технології в процесі забезпечення громадської безпеки і правопорядку;

–умови та підстави використання ІКТ (відеоспостереження, автоматизовані бази даних, біометричні системи, аналітичні алгоритми, штучний інтелект);

– порядок обробки, зберігання та передачі інформації;

– гарантії захисту прав громадян від неправомірного використання цифрових технологій.

Таким чином, пропонуємо доповнити статтю 23 Закону України «Про Національну поліцію» новим п. 26-1 такого змісту: *«Застосовує інформаційно-комунікаційні технології, у тому числі технології розпізнавання облич, аналізу поведінкових шаблонів, геолокаційного спостереження тощо, для виявлення та фіксації правопорушень, моніторингу публічного порядку, з'ясування причин та умов правопорушень, а також аналітичної обробки інформації. Застосування інформаційно-комунікаційних технологій здійснюється відповідно до спеціального порядку, затвердженого Кабінетом Міністрів України».*

Частину першу статті 8 Закону України «Про оперативно-розшукову діяльність» доповнити пунктом 22 такого змісту: *«Застосовувати інформаційно-комунікаційні технології в тому числі програмно-апаратні засоби, бази даних, системи штучного інтелекту, аналітичні платформи, технологій розпізнавання облич, аналізу поведінкових шаблонів, геолокаційного спостереження тощо, в оперативно-розшуковій діяльності здійснюється виключно з дотриманням принципів законності, пропорційності, необхідності та забезпечення захисту прав і свобод людини і громадянина. Види інформаційно-комунікаційних технологій, порядок їх застосування, зберігання і обробки отриманої інформації, а також механізми контролю за їх використанням визначаються цим Законом та іншими нормативно-правовими актами, прийнятими відповідно до нього».*

Доповнити частину першу статті 25 Закону України «Про Службу безпеки України» новим пунктом 12-1 такого змісту: *«Застосувати сучасні інформаційно-комунікаційні технології, в тому числі розвідувальне програмне забезпечення, системи автоматизованого аналізу (включаючи ШІ) тощо, виключно в межах спеціальних процедур, визначених законом та внутрішніми регламентами СБУ».*

Доповнити пункт 7 частини другої статті 7 Закону України «Про захист персональних даних» новим абзацом такого змісту: *«Обробка персональних даних органами, що здійснюють оперативно-розшукову, слідчу або іншу правоохоронну діяльність із застосуванням інформаційно-комунікаційних технологій, допускається виключно за умови технічного аудиту системи, ведення журналу доступів та не повинна порушувати права суб'єктів персональних даних, за винятком випадків, прямо передбачених законом. Усі операції з даними (збирання, доступ, передача, аналіз) фіксуються в автоматизованому режимі. Органи, що використовують інформаційно-комунікаційні технології у роботі з персональними даними, зобов'язані пройти щорічну незалежну перевірку систем захисту інформації».*

3. Підзаконний рівень. Доцільно розробити стандарти технічного застосування ІКТ (накази МВС, СБУ, ДБР тощо), а також детальні інструкції щодо їхнього використання в окремих напрямах правоохоронної діяльності – оперативно-розшуковій, слідчій, превентивній тощо.

У цьому контексті вартої уваги є позиція науковців, які пропонують ухвалення спеціального нормативного акту, спрямованого на регулювання використання ІКТ у правоохоронній діяльності. Погоджуємось, що це дозволить забезпечити системність нормативно-правового регулювання в зазначеній сфері, а саме:

– закріпити понятійно-категоріальний апарат, що визначає ІКТ у сфері правоохоронної діяльності;

– сформулювати принципи їх використання (законність, пропорційність, обґрунтованість, технічна надійність);

– установити механізми контролю, нагляду й аудиту впровадження ІКТ;

– визначити вимоги до інтероперабельності систем, кіберзахисту та безпеки даних;

– передбачити юридичну відповідальність за зловживання та несанкціоноване використання інформації.

Таким чином, розбудова системного правового регулювання у сфері використання ІКТ не лише підвищить ефективність діяльності правоохоронних органів, але й сприятиме зміцненню гарантій дотримання прав і свобод людини в умовах цифровізації, забезпеченню прозорості роботи правоохоронних органів та формуванню довіри громадян до застосування сучасних технологій у сфері безпеки й правопорядку. Крім того, такий комплексний підхід створить підґрунтя для подальшого розвитку цифрових інструментів у правовій сфері та інтеграції України в міжнародні стандарти інформаційної безпеки та електронного правосуддя.

Висновки до розділу 1

Проведене дослідження в цьому розділі дисертаційної роботи дозволяє запропонувати такі висновки:

1. Визначено, що методологія дослідження процесу впровадження і застосування ІКТ у діяльності правоохоронних органів охоплює кілька взаємопов’язаних аспектів. По-перше, вона розглядається як вчення про процес пізнання та систему методів наукового дослідження, що визначають логіку та інструментарій наукового пошуку. По-друге, методологія виступає як практична основа здійснення наукової роботи, спрямованої на отримання нового знання у сфері цифровізації діяльності правоохоронних органів, що передбачає застосування конкретних засобів, прийомів і методів дослідження. По-третє, це сукупність методів, які використовуються у певному науковому дослідженні для досягнення поставленої мети та вирішення дослідницьких завдань. Сутність методологічних засад полягає в інтеграції різних рівнів пізнання – філософського, загальнонаукового, спеціально-юридичного й

міждисциплінарного. Вона забезпечує перехід від абстрактного розуміння ролі технологій у праві до формування конкретних концептуальних положень щодо їхнього впровадження, регулювання та контролю в діяльності правоохоронних органів, уповноважених забезпечувати законність і правопорядок. Методологічні засади визначають структуру дослідження, логіку формулювання висновків і практичних рекомендацій, забезпечуючи наукову новизну й обґрунтованість отриманих результатів.

2. Досліджено суть поняття «інформаційно-комунікаційні технології в діяльності правоохоронних органів», що полягає в ефективному використанні сучасних цифрових технологій для підвищення результативності, оперативності та прозорості роботи правоохоронних органів.

Запропоновано визначити термін *інформаційно-комунікаційні технології в діяльності правоохоронних органів як сукупність наукових, технічних, програмних і організаційних рішень, що використовуються для збирання, обробки, зберігання, передачі та аналізу інформації або створення нового інформаційного продукту з метою забезпечення законності, правопорядку, оперативного реагування на правопорушення, підтримки розслідувань і прийняття управлінських рішень у правоохоронних структурах*. Зроблено висновок, що інформаційно-комунікаційна технологія не може існувати і функціонувати сама по собі, а лише в сукупності з інформацією (будь-якими даними) та відповідною інфраструктурою, яка визначається специфікою діяльності її суб’єктів, від яких залежить виготовлення та постачання інформаційного продукту, а також його обіг за допомогою інформаційної технології.

3. Аргументовано, що використання ІКТ у діяльності правоохоронних органів спирається на поєднання базових (загальноправових) принципів, галузевих принципів, притаманних інформаційному й адміністративному праву та інституційних принципів здійснення правоохоронної діяльності. Запропоновано поділ галузевих принципів застосування ІКТ в діяльності правоохоронних органів залежно від рівня та сфери їх дії (ступеня

універсальності та спеціалізації) на: у*ніверсальні* що мають загальний, всеохоплюючий універсальний характер і застосовуються у всіх без винятку формах правоохоронної діяльності (це принципи: прозорості, відповідальності, підзвітності, необхідності і пропорційності, надійності тощо); с*пеціальні* – визначають засади роботи з окремими елементами ІКТ або дії окремих суб'єктів правоохоронної діяльності при застосуванні ІКТ (принципи: конфіденційності, оспорюваності і відшкодування, верховенство інтересів людини (людського контролю)).

Надано авторське визначення терміну *«принципи використання інформаційно-комунікаційних технологій в діяльності правоохоронних органів»* – це система керівних ідей, нормативно й доктринально обґрунтованих вимог, що визначають зміст, спрямованість та межі правового регулювання процесів упровадження, застосування і контролю за використанням ІКТ у діяльності правоохоронних органів.

4. Сформульовано зміст поняття *«правова основа застосування інформаційно-комунікаційних технологій в діяльності правоохоронних органів»,* під якою пропонується розуміти сукупність конституційних положень, міжнародно-правових стандартів, норм національного законодавства, підзаконних нормативно-правових актів і доктринальних положень, які визначають допустимі межі, порядок, форми та гарантії використання інформаційно-комунікаційних технологій правоохоронними органами з метою реалізації їхніх функцій за умови дотримання прав і свобод людини, забезпечення інформаційної безпеки та законності. Зазначено, що систематизація нормативних актів, що регулюють використання інформаційно-комунікаційних технологій у діяльності правоохоронних органів, є ключовою передумовою створення ефективного правового механізму забезпечення цифрової трансформації сфери публічної безпеки. Запропоновано розширити підходи до класифікації відповідних актів, виокремивши такі її критерії: за предметом правового регулювання; за функціональним призначенням; за ступенем спеціалізації; за напрямом впливу.

РОЗДІЛ 2
ТЕОРЕТИКО-ПРАВОВІ АСПЕКТИ ВПРОВАДЖЕННЯ І ВИКОРИСТАННЯ ОКРЕМИХ ВИДІВ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ В ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

2.1 Концептуальні засади впровадження та використання технологій штучного інтелекту правоохоронними органами у процесах збору, накопичення, обробки та аналізу інформації

Штучний інтелект є одним із найдинамічніших напрямів сучасної науки й техніки, що справляє дедалі відчутніший вплив на всі сфери суспільного життя: від економіки, охорони здоров'я та освіти до оборони, управління й безпеки. Цифрова трансформація суспільства зумовлює об'єктивну необхідність упровадження технологій ШІ також у такі чутливі сфери, як правова система та правоохоронна діяльність, де держава здійснює реалізацію своїх владних повноважень, у тому числі тих, що безпосередньо пов'язані з обмеженням прав і свобод людини.

У цьому контексті впровадження систем штучного інтелекту в правоохоронну практику набуває не лише технологічного, а й глибокого правового, етичного та соціального значення. Застосування алгоритмічних інструментів ШІ у діяльності правоохоронних органів – зокрема для запобігання кримінальним правопорушенням, аналізу ризиків, прогнозування правопорушень, ідентифікації осіб, обробки великих масивів даних чи моніторингу публічного простору – відкриває нові можливості підвищення оперативності та ефективності реагування на загрози громадській безпеці і правопорядку.

Програмні рішення на основі штучного інтелекту здатні значно перевищити людські можливості щодо швидкості оброблення інформації, виявлення закономірностей, побудови аналітичних моделей і забезпечення превентивного

контролю. Разом із тим, у правовій літературі наголошується, що масове використання таких технологій у діяльності правоохоронних органів породжує комплекс нових юридичних викликів і потребує належного нормативного врегулювання на законодавчому і галузевому рівнях. Йдеться насамперед про визначення стандартів законності, прозорості та обґрунтованості алгоритмічних рішень, а також про гарантування захисту прав людини від можливих зловживань, порушень приватності чи дискримінаційних практик [110, с. 506]. Усе це зумовлює необхідність формування концептуальних засад використання ШІ в процесах обробки інформації, зокрема визначення принципів, методів і правових механізмів, що встановлюють умови інтеграції штучного інтелекту в правоохоронну практику з урахуванням вимог законності, безпеки, надійності та забезпечення захисту прав людини..

Значний внесок у вивчення ролі штучного інтелекту в правоохоронній діяльності, розслідуванні окремих видів кримінальних правопорушень і воєнних злочинів, судочинстві, а також у підвищенні ефективності органів кримінальної юстиції в умовах воєнного стану зробили Л. Аркуша, О. Ващук, В. Гусєва, В. Журавель, І. Когутич, В. Коновалова, Є. Лук'янчиков, М. Степанюк, В. Тіщенко, Н. Філіпенко, С. Лукашевич, В. Шепітько, В. Юсупов та інші науковці. Проблемні аспекти застосування технологій штучного інтелекту в кримінальному провадженні стали предметом наукового аналізу у працях О. Верхогляд-Герасименко, Ю. Гусак, Д. Кандуєва, О. Капліної, С. Кітіка, І. Крицької, А. Туманянца, В. Шевчука та інших дослідників. Водночас комплексне дослідження ролі технологій штучного інтелекту в діяльності правоохоронних органів, а також у забезпеченні безпеки й обороноздатності України в сучасних умовах воєнного часу досі залишається фрагментарним. З огляду на це, зазначена проблематика набуває особливої актуальності, оскільки безпосередньо пов'язана з підвищенням ефективності реалізації правоохоронних функцій у сфері безпеки та оборони держави в умовах воєнного стану.

На сьогоднішній день не існує єдиного визначення штучного інтелекту, прийнятого науковою спільнотою. Це пояснюється тим, що штучний інтелект є

багатовимірним і міждисциплінарним явищем, що поєднує технологічні, когнітивні, соціальні та правові аспекти. Його дослідження відбувається на перетині різних наук – від інформатики та когнітивної психології до філософії, права, етики та соціології. Відповідно, у науковій літературі сформувалися різні підходи до вивчення ШІ, що відрізняються предметом, методами та цілями дослідження. Така різноманітність підходів відображає складність явища, багаторівневий характер інтелектуальних систем та їхню здатність взаємодіяти із соціальними і правовими інститутами. Аналіз наукової літератури в сфері дослідження ШІ дозволяє нам визначити наступні теоретичні підходи до розуміння його природи, суті і значення:

Когнітивно-символічний підхід. У межах цього підходу ШІ розглядається як система оперування символами, правилами і логічними структурами. Інтелект у такому розумінні моделюється шляхом формального опису процесів мислення та пізнання. Когнітивно-символічний підхід особливо цінний для вирішення задач, де необхідна висока точність логічного аналізу та можливість формального обґрунтування висновків. Американський учений John McCarthy, відомий як один із піонерів у галузі штучного інтелекту, запропонував концепцію «Фізичної символічної системи» (Physical Symbol System Hypothesis), яка передбачає, що система, що оперує фізичними символами, володіє необхідними та достатніми засобами для здійснення загальної інтелектуальної діяльності. Крім того, він є творцем мови програмування LISP, яка стала базовою для розробки експертних систем та інших символічних застосувань [111]. Наступні дослідники, Allen Newell та Herbert A. Simon, розробили концепцію фізичної символічної системи, яка лягла в основу їхнього підходу до штучного інтелекту. Вони створили першу експертну систему «Logic Theorist», здатну доводити теореми в символічній логіці, що стало важливим етапом у розвитку когнітивного моделювання та ШІ. Herbert A. Simon вважав, що інтелектуальна діяльність людини може бути описана як маніпуляція символами. Він також працював над створенням моделей людського пізнання та прийняття рішень, що лягли в основу когнітивної науки та ШІ [112].

Наступним етапом розвитку поглядів на штучний інтелект став *нейронний підхід.* Основоположником цього напрямку вважають американського нейропсихолога та нейрофізіолога Уоррена Маккалока. Маккалок активно брав участь у першій групі кібернетиків «Проєкт людина–машина», яка неофіційно сформувалася під час конференції в Нью-Йорку на тему «Cerebral Inhibition Meeting» (1942). Разом із Волтером Піттсом Маккалок висунув гіпотезу, згідно з якою нейрони спрощено розглядалися як пристрої, що оперують двійковими числами. На початку XX століття американський учений Клод Шеннон довів, що двійкові «одиниця» та «нуль» повністю відповідають двом станам електричного кола (включено/вимкнено), тому двійкова система є оптимальною для електронно-обчислювальних пристроїв. Маккалок і Піттс запропонували конструкцію мережі електронних нейронів та показали, що така мережа здатна виконувати практично будь-які числові та логічні операції. Згодом вони припустили, що мережа електронних нейронів може навчатися, розпізнавати образи та узагальнювати інформацію, тобто демонструє ознаки інтелекту. Отже, н*ейронно-мережевий підхід* трактує інтелект як здатність системи навчатися на основі даних, виявляти закономірності та прогнозувати результати. Такий підхід фокусується не на формальних правилах, а на динамічних процесах обробки інформації та адаптації до змінних умов. Зміст ШІ у нейронно-мережевому підході відображається через здатність системи навчатися, адаптуватися та робити прогнозні чи класифікаційні рішення, тобто ШІ не символічний, а прикладний та емпіричний [113].

Філософсько-теоретичний підхід до вивчення штучного інтелекту спрямований на осмислення природи інтелекту, свідомості та розуму, а також на визначення того, як ці концепти можуть бути відтворені в штучних системах. Він не обмежується технічними аспектами чи алгоритмами, а ставить фундаментальні питання про природу мислення та межі машинного інтелекту. Філософське осмислення ШІ передбачає аналіз різних позицій до визначення його природи – від античних уявлень про душу до сучасних дискусій про штучну свідомість. Як зазначає О. М. Варипаєв: «Філософські концепції дедалі

активніше інтегруються у сферу розробки штучного інтелекту, насамперед у контексті етичного та антропологічного супроводу технологічного проєктування. Створюється ефект когнітивного відображення, у межах якого людина трактується не як незалежний агент, а як структурний елемент цифрового середовища, що зумовлює методологічний зсув від техноцентризму до антропоорієнтованих підходів, які фіксують зміну форм людської присутності в інтелектуальному просторі. Штучний інтелект виконує не лише інструментальну функцію, а й виступає предметом філософської рефлексії, виявляючи редукціонізм у розумінні мислення» [114, с. 15]. Основною проблемою, що порушується в наукових працях, є філософське визначення природи ШІ: чи є штучний інтелект лише складним механізмом, який імітує людське мислення, чи він здатний на справжню свідомість і самосвідомість? Сучасні філософи, такі, наприклад, як Нік Бостром та Лучано Флориді, розглядають ШІ як радикальну технологію, що змінює не лише суспільство, а й саму природу людини. Вони наголошують на необхідності створення нових етичних та регуляторних норм, адже ШІ здатен досягати рівня, що принципово змінює його статус як технології [115]. Як зазначає Т. Попович: «Застосування класичних етичних принципів, заснованих на свободі вибору та відповідальності людини, до сфери ШІ виявляє їх обмеження, оскільки користувачі систем ШІ часто позбавлені можливості повністю зрозуміти природу технології та наслідки її використання. Це вимагає формування нових підходів до етичного регулювання, які поєднуватимуть прозорість технологічних процесів із забезпеченням прав та інтересів людини» [116, с. 131].

Правові та соціально-гуманітарні підходи. Стрімкий розвиток цифрових технологій і широке впровадження ШІ породили потребу в аналізі його правових та етичних аспектів. Так, у своїх працях Н. Є. Філіпенко та С. Ю. Лукашевич наголошують, що: «застосування інформаційно-комунікаційних технологій і штучного інтелекту в житті сучасної людини, соціуму й держави здебільшого носять соціально-філософський характер, оскільки вони охоплюють широкий комплекс питань із взаємодії людини та ШІ в різних сферах суспільного життя,

порушуючи, окрім власне етичних і моральних проблем, також екзистенційні, аксіологічні й інші. …До того ж, їхня дія погіршує стан і становище людини у світі. Отже, вони потребують осмислення та дозволу як з етичних міркувань, так і з позицій соціальної філософії. …В той же час використання штучного інтелекту потребує спеціального правового регулювання, оскільки йдеться про життя та здоров'я людей» [117]. Ці підходи зосереджуються на питаннях регулювання, забезпеченні прозорості алгоритмів, підзвітності рішень, захисті прав людини та запобіганні дискримінації. Вони вивчають ШІ як соціальний феномен, що впливає на державні інститути, правоохоронну діяльність, фінансові системи та інші критично важливі сфери. Серед дослідників в цьому аспекті необхідно зазначити також праці О. А. Баранова, який зазначає, що сучасні уявлення про значення та особливості застосування роботів зі ШІ, як наступного покоління розвитку ідей автоматизації діяльності людини, можна звести до двох основних пануючих груп, зміст яких є визначальним щодо встановлення їх правового статусу: робот – інструмент (об'єкт); робот – суб'єкт. [118, с. 42]. В умовах цифрової трансформації суспільства такі дослідження є ключовими для створення безпечного та етичного середовища використання інтелектуальних технологій.

В юридичній науковій літературі існують десятки варіантів визначення поняття «штучний інтелект». Так, автори комплексного дослідження «Стратегія розвитку штучного інтелекту в Україні» визначають штучний інтелект як: «функцію штучної свідомості, яка представлена створеною та контрольованою нею системою алгоритмів, забезпечує самонавчання згідно з наявною інформацією, набутими знаннями, правилами, законами суспільства та своїм досвідом, створення на цій основі нових знань для виконання доручень людини, а також здатність проводити самодіагностику й обґрунтовувати прийняті нею рішення» [119, с. 62].

Автори аналітичного звіту «Використання технологій штучного інтелекту у правоохоронній діяльності» визначають штучний інтелект як: «унікальний продукт технічного прогресу, що дає змогу машинам вчитися, використовуючи

людський і власний досвід, пристосовуватися до нових умов в рамках свого застосування, виконувати різнопланові завдання, які тривалий час були під силу лише людині, прогнозувати події й оптимізувати ресурси різного характеру. Під ним розуміється здатність автоматичних систем брати на себе функції людини, вибирати і приймати оптимальні рішення на основі раніше отриманого життєвого досвіду і аналізу зовнішніх впливів» [120, с. 9].

Г. Андрощук тлумачить поняття штучного інтелекту як «штучно створену людиною систему, здатну обробляти інформацію, яка до неї надходить, пов'язувати її зі знаннями, якими вона вже володіє, і відповідно формувати своє уявлення про об'єкти пізнання» [121, с. 85]. В свою чергу А. О. Гачкевич підходить до визначення штучного інтелекту, як виду технологій, які на основі застосування моделей, побудованих завдяки опрацюванню отриманої інформації, створюють для поставлених цілей вихідні дані – рішення, прогнози, рекомендації, контент – тотожні результатам втілення когнітивних здібностей людини [122].

Цікавим є запропоноване визначення дефініції поняття «штучний інтелект» О. А. Барановим: «це певна сукупність методів, способів, засобів та технологій, насамперед, комп'ютерних, що імітує (моделює) когнітивні функції, які мають критерії, характеристики та показники еквівалентні критеріям, характеристикам та показникам відповідних когнітивних функцій людини» [123, с. 46].

Різні міжнародні інституції також не досягли консенсусу щодо визначення змісту ШІ. Так, Європейська комісія розробила комплексний документ з цього питання, а Організація економічного співробітництва та розвитку включила визначення ШІ у свої рекомендації.

Міжнародний стандарт ISO/IEC TR 24028:2020 розглядає штучний інтелект як «здатність інженерної системи набувати, опрацьовувати та застосовувати знання та вміння» [124].

Рамкова конвенція Ради Європи «Про штучний інтелект, права людини, демократію та верховенство права» містить наступне визначення: «система штучного інтелекту» означає машинну систему, яка для досягнення явних або

неявних цілей робить висновок на основі вхідних даних, які вона отримує, про те, як генерувати вихідні дані, такі як прогнози, контент, рекомендації або рішення, які можуть впливати на фізичне або віртуальне середовище. Різні системи штучного інтелекту відрізняються за рівнем автономності та адаптивності після розгортання [125].

Чинне українське законодавство містить визначення цієї дефініції у Концепції розвитку штучного інтелекту в Україні. А саме: «Штучний інтелект – організована сукупність інформаційних технологій, із застосуванням якої можливо виконувати складні комплексні завдання шляхом використання системи наукових методів досліджень і алгоритмів обробки інформації, отриманої або самостійно створеної під час роботи, а також створювати та використовувати власні бази знань, моделі прийняття рішень, алгоритми роботи з інформацією та визначати способи досягнення поставлених завдань» [109].

Будь-який інтелект спирається на діяльність. У свою чергу, діяльність мозку – це мислення. Інтелект і мислення пов’язані багатьма цілями і завданнями: розпізнавання ситуацій, логічний аналіз, планування поведінки. Характерними особливостями інтелекту є здатність до навчання, узагальнення, накопичення досвіду, адаптація до умов, що змінюються в процесі вирішення завдань. Висока продуктивність нових технологій значною мірою залежить від використання в них алгоритмів ШІ. Впровадження штучного інтелекту у сферу правоохоронної діяльності має супроводжуватися не лише технічними стандартами, а й широкою правовою та етичною легітимацією з боку суспільства. Якщо суспільство надає поінформовану згоду на використання таких технологій, це означає, що держава зобов’язана забезпечити чітке, ефективне та пропорційне регулювання цієї сфери. Незалежно від того, йдеться про механізми саморегулювання, кодекси етики чи імперативне державне регулювання, всі моделі управління мають ґрунтуватися на загальновизнаних етичних принципах – повазі до людської гідності, недискримінації, прозорості, підзвітності та верховенстві права [126, с. 282]. Водночас, В. І. Павликівський висловлює думку, що ідеї етичного стримування технологій мають радше світоглядне та філософське значення і не

можуть розглядатися як реальний інструмент правового регулювання в умовах сучасного розвитку ШІ та автономних систем [127, с. 136]. У сучасних умовах цифровізації суспільних відносин та активного впровадження технологій штучного інтелекту у діяльність органів правопорядку постає об'єктивна необхідність у формулюванні спеціальних принципів використання ШІ правоохоронцями. Водночас слід наголосити, що ей процес здійснюється не у відриві від загальної правової системи, а, навпаки, базується на загальноправових, галузевих та міжгалузевих принципах, зокрема – законності, верховенства права, поваги до прав і свобод людини, пропорційності, добросовісності, підзвітності та прозорості.

Разом із тим, динаміка розвитку цифрових технологій та зростання ролі алгоритмічних систем у процесах прийняття рішень обумовлюють потребу у створенні єдиних юридичних стандартів і правил, спрямованих на забезпечення ефективного, безпечного та етичного використання ШІ у правоохоронній діяльності. Йдеться про своєрідний «правовий каркас», який визначатиме: межі допустимого застосування ШІ у діяльності правоохоронних органів; механізми контролю, нагляду та аудиту алгоритмічних систем; обов'язковість проведення оцінки впливу таких технологій на права людини до їхнього впровадження.

У цьому контексті формулювання спеціальних принципів впровадження та застосування ШІ набуває особливої ваги, адже саме вони мають враховувати специфіку діяльності правоохоронних органів, що пов'язана з реалізацією владних повноважень, обмеженням прав осіб, збором та обробкою персональних даних. Для цього необхідно, по-перше, науково обґрунтувати і визначити такі принципи, а по-друге – закріпити їх у чинному законодавстві, що забезпечить їхню нормативну визначеність і практичну реалізацію.

У наукових працях вітчизняних і зарубіжних дослідників (зокрема, М. Хільдебранд, Л. Флоріді, В. Бутенко, О. Петришина, Т. Гуржія) вже запропоновано низку підходів до визначення та класифікації принципів застосування ШІ. На наш погляд, найбільш універсальними з них, які повинні бути покладені в основу використання штучного інтелекту у правоохоронній

сфері, є принципи конфіденційності, оспорюваності і відшкодування, а також законної мети і верховенства інтересів людини [126, с. 283]. Саме вони створюють передумови для формування балансу між ефективністю цифрових інструментів і гарантіями дотримання основоположних прав людини у діяльності органів правопорядку. Враховуючи викладене, подальший аналіз доцільно зосередити на особливостях реалізації принципів ШІ у діяльності правоохоронних органів, які забезпечують практичне втілення зазначених засад. Це дасть змогу виявити їхнє нормативне значення, взаємозв'язок із загальноправовими принципами та роль у гарантуванні прав і свобод людини під час застосування алгоритмічних технологій у сфері правопорядку.

Принцип конфіденційності. Його зміст полягає у забезпеченні максимальної поваги до приватного життя та особистої автономії людини в умовах використання штучного інтелекту у правоохоронній діяльності. Правоохоронні органи повинні використовувати системи ШІ таким чином, щоб мінімізувати ризики порушення приватності всіх учасників правовідносин – користувачів цифрових сервісів, потерпілих, підозрюваних, свідків та інших осіб. Це передбачає охорону їхньої фізичної і психічної недоторканності, збереження особистого простору, конфіденційності комунікацій, а також безпечне поводження з персональними даними.

Повага до приватного життя є базовою вимогою законної поліцейської діяльності, адже виконання правоохоронних функцій неминуче пов'язане зі збором, аналізом і зберіганням відомостей, що стосуються особистої сфери людини. Тому обов'язок зберігати конфіденційність виступає загальним професійним стандартом для працівників правоохоронних органів, а використання ШІ лише підсилює потребу в його дотриманні. Оскільки системи штучного інтелекту істотно розширюють можливості щодо обробки даних, особливо персональних, держава має забезпечити ефективні механізми контролю, аудиту та нагляду за збереженням конфіденційності на всіх етапах життєвого циклу таких систем – від розробки алгоритмів до практичного застосування.

Водночас принцип конфіденційності є складовою реалізації принципу законності, оскільки він гарантує недопущення свавільного чи непропорційного втручання у приватну сферу особи. Будь-яке обмеження права на приватність у процесі застосування ШІ повинно відповідати критеріям легітимності, необхідності та пропорційності. Особливу увагу слід приділяти питанню формування та використання навчальних даних для алгоритмічних систем – правоохоронні органи повинні передбачати надійні гарантії конфіденційності, контролювати умови їх використання або вимагати дотримання цих стандартів від зовнішніх розробників.

Зазначений підхід узгоджується з положеннями Конвенції Ради Європи № 108+ про захист осіб стосовно автоматизованої обробки персональних даних (2018 р.), Загального регламенту ЄС про захист даних (GDPR, 2016/679), а також Рекомендаціями Ради Європи CM/Rec (2021)1 щодо впливу алгоритмічних систем на права людини. Усі ці акти наголошують на необхідності дотримання принципів конфіденційності, прозорості та підзвітності при використанні технологій, що впливають на обробку персональної інформації, особливо в діяльності органів, наділених владними повноваженнями.

Зміст принципу *оспорюваності та відшкодування* полягає у забезпеченні реальної можливості оскарження рішень, ухвалених із використанням систем штучного інтелекту, а також отримання належного відшкодування у випадках заподіяння шкоди внаслідок їх застосування. Правоохоронні органи повинні гарантувати наявність відповідних технологічних, процедурних і організаційних механізмів, що дозволяють як користувачам систем, так і особам, на яких впливають результати алгоритмічних рішень, ініціювати їх перегляд або оскарження. Це є необхідною умовою забезпечення підзвітності технологій і збереження довіри до процесів, у яких використовується ШІ.

Принцип відшкодування також передбачає, що у випадках, коли рішення, прийняті за участі ШІ, спричинили несправедливі або неправомірні наслідки, держава повинна забезпечити постраждалим особам ефективний механізм захисту і компенсації. Це включає можливість звернення до компетентних

органів із вимогою про перегляд рішення або відшкодування завданої шкоди. Відповідно, цей принцип тісно пов'язаний із правом людини на ефективний засіб правового захисту та є проявом принципу законності у сфері застосування технологій штучного інтелекту.

Слід визнати, що навіть за умов високої технічної досконалості системи ШІ не є безпомилковими, а їхні результати можуть містити похибки, що призводять до порушення прав людини. Тому для зміцнення суспільної довіри до використання штучного інтелекту в правоохоронній діяльності необхідно забезпечити гарантовану можливість оскарження і компенсації шкоди для всіх осіб, яких можуть торкатися такі рішення.

Положення цього принципу узгоджуються з Концепцією розвитку штучного інтелекту в Україні яка визначає, що одним з принципів розвитку та використання технологій штучного інтелекту є «покладення на організації та осіб, які розробляють, впроваджують або використовують системи штучного інтелекту, відповідальності за їх належне функціонування відповідно до зазначених принципів» [109].

Принцип верховенства інтересів людини. Його сутність полягає у визнанні людини, її гідності, свобод і прав найвищою цінністю у процесі впровадження та використання технологій штучного інтелекту в правоохоронній діяльності. Таке визначення змісту принципу відповідає як національним стандартам прав людини (зокрема Конституції України), так і текстам міжнародних документів, таких як Декларація Блетчлі (The Bletchley Declaration), що була прийнята країнами-учасницями саміту з безпеки ШІ 1–2 листопада 2023 року. У цій декларації підкреслюється, що ШІ має бути розробленим, розгорнутим та використаним таким чином, щоб залишатися орієнтованим на людині, надійним, відповідальним і безпечним [128].

Людська свобода волі передбачає здатність діяти відповідно до власних рішень, здійснювати вибір і досягати цілей без примусу, маніпуляцій чи технічного тиску. Відтак правоохоронні органи повинні гарантувати, що системи штучного інтелекту, які вони впроваджують, не обмежують автономію людини

та не підміняють її свідомі рішення, а лише сприяють підвищенню ефективності діяльності. Застосування ШІ має здійснюватися з урахуванням необхідності збереження людського контролю над ключовими процесами. Якщо посадові особи чи установи надмірно покладаються на результати, згенеровані алгоритмами, ігноруючи власну аналітичну оцінку або етичні міркування, це може спричинити серйозні помилки й завдати шкоди як окремим особам, так і суспільству загалом. Тому системи штучного інтелекту повинні бути сконструйовані таким чином, щоб підтримувати та доповнювати рішення людини, а не заміщати їх. Особливе значення має належна підготовка персоналу, який працює з технологіями ШІ, з метою формування компетенцій, що дозволяють використовувати ці системи свідомо, відповідально та критично.

На інституційному рівні дотримання цього принципу передбачає уникнення надмірної технологічної залежності правоохоронних органів від систем ШІ, яка може порушити баланс між інноваціями та правовими ризиками. Необхідно підтримувати професійні навички працівників, зокрема здатність здійснювати оперативний аналіз, ухвалювати рішення й реагувати на нестандартні ситуації незалежно від функціонування алгоритмічних систем. Таким чином, технологічні рішення повинні залишатися допоміжним засобом, а не основним чинником прийняття рішень у сфері правопорядку.

Ще одним важливим аспектом реалізації принципу верховенства інтересів людини є захист права на інформацію та недопущення маніпулювання поведінкою громадян за допомогою алгоритмічних механізмів. Зокрема, використання чат-ботів або автоматизованих систем для надання правової допомоги чи прийому скарг має супроводжуватися належним аудитом, тестуванням і моніторингом їхньої роботи, щоб уникнути упередженості або помилок, які можуть обмежити доступ до інформації та вплинути на можливість особи приймати незалежні рішення. Зміст цього принципу безпосередньо узгоджується з Рекомендаціями ЮНЕСКО щодо етики штучного інтелекту [129], у яких підкреслюється, що ШІ має служити людині, сприяти розвитку її потенціалу та ніколи не замінювати її як автономного суб’єкта прийняття рішень.

Дотримання принципу верховенства інтересів людини є ключовою умовою забезпечення етичної легітимності та правової допустимості використання ШІ у правоохоронній діяльності.

З огляду на розглянуті принципи використання штучного інтелекту правоохоронними органами, логічним продовженням цього дослідження є аналіз суб'єктного складу відповідних правовідносин та встановлення взаємозв'язків між учасниками у процесі застосування ШІ. Адже ефективність реалізації визначених принципів значною мірою залежить від того, які органи та посадові особи уповноважені здійснювати впровадження, контроль і нагляд за застосуванням технологій ШІ, а також від чіткості розподілу їхніх повноважень і відповідальності. Саме тому подальший розгляд має бути присвячений визначенню системи суб'єктів, їх функцій та ролі у процесі використання ШІ, а також механізмів координації та підзвітності між ними з метою забезпечення законності, прозорості та захисту прав людини у використанні інтелектуальних технологій.

Суб'єкти використання штучного інтелекту в правоохоронній діяльності становлять систему органів, установ, посадових осіб та інших учасників, наділених відповідними повноваженнями щодо розроблення, впровадження, застосування, контролю й нагляду за використанням технологій ШІ у сфері забезпечення правопорядку. Їх можна поділити на кілька основних груп залежно від функціонального призначення.

У першу групу необхідно віднести безпосередньо правоохоронні органи, уповноважені законом здійснювати оперативно-розшукову, кримінально-процесуальну та іншу правоохоронну діяльність із використанням ІКТ і ШІ, а саме:

– Національна поліція України – діє відповідно до Закону України «Про Національну поліцію» від 02.07.2015 № 580-VIII, який визначає завдання поліції щодо забезпечення публічної безпеки, запобігання злочинам та використання сучасних інформаційних технологій (ст. 23, 25).

– Служба безпеки України – здійснює заходи з протидії тероризму, кіберзагрозам і захисту державної безпеки на підставі Закону України «Про Службу безпеки України» від 25.03.1992 № 2229-XII (ст. 2, 7).

– Національне антикорупційне бюро України – діє відповідно до Закону України «Про Національне антикорупційне бюро України» від 14.10.2014 № 1698-VII (ст. 1, 7), який визначає використання інформаційно-аналітичних систем у сфері запобігання та протидії корупції.

– Державне бюро розслідувань – керується Законом України «Про Державне бюро розслідувань» від 12.11.2015 № 794-VIII (ст. 1, 4, 5), що передбачає застосування новітніх технологій для ефективності досудового розслідування.

– Офіс Генерального прокурора – відповідно до Закону України «Про прокуратуру» від 14.10.2014 № 1697-VII (ст. 2, 6), здійснює нагляд за додержанням законності при застосуванні ШІ та ІКТ у діяльності правоохоронних органів.

Другу групу становлять органи державного управління і регулювання. Ця група формує державну політику, стандарти та нормативне забезпечення у сфері ШІ:

– Міністерство цифрової трансформації України (Мінцифра) – відповідно до Положення про Міністерство цифрової трансформації України, затвердженого постановою КМУ від 18.09.2019 № 856, є головним органом у системі центральних органів виконавчої влади, що реалізує державну політику у сфері цифровізації, розвитку штучного інтелекту та захисту даних.

– Міністерство внутрішніх справ України – діє на основі Положення про Міністерство внутрішніх справ України, затвердженого постановою КМУ від 28.10.2015 № 878, яке визначає його повноваження щодо координації впровадження ІКТ у правоохоронних органах.

– Верховна Рада України – встановлює правові засади використання ШІ через ухвалення законів, зокрема Закону України «Про інформацію» від

02.10.1992 № 2657-XII та Закону України «Про захист персональних даних» від 01.06.2010 № 2297-VI, які містять базові принципи обробки інформації й персональних даних у цифровому середовищі.

В третю групу об'єднаємо Інституції контролю, нагляду та захисту прав людини. Такі, як:

– Уповноважений Верховної Ради України з прав людини – діє на підставі Закону України «Про Уповноваженого Верховної Ради України з прав людини» від 23.12.1997 № 776/97-ВР (ст. 13–17), здійснюючи парламентський контроль за дотриманням прав і свобод у сфері автоматизованої обробки даних.

– Національна комісія із захисту персональних даних та доступу до публічної інформації – її створення запропоновано у проєкті Закону України «Про захист персональних даних» (нова редакція, 2023), що узгоджується з вимогами Регламенту ЄС 2016/679 (GDPR).

– Громадські організації (наприклад, Digital Security Lab, Privacy Hub, CEDem, Ініціатива AI4Ukraine / AI4UA) – здійснюють незалежну експертизу алгоритмів та етичного використання ШІ.

Наступна (четверта) група складається з розробників та технічних адміністраторів систем ШІ. Серед них – державні наукові установи, ІТ-компанії, дослідницькі центри, які несуть відповідальність за технічну безпеку, надійність і відповідність розроблених систем вимогам законодавства. Їхня діяльність регулюється Законом України «Про наукову і науково-технічну діяльність» від 26.11.2015 № 848-VIII [130]; Законом України «Про технічні регламенти та оцінку відповідності» від 15.01.2015 № 124-VIII [131].

Нарешті останню (п'яту), але не менш важливу групу становлять громадяни, які виступають одночасно користувачами систем ШІ та суб'єктами, на яких впливають рішення, ухвалені з використанням алгоритмічних технологій. Вони є кінцевими бенефіціарами застосування ШІ, адже технології мають підвищувати ефективність правоохоронної діяльності, не порушуючи при цьому права і свободи людини. Так, громадяни мають право на оскарження рішень, прийнятих із застосуванням ШІ, включаючи можливість вимагати перевірки, перегляду або

скасування рішень у разі, якщо вони були прийняті з порушенням закону або призвели до несправедливих наслідків. Це право тісно пов'язане з обов'язком органів забезпечити прозорість, пояснюваність та підзвітність алгоритмічних систем, що використовуються в правоохоронній діяльності. Також, громадяни мають право на відшкодування шкоди, завданої внаслідок неправомірного або некоректного застосування систем ШІ. Держава зобов'язана створити належні механізми для реалізації цього права, забезпечуючи доступність процесу відшкодування та ефективний правовий захист. Це включає як адміністративні, так і судові процедури, які дозволяють особам, чиї права порушені, звертатися за компенсацією шкоди.

Не менш важливим є право громадян на захист персональних даних. Системи ШІ в правоохоронній сфері обробляють великі обсяги інформації, включно з даними про приватне життя громадян. Законодавство України гарантує громадянам контроль за власними даними та право знати, як і з якою метою вони використовуються, а також право вимагати їх коригування чи видалення у випадках неправомірної обробки. Основою цих прав є такі нормативно-правові акти:

– Конституція України (ст. 3, 32, 55) – закріплює верховенство прав людини, право на свободу та недоторканність приватного життя, а також на судовий захист своїх прав;

– Закон України «Про звернення громадян» [132] – регламентує порядок подання скарг, заяв і запитів до органів влади та гарантує розгляд звернень громадян у встановлені терміни;

– Закон України «Про інформацію» [133] (ст. 31-33) – визначає право на доступ до інформації, обмеження щодо обробки даних та механізми захисту від незаконного використання інформації.

Отже, громадяни є одними з ключових суб'єктів правовідносин у сфері застосування ШІ правоохоронними органами, оскільки їхні права та інтереси визначають межі допустимого використання технологій, стимулюють створення

прозорих та підзвітних алгоритмічних систем, а також забезпечують баланс між ефективністю правоохоронної діяльності та дотриманням прав людини.

Таким чином, система суб'єктів використання ШІ в процесі забезпечення правопорядку є багаторівневою, що охоплює як органи державної влади, так і суспільні інституції. Її ефективне функціонування потребує належного розподілу компетенцій, взаємодії та відповідальності, що є передумовою законного й етичного застосування штучного інтелекту.

Для ефективного впровадження, використання та контролю систем штучного інтелекту у правоохоронній сфері необхідна чітко структурована система координації та підзвітності, що забезпечує взаємодію між усіма зазначеними вище суб'єктами – від державних органів до громадян. Так, базові механізми координації та підзвітності у використанні ШІ в правоохоронній сфері частково відображені в чинному законодавстві України, хоча ще не завжди безпосередньо стосуються штучного інтелекту. Така система включає кілька рівнів і форм механізмів. Наприклад, *Міжвідомчу координацію та контроль* за законністю використання алгоритмів ШІ у своїй діяльності правоохоронними органами можна забезпечити шляхом створення міжвідомчих робочих груп або комісій на базі Міністерства внутрішніх справ та Мінцифри для розробки, тестування та впровадження алгоритмічних систем. Ці групи можуть об'єднати представників правоохоронних органів, наукових установ, розробників і контролюючих органів. Також було б корисним створити спільні аналітичні платформи, які дозволють обмінюватися даними про ефективність систем, виявляти помилки та ризики порушення прав людини. Загальні засади міжвідомчої взаємодії закріплюються, наприклад, Законом України «Про Національну поліцію», який встановлює, що поліція діє на підставі законів та під контролем центральних органів виконавчої влади, а також координує діяльність між територіальними підрозділами» (ст. 23-25) та Положенням про Міністерство внутрішніх справ України, затверджене Постановою КМУ від 28 жовтня 2015 р. [134] яке зазначає, що МВС «здійснює інформаційну взаємодію з іншими державними органами» і визначає взаємодію МВС із підпорядкованими

органами, включно з інформаційними системами та технологічною підтримкою. Звісно, ці норми носять загальний характер, але їх можна застосовувати і в сфері впровадження ШІ в діяльність правоохоронних органів.

Підзвітність правоохоронних органів перед державними регуляторами має закріплюватися нормативно визначеним обов'язком звітування перед МВС, Генеральною прокуратурою, Мінцифрою про використання ШІ: типи застосованих алгоритмів, обсяг оброблюваних даних, результати аналізу та оцінки впливу на права людини. Також має бути передбачений внутрішній аудит і перевірки: правоохоронні органи проводять регулярний аудит алгоритмів і процесів, а зовнішні регулятори контролюють відповідність застосування ШІ законодавству та етичним стандартам. На сьогодні, чинне законодавство встановлює обов'язок Національної поліції, СБУ, НАБУ, ДБР, Прокуратури звітувати про свою діяльність перед парламентом та іншими контролюючими органами. Наприклад, Закон України «Про Національну поліцію» у п.3 ст.28 встановлює, що «Міністерство внутрішніх справ України у межах компетенції здійснює контроль за дотриманням вимог законів та інших нормативно-правових актів під час формування та користування поліцейськими інформаційними реєстрами та базами (банками) даних». Здійснення внутрішнього контролю за застосуванням інформаційно- аналітичного забезпечення прокурорів передбачено в Законах України: «Про прокуратуру» (ст. ст. 11,13); «Про інформацію» і «Про захист персональних даних», які регламентують порядок обробки інформації та забезпечують правовий механізм контролю за доступом до даних. Ці акти створюють законодавчу основу для звітності та внутрішнього аудиту в тому числі і алгоритмічних систем.

Підзвітність перед громадянами та суспільством забезпечується нормативним визначенням механізмів оскарження рішень, прийнятих із застосуванням ШІ, які дозволяють постраждалим особам або користувачам систем ініціювати перевірку або перегляд рішень через офіційні канали (скарги, адміністративні позови, звернення до омбудсмана). Конституція України (ст. ст. 3, 32, 55) гарантує права на приватність, захист персональних даних та доступ

до правового захисту. Закони України «Про звернення громадян» і «Про доступ до публічної інформації» [135] визначають право на подання скарг, заяв і запитів до органів влади. Закон України «Про інформацію» (ст. ст. 31-33) також встановлює право громадян на доступ до відкритої публічної інформації, що дозволяє контролювати роботу органів влади.

Взаємна відповідальність розробників та адміністраторів систем ШІ полягає в дотриманні технічних та етичних стандартів при створенні алгоритмів, включаючи аудит даних, перевірку на упередженість і помилки, а також тестування на відповідність законодавству. Важливим на цьому рівні є впровадження систем моніторингу та журналів подій, які фіксують діяльність ШІ, використання даних та прийняті рішення, що дозволяє відстежувати будь-які порушення та забезпечує доказову базу для контролю. Наприклад, Закон України «Про Національну поліцію» встановлює вимогу щодо фіксаії кожної дії посадової особи щодо отримання інформації з інформаційних ресурсів органів державної влади. Такі дії фіксуються «..у спеціальному електронному архіві інформаційно-комунікаційної системи, за допомогою якої отримано відомості. В електронному архіві фіксуються прізвище, ім’я, по батькові, посада та номер спеціального жетона (в разі наявності), вид отриманої інформації, реєстр, з якого отримувалася інформація, час отримання інформації та інші дані, необхідні для ідентифікації особи, яка отримувала інформацію з інформаційних ресурсів, реєстрів та баз (банків) даних.» (ст. 27 Закону). Закони України «Про захист персональних даних» та «Про інформацію» регламентують аудит і перевірку використання персональних даних, що застосовуються у алгоритмах. Ці документи створюють юридичну базу для аудиту алгоритмів, хоча спеціальних норм щодо ШІ поки що не впроваджено. Водночас робота правоохоронних органів на сучасному етапі все більше потребує застосування новітніх технологій, а значить потреба в спеціальному нормативному регулюванні є все більш нагальною.

Розглянуті вище принципи використання штучного інтелекту в правоохоронній діяльності, а також окреслення системи правоохоронних органів,

які застосовують відповідні технології, та характеру їх взаємозв'язків, формують необхідне теоретико-правове підґрунтя для подальшого аналізу. Водночас наведені загальні положення потребують конкретизації через дослідження практичного виміру застосування ШІ. У зв'язку з цим логічним наступним кроком є перехід до характеристики окремих технологій з елементами штучного інтелекту, що використовуються правоохоронними структурами у щоденній діяльності (зокрема в аналітичній роботі, обробці масивів даних, прогнозуванні ризиків, розпізнаванні образів, документуванні своєї діяльності). Саме аналіз таких технологій дозволяє встановити, як принципи та організаційно-правові механізми реалізуються на практиці, а також виявити правові ризики і межі допустимого використання ШІ у правоохоронній сфері.

Отже, в сучасному світі збір і накопичення інформації, необхідної для реалізації функції правоохоронного органу здійснюється за допомогою використання різноманітних технічних засобів та інформаційних джерел, таких як: камери відеоспостереження, соціальні мережі, інформаційні системи і бази даних, публікації в ЗМІ і мережі Інтернет, повідомлення громадян тощо. Надвеликі обсяги інформації потребують автоматизованої обробки і аналітики. Тому використання алгоритмів ШІ є нагальною необхідністю. Наприклад, в Україні застосовується програмне забезпечення з алгоритмами ШІ при перевірці декларації особи, уповноваженої на виконання функцій держави або місцевого самоврядування. Відповідна процедура, її підстави і наслідки закріплені в «Порядку проведення повної перевірки декларації особи, уповноваженої на виконання функцій держави або місцевого самоврядування», затвердженого Наказом Національного агентства з питань запобігання корупції від 29 січня 2021 року № 26/21 [136]. Документ визначає, що за допомогою програмних засобів Єдиного державного реєстру декларацій осіб, уповноважених на виконання функцій держави або місцевого самоврядування, за результатами проведеного логічного та арифметичного контролю визначається показник рейтингу ризику декларації – тобто числовий показник ступеня виявлених невідповідностей (ризиків) у декларації. За офіційними даними, опублікованими на офіційній

сторінці Національного агентства з питань запобігання корупції (НАЗК) та Східного міжрегіонального управління Державної служби України з питань праці, спостерігається суттєве зростання кількості декларацій, що успішно проходять автоматизовану перевірку, що підтверджує ефективність ризик-орієнтованого підходу та використання алгоритмічних інструментів обробки декларацій. Така динаміка може бути зумовлена як підвищенням рівня доброчесності суб'єктів декларування, так і удосконаленням програмних засобів Єдиного державного реєстру декларацій (*Таблиця 2.1*) [137].

Таблиця 2.1

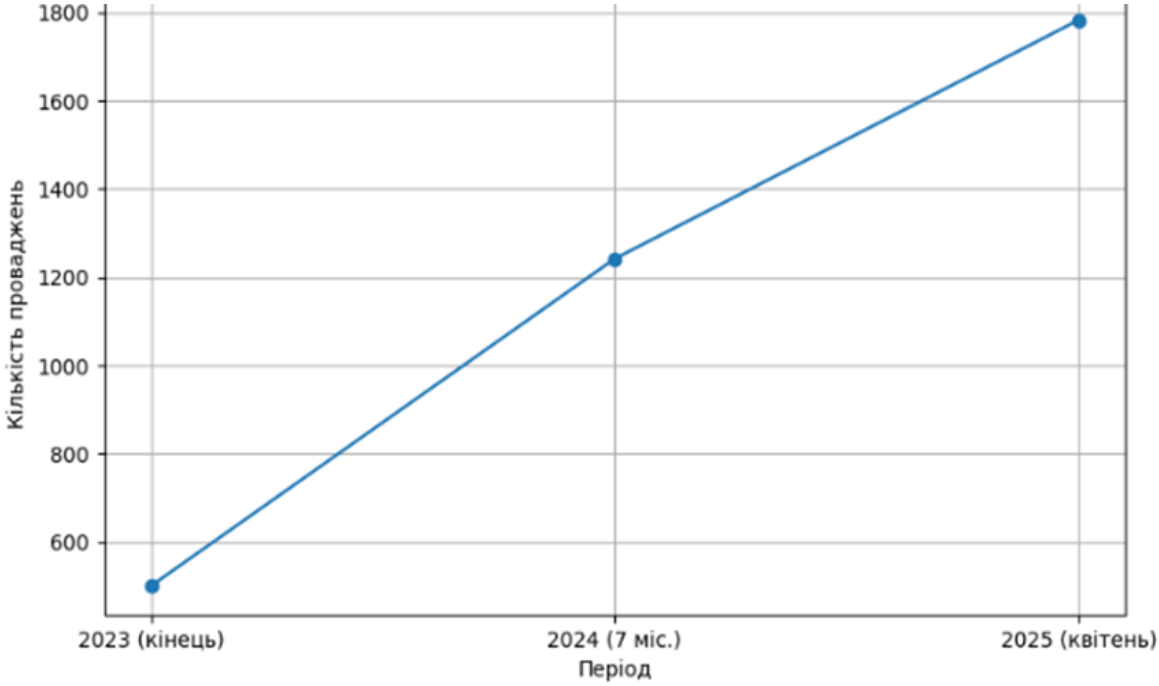
Динаміка результатів автоматизованих перевірок декларацій (2021–2025 рр.)

Рік	Допущені до автоперевірки	Успішно пройшли	Неуспішно пройшли
2021	583 919	163 970	**419 949**
2022	546 006	143 169	**402 837**
2023	621 280	146 769	**474 511**
2024	596 659	241 284	**355 375**
2025*	≈ 670 000	≈ 320 000	**≈ 350 000**

* 2025 рік — на основі офіційних повідомлень НАЗК про понад 670 тис. декларацій та зафіксованого зростання частки успішних автоперевірок.

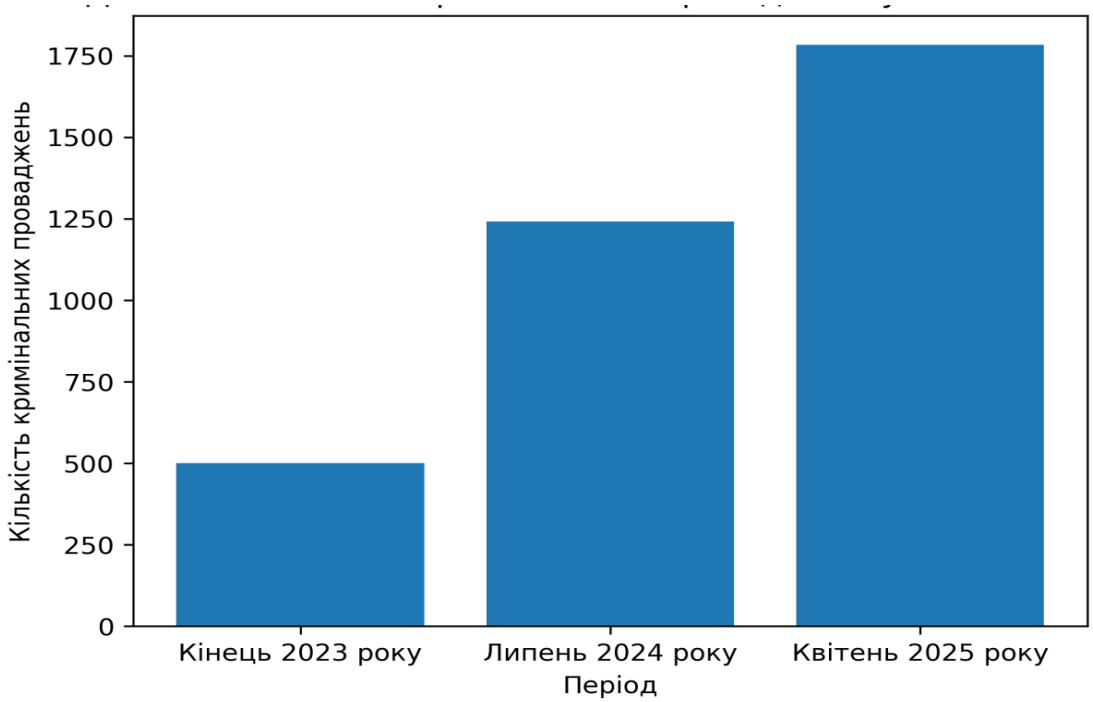
16 грудня 2021 року Національне антикорупційне бюро України та Спеціалізована антикорупційна прокуратура (САП) розпочали реєстрацію перших кримінальних проваджень у системі iCase, що передбачає поступовий перехід на електронний обмін документами у кримінальному провадженні за участі НАБУ, САП та Вищого антикорупційного суду (ВАКС). Це стало початком нового етапу цифровізації кримінальної юстиції в Україні. Після початку повномасштабного вторгнення процес тимчасово призупинився до літа 2022 року. Наразі система iCase активно розвивається, зростає кількість внесених кримінальних проваджень. Станом на кінець 2023 року до системи було внесено понад 500 проваджень, а за перші сім місяців 2024 року їхня кількість зросла у 2,5 рази – до 1 242. За даними офіційних джерел, станом на квітень 2025 року до

системи iCase внесено 1 783 кримінальних проваджень (*Малюнок 2.1*). Система також дозволяє автоматично генерувати процесуальні документи за 67 типових форм, що істотно скорочує час на взаємодію між учасниками кримінального провадження.



Малюнок 2.1 Кількість кримінальних проваджень, внесених у систему iCase, з кінця 2023 року до квітня 2025 року

У 2025 році підрозділи НАБУ та САП використали систему для подання 730 клопотань до Вищого антикорупційного суду за чотири місяці *(Малюнок 2.2)*. При цьому 434 клопотання про обрання запобіжного заходу підозрюваним було подано через iCase, що становить майже 80 % від загальної кількості таких клопотань. Водночас 287 клопотань про тимчасовий доступ до речей і документів було подано через цю систему, що становить приблизно 60 % від загального обсягу таких клопотань [138].



Малюнок 2.2 Кількість клопотань, поданих до Вищого антикорупційного суду через систему iCase за перші чотири місяці 2025 року

Треба зазначити, що в межах даного дисертаційного дослідження неможливо охопити науковим аналізом увесь спектр інформаційних технологій, які використовуються правоохоронцями під час здійснення своїх повноважень. Тому в подальшому буде зосереджено увагу на найбільш цікавих та корисних, на наш погляд, технологіях з елементами штучного інтелекту, які вже використовуються в практичній діяльності окремих правоохоронних органів, зокрема в діяльності Національної поліції, СБУ та ДБР. Це: 1) відеоспостереження (або відео аналітика); 2) технологія розпізнавання обличь; 3) генерація документів штучним інтелектом.

1. **Відеоспостереження у правоохоронній сфері** в умовах сьогодення відіграє ключову роль, адже у сучасному цифровому середовищі інформаційні дані набувають ключового значення як джерело та інструмент для правоохоронних органів у забезпеченні громадської безпеки. Виконання повноважень із підтримки правопорядку здійснюється із застосуванням ІКТ та алгоритмів штучного інтелекту, серед яких особливе місце займають системи відеоспостереження з інтегрованою ШІ-аналітикою. Наприклад, застосування

алгоритмів ШІ може значно підвищити ефективність і дієвість поліцейських центрів, що працюють в режимі реального часу, автоматизувавши аналіз великих обсягів даних, надаючи інформацію в реальному часі та прогнозуючи злочинну діяльність. Системи ШІ можуть відстежувати записи з камер спостереження, виявляти підозрілу поведінку та сповіщати правоохоронців про потенційні загрози, дозволяючи їм швидше й точніше реагувати на інциденти, а також оптимізувати процес документування інцидентів шляхом створення детальних і неупереджених звітів, що заощадить час співробітників і забезпечить узгодженість записів. Аналізуючи дані з різних джерел, таких як соціальні медіа, публічні записи та сенсорні мережі, ШІ може допомогти визначити закономірності та тенденції, які можуть свідчити про нові злочинні дії, уможливлюючи профілактичні заходи для запобігання злочинам ще до того, як вони відбудуться.

Так, використання ШІ при зборі й аналізі інформації, отриманої з камер відеоспостереження вже декілька років застосовується правоохоронними органами України в різних регіонах країни. Наприклад у м. Вінниця була впроваджена система автоматичного розпізнавання номерів та типу автомобілів. У роботу Ситуаційного центру ГУНП та підрозділів вінницької поліції впроваджено безпековий проєкт «Vezha», в основі якого лежить використання нейронових мереж та ШІ аналітики відеопотоку з понад 600 камер відеоспостереження, які працюють як на вулицях, так і всередині комунальних закладів: зокрема в школах та «Прозорих офісах» [120]. Даний програмний продукт має можливості для:

– автоматичної ідентифікації номерних знаків та збору та зберігання відповідної інформації про транспортні засоби, які потребують ідентифікації;

– виявлення та розпізнавання осіб у потоці людей, а також визначення їх статі, віку, раси та етнічної приналежності;

– розпізнавання типу об'єктів та надає попередження відповідно до заданих правил;

– аналітики трафіку для визначення рівня навантаженості доріг та інтенсивності руху людей;

– для ефективного відстеження людей з різних камер, пошуку зниклих дітей у місцях масового скупчення та ідентифікації людей за їх зовнішніми ознаками;

– детекції зброї – розпізнає різні типи зброї в режимі реального часу за допомогою існуючих камер та обладнання.

У м. Маріуполі до 2022 року поліція використовувала у своїй роботі можливості унікального Єдиного аналітичного сервісного центру, в основу якого покладено новітні технології ШІ та машинного навчання. Система, яка базується на аналітичній платформі ULA, здійснювала моніторинг оперативної ситуації у регіоні. Поліція обробляла сигнали, отримані від інтелектуальної відеоаналітики та мобільних додатків, щоб реагувати на ситуацію у режимі реального часу, та відправляти на місце події наряди, які знаходяться найближче [120].

У м. Харків деякий час працював програмно-апаратний комплекс аналітичного супроводу оперативно-розшукової діяльності та підтримки прийняття рішень (Ricas), який розробили співробітники Управління інформаційного забезпечення ГУ НПУ в Харківській області спільно з місцевими ІТ-компаніями. Головною особливістю системи була візуалізація на географічній карті інформації НП України з її подальшим аналізом. RICAS дозволяв виконувати наступні види аналізу: кримінальної обстановки; розслідувань; загального профілю; конкретного розслідування; групової злочинності.

За даними річного звіту Національної поліції за 2024 рік, у регіонах активно розвивається система відеонагляду: підрозділи поліції мають доступ до понад 68,7 тис. камер, з яких 44,5 тис. належать до системи «Безпечне місто/регіон», у тому числі 9,7 тис. – з аналітичними можливостями. Водночас введено в експериментальну експлуатацію інтеграційну платформу відеоспостереження та відеоаналітики НПУ, до якої інтегровано низку регіональних систем; загалом підключено понад 11,1 тис. камер, із них 2,7 тис. – з аналітичними функціями. Окремим напрямом цифровізації є підвищення рівня безпеки дорожнього руху шляхом впровадження системи автоматичної фіксації адміністративних

правопорушень: за перші два роки до неї підключено 293 стаціонарні технічні засоби. На жаль, статистична інформація за 2025 рік поки що відсутня [139].

Проблема правомірності встановлення та використання апаратних комплексів відеоспостереження полягає в тому, що в Україні відсутній нормативний акт, який надавав би державним органам або органам місцевого самоврядування право здійснювати масовий нагляд за життям громадян. На практиці більшість таких систем перебуває на балансі місцевих органів влади або комунальних підприємств, однак у них немає чітких правових підстав для встановлення обладнання чи доступу до баз даних інших органів, наприклад, для функції розпізнавання облич. Кожен регіон самостійно визначає порядок обробки відеопотоків, використовуючи обладнання з різним технічним та програмним забезпеченням, що ускладнює інтеграцію муніципальних систем з інформаційними мережами Національної поліції. Доступ правоохоронців до відеоданих часто можливий лише за попереднім дозволом власника системи – органів місцевого самоврядування, які не мають єдиного підходу щодо надання такої можливості. Водночас правоохоронні органи можуть вести відеоспостереження лише за окремими громадянами на підставі та в порядку, передбаченому Законом України «Про оперативно-розшукову діяльність». Таким чином, відсутність узгодженого законодавчого регулювання створює «конфлікт інтересів» та негативно впливає на рівень громадської безпеки. На наш погляд, встановлення і використання систем відеоспостереження в громадських місцях, на дорогах, в громадському транспорті має підпорядковуватися правоохоронним органам [140, с. 67]. Це дозволить усунути правову невизначеність та забезпечити ефективну взаємодію між правоохоронними органами та місцевими адміністраціями. Крім того, підпорядкування систем відеоспостереження у громадських місцях правоохоронним органам сприятиме підвищенню рівня громадської безпеки. Використання відеоаналітики на основі ШІ трансформує підхід до моніторингу публічного простору – від пасивного спостереження до активного аналітичного контролю, що значно підвищує ефективність і превентивний потенціал діяльності правоохоронних органів.

2. **Технологія «система розпізнавання облич»** («Facial recognition technology» або FRT) у межах впровадження можливостей штучного інтелекту в роботі підрозділів Національної поліції, СБУ, ДБР та інших структур набуває особливого значення. Практичне застосування систем розпізнавання облич у правоохоронних органах передбачає поєднання технологічних і правових аспектів: від належної організації збору й обробки відеоінформації до встановлення правил зберігання даних, контролю за доступом і механізмів оскарження рішень, ухвалених на основі ШІ. Таке поєднання забезпечує баланс між ефективністю правоохоронної діяльності та захистом прав і свобод громадян, а також створює основу для формування національної практики етичного та законного використання технологій штучного інтелекту. Тому необхідно провести комплексний аналіз технологічних можливостей і правового регулювання розпізнавання облич як складової частини процесів збору, накопичення, обробки та аналізу інформації у правоохоронних органах.

В якості прикладу ефективності використання цієї технології українськими правоохоронцями, можна навести результати роботи з американською платформою Clearview AI за допомогою якої прикордонники змогли ідентифікувати понад 10 000 осіб, серед яких: захоплені громадяни України; особи, причетні до незаконного перевезення дітей з тимчасово окупованих територій України до Російської Федерації; військовослужбовці Російської Федерації та члени Збройних сил Росії; російські пропагандисти, які надають матеріальну підтримку окупаційним військам та беруть участь в інформаційній війні проти України; колаборанти та зрадники України; особи, причетні до кримінальних та адміністративних правопорушень тощо. Як зазначив заступник Міністра внутрішніх справ України Леонід Тимченко «З початком військової агресії Російської Федерації проти України оперативні підрозділи Національної поліції України та Міністерства внутрішніх справ використовують цифрову платформу американської компанії Clearview AI в ідентифікації осіб під час документування воєнних злочинів» [141]. За даними офіційних повідомлень та інтерв’ю з представниками українських державних установ, понад 1 500

співробітників із 18 урядових органів, серед яких Національна поліція, Державна прикордонна служба, прокуратури та Державне бюро розслідувань, активно використовують цю технологію для ідентифікації осіб. В межах воєнного конфлікту станом на кінець 2023 року за допомогою Clearview AI було ідентифіковано понад 230 000 російських військовослужбовців та осіб, причетних до агресії проти України, а також більше 71 000 загиблих військовослужбовців Російської Федерації, інформація про яких була опублікована на спеціалізованому вебресурсі *Poter.net*. Крім того, за допомогою технології вдалося встановити місцеперебування 198 українських дітей, насильно вивезених до Росії або на тимчасово окуповані території [142].

В той же час використання систем відеоспостереження тісно перетинається з певними обмеженнями, які встановлені інформаційним законодавством. Технології розпізнавання облич – це перш за все обробка персональних даних, для яких діє спеціальний правовий режим доступу. Основні застереження стосуються питань конфіденційності і захисту зібраної інформації, а тому законодавець має встановити чіткі правила щодо суб'єктів, об'єктів, підстав та умов застосовування FRT [143].

Використання технологій розпізнавання обличчя в реальному часі передбачає збір, порівняння та/або зберігання зображень облич в ІТ-системі з метою ідентифікації особи. Таким чином, це є втручанням у право на захист персональних даних, передбачене Законом України «Про захист персональних даних». Але, стаття 7 Закону України «Про захист персональних даних» визначає що заборона на обробку персональних даних не застосовується, якщо вона «стосується вироків суду, виконання завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом та здійснюється державним органом в межах його повноважень, визначених законом». На наш погляд таке формулювання є доволі широким, не встановлює межі необхідності і не передбачає дотримання принципу пропорційності, а тому може використовуватись неправомірно. В цьому контексті, може бути корисним законодавчий досвід ЄС, який має вже певну нормативну базу в цій сфері, яка

затвердила стандарти і визначила критерії пропорційності і необхідності використання FRT в діяльності поліції [143], [144].

Мета застосування технології розпізнавання облич завжди визначається конкретною сферою її використання. Такі системи не можуть застосовуватися без обмежень. Використання FRT має обмежуватися як щодо типів злочинів, так і щодо категорій осіб, які підлягають ідентифікації. Наприклад, у сфері кримінального права, FRT доцільно застосовувати, зокрема, у справах про тяжкі та особливо тяжкі злочини, що становлять серйозну загрозу національній безпеці (наприклад, внутрішній або міжнародний тероризм) або громадському здоров'ю (наприклад, контроль за розповсюдженням інфекційних захворювань, коли FRT може допомогти у визначенні контактних осіб).

Щодо суб'єктів ідентифікації, законодавство має чітко визначати категорії осіб, щодо яких допускається використання FRT. Це можуть бути: жертви злочинів, зокрема зниклі діти; особи, підозрювані або причетні до вчинення злочинів, що підпадають під тяжкі категорії; люди, зниклі безвісти внаслідок бойових дій або окупації територій. Звісно, кожна з цих категорій осіб наділяється певним комплексом прав і свобод, які мають бути гарантованими.

Так, право бути поінформованим є необхідною умовою для реалізації інших прав, таких як право запитувати доступ до збережених даних, право вимагати їх видалення або виправлення і право подати скаргу до наглядового органу та отримати ефективний засіб правового захисту. З огляду на право бути поінформованим, особи, які відстежуються за допомогою FRT, повинні бути попереджені про використання FRT і конкретні місця, де розташовані камери. Якщо це неможливо – наприклад, через таємницю, необхідну для деяких кримінальних розслідувань – особи повинні бути проінформовані постфактум. Щоб захистити поточні розслідування, слід запровадити механізми обмеження права на отримання інформації в певних ситуаціях, оскільки правоохоронним органам іноді доводиться розвивати свою роботу в таємниці, щоб зберегти кримінальні докази [145].

Наприклад, законодавство ЄС містить підстави і критерії обмеження щодо біометричної ідентифікації в режимі реального часу в громадських місцях. Так, згідно з Директивою (ЄС) 2016/680 Європейського Парламенту та Ради від 27 квітня 2016 року [146] (див. також статтю 5/1 GDPR), органи влади зобов'язані інформувати громадян про те, що вони підпадають під FRT і про пов'язані з цим ризики [143]. Українське законодавство, в свою чергу, встановлює підстави обробки персональних даних без згоди суб'єкта персональних даних лише як виключення з загального правила без конкретизації умов і обґрунтованості таких дій.

Вважаємо, що необхідність застосування технології FRT має бути винятком, дозволеним за суворими вимогами. Такі вимоги повинні включати попередню оцінку ймовірності та серйозності шкоди громадянам та можливих наслідків використання FRT для прав і свобод громадян; суворе дотримання принципів необхідності та пропорційності; та попередній дозвіл, наданий судовим органом або компетентним адміністративним органом держави. Отже, має бути прописана процедура надання дозволу на обробку персональних даних людини за допомогою технології FRT. З огляду на те, що пошук може здійснюватися як за давні злочини так і по «гарячих слідах», процедура надання дозволу, звісно, має передбачати прискорений режим.

Ще одним важливим питанням в сфері застосування технології FRT правоохоронними органами є с*ертифікація і стандартизація протоколів ШІ*, які використовуються при відео-ідентифікації особи. Незважаючи на те, що це більше технічне питання, ніж юридичне, нормативний акт про використання FRT у правоохоронних органах має встановити певний стандарт (критерій) точності. Необхідно пам'ятати, що помилки, які виникли через недостатню точність результатів роботи системи, загрожують правовими наслідками для всіх учасників цієї процедури. Так, помилки FRT можуть призвести до хибних опрацювань даних (наприклад, помилкові збіги, коли людину помилково ідентифіковано як розшукувану особу, як-от неточне розміщення в списку спостереження) і хибно-негативних результатів (наприклад, особу не виявляють,

навіть якщо вона перебуває на записах спостереження). Рівень достовірності зіставлення зображень має вирішальне значення для правоохоронних органів. Помилка в ідентифікації злочинця може призвести до таких наслідків, як затримання (що у випадку помилкової ідентифікації було б незаконним) і публічне розкриття особи, що призвело б до соціальної дискредитації та шкоди репутації [147]. Точність безпосередньо залежить від використовуваної техніки, яка має бути сучасною та точності алгоритму, яка вимірюється за кількістю помилкових спрацьовувань і помилково негативних результатів. З цього випливає необхідність залучення фахівців, для вироблення відповідних технічних стандартів ШІ, а також органу, що визначає відповідність певної розробки заданим стандартам і рекомендує її до використання правоохоронними органами.

Дотримання права людини на рівність, неупередженість і недискримінацію під час обробки даних відеоспостереження за допомогою алгоритмів штучного інтелекту залежить від якості відповідного машинного навчання. У FRT дані – це зображення, які використовуються для навчання алгоритму, і вони мають бути різноманітними та якісними. FRT «навчений» розпізнавати обличчя на основі набору їх зображень. Необхідно зазначити, що алгоритми технології розпізнавання облич ніколи не дають остаточних результатів (так чи ні), а лише ймовірні з відповідним відсотком вірогідності. Тобто програмне забезпечення ніколи не може визначити, що два шаблони належать одній особі (тобто точні збіги), а лише те, наскільки ймовірно, що вони належать одній особі. Порівнявши шаблони, програмне забезпечення може вказати рівень ймовірності того, що два шаблони збігаються. Перевищення порогу, встановленого раніше системою, підтвердить відповідність. Ці ймовірності залежать від того, наскільки точним є програмне забезпечення. Отже великого значення для машинного навчання відіграють дані, на основі яких навчають алгоритм. Таким чином, надмірне чи недостатнє представлення в системі окремих категорій і груп населення (за расовою, етнічною, віковою належністю), може призводити до «перекосів» і некоректної роботі технології, а також до можливих упереджених результатів у висновках, отриманих в результаті використання неповних та/або помилкових

даних. Також має значення якість зображень які використовуються для тренувань, і періодичність їх оновлення, а також місце розташування камери спостереження. Так, у своїй роботі Д. Харвелл пише що у контрольованому середовищі, в якому особа перебуває в певному місці та під належним освітленням для «впізнання», наприклад у поліцейській дільниці чи аеропорту, зазвичай використовується ідентифікація постфактум. Навпаки, у неконтрольованому середовищі (громадські або публічні місця) часто використовуються випадкові зображення з камер відеоспостереження, особливо зображення людей, що проходять вулицею, і спостереження відбувається в режимі реального часу [148]. Таким чином, кількість помилок системи може різнитися від наявності різних факторів, що впливають на результати її роботи. На думку науковця, закон має встановити різні правові наслідки для цих двох типів збігу, наприклад, вимагаючи додаткових методів ідентифікації для останніх, а саме, інших форм біометричної ідентифікації (відбитки пальців, ДНК) – до того, як будуть вжиті будь-які заходи поліції щодо цієї особи.

З огляду на все вищесказане, величезного значення набуває механізм людського контролю за результатами роботи технології FRT. Питання юридичної сили результатів і висновків, згенерованих технологіями ШІ на підставі аналізу зібраних або введених в систему даних потребують особливої уваги і ретельного вивчення. Для того щоб відповісти на питання чи може бути такий результат прийнятий до розгляду державним органом влади, судом чи правоохоронним органом і вважатися чи доказом в судовому провадженні, чи підставою для прийняття відповідних рішень, чи юридичним фактом, що породжує правові наслідки, необхідно законодавчо прописати підстави і процедуру отримання таких результатів. Чи може висновок, згенерований ШІ мати юридичні наслідки і використовуватись в діяльності правоохоронців як факт, що не потребує додаткової процедури перевірки, чи необхідне втручання і контроль людини для надання йому юридичної сили? Ці питання поки не знайшли свого відображення у вітчизняному законодавстві. В свою чергу законодавство ЄС в статті 22 GDPR і статті 11 Директиви «Про правоохоронну діяльність» загалом забороняє

автоматизоване прийняття рішень, тобто будь-яке «рішення, засноване виключно на автоматизованій обробці, включаючи профілювання, яке створює юридичні наслідки щодо нього чи неї або подібним чином істотно впливає на нього чи неї. Крім випадків, коли це дозволено законодавством ЄС або держави-члена, яке передбачає відповідні гарантії прав і свобод суб'єкта даних та право на людське втручання з боку контролера». Таким чином, європейське законодавство йде по шляху обов'язкового контролю з боку людини за результатами роботи технології. Як зазначає Агентство Європейського Союзу з основоположних прав: «…концепція «автоматизованого» прийняття рішень потребує подальшого обговорення і дослідження. Наприклад, у деяких випадках втручання людини може полягати в тому, щоб просто «підписати» всі результати системи, отже, роблячи її практично автоматизованою. На противагу цьому можуть бути випадки упередженості коли люди переглядають і потенційно перекривають результати системи. Дослідження показують, що людина скасовує результати алгоритмів, головним чином тоді, коли її результат не узгоджується зі власними стереотипами (наприклад, знову ставить групи меншин у невигідне становище). Ця поведінка загрожує принципам рівності, неупередженості і додає цінності автоматизованій обробки через те, що вона може бути точнішою або, а іноді навіть справедливішою, ніж оцінка людей» [147].

Отже, європейські інституції наполягають на тому що: «позитивний результат не може призвести до автоматичного арешту, заснованого виключно на технології (Консультативний комітет Конвенції про захист осіб щодо автоматизованої обробки персональних даних, 2021). Будь-який потенційний збіг повинен бути згодом підтверджений людиною-оператором, щоб запобігти помилковим спрацьовуванням (Інститут IJIS та Міжнародна асоціація начальників поліції, 2019 (див. розділ про точність FRT)). Втручання людини має бути автономною оцінкою, а не сліпим підтвердженням результатів, наданих програмним забезпеченням» [145].

З огляду на те, що застосування правоохоронцями відеоспостереження завжди є втручанням в основні права людини (на конфіденційність особистого

життя, свободу, рівність), вважаємо, що у законі має бути чітко прописана відповідальність правоохоронних органів у сфері використання технологій FRT. «Для того, щоб громадяни прийняли певні форми стеження та погодилися на нього, держава повинна нести відповідальність за наслідки своїх дій» [149]. Слід запровадити механізм стримувань і противаги щодо використання FRT. Такий механізм може, наприклад, вимагати обов'язкового схвалення перед запровадженням особливо складних процесів розпізнавання обличчя (таких як загальне спостереження в громадських місцях) проходження сертифікації розробниками, а потім і постійного моніторингу. В законодавстві має бути передбачена юридична відповідальність як розробників технології за порушення, наприклад, технічних регламентів або процедури тестування, впровадження, легалізації відповідного програмного продукту, так і правоохоронних органів за неправомірне або надмірне використання технології FRT.

Також, у законодавстві має бути чітко вказано, як довго зберігатиметься зображення особи, зібране і оброблене за допомогою технології FRT. На наш погляд, при визначенні максимального періоду зберігання слід враховувати принципи необхідності та пропорційності відповідно до їх тлумачення, а також положень ст.6 Закону України «Про захист персональних даних»: «п. 5. Обробка персональних даних здійснюється для конкретних і законних цілей, визначених за згодою суб'єкта персональних даних, або у випадках, передбачених законами України, у порядку, встановленому законодавством. (…) п. 8. Персональні дані обробляються у формі, що допускає ідентифікацію фізичної особи, якої вони стосуються, не довше, ніж це необхідно для законних цілей, у яких вони збиралися або надалі оброблялися». Як вбачається з викладеного вище, Закон не визначає конкретних строків обробки (зберігання) даних. Так само, Законом безпосередньо не визначається «строк чинності згоди на обробку даних». Разом з тим, відповідно до статті 6 Закону персональні дані обробляються не довше, ніж це необхідно для законних цілей, у яких вони збиралися або надалі оброблялися. Крім того, у разі обробки даних на підставі згоди, суб'єкт даних

може її відкликати. У такому разі, подальша обробка даних може провадитися лише за наявності інших підстав обробки даних (визначених у статті 11 Закону) та виключно у межах, обумовлених такими підставами.

Таким чином, в Законі України «Про захист персональних даних» можна встановити різні терміни збереження зображення, отриманого внаслідок відеоспостереження для різних категорій осіб і цілей. Визначення періоду зберігання повинно враховувати типи зацікавлених осіб та отримані результати, оскільки виявлені збіги зображень різних типів суб'єктів даних (зниклі без вісті, жертви злочинів, злочинці, підозрювані у скоєнні злочинів особи тощо) можуть призвести до різних рішень щодо них.

Сьогодні в Європі є вже десятки документів, направлені на регулювання питань, пов'язаних зі штучним інтелектом і окремими його технологіями, такими як FRT. В Україні, на жаль, діє тільки один спеціальний нормативний акт в цій сфері – «Концепція розвитку штучного інтелекту в Україні», що є недостатнім для розвитку і правомірного впровадження і застосування технологій ШІ у правоохоронній діяльності.

На наш погляд, чинне законодавство потребує доповнення правовими нормами щодо сфери застосування технології FRT або прийняття спеціального нормативного акту щодо впровадження і застосування технологій ШІ, окремим розділом якого має стати впровадження технології FRT в правоохоронну діяльність.

3. Актуальність інструменту використання **документів, створених або згенерованих за допомогою штучного інтелекту,** в діяльності правоохоронних органів обумовлена тим фактом, що у сучасній правовій практиці та діяльності правоохоронних органів спостерігається значне збільшення обсягів інформації, яку необхідно опрацьовувати для забезпечення ефективного здійснення правосуддя та попередження злочинності. Аналізуючи дані з різних джерел, системи штучного інтелекту здатні виявляти закономірності, що можуть передбачати або пояснювати злочинну поведінку. Використання таких технологій у професійній діяльності юристів і правоохоронців спрямоване на

оптимізацію процесів обробки інформації, автоматизацію рутинних завдань та підвищення оперативності прийняття рішень.

Сучасні програмні продукти на основі ШІ дозволяють автоматизовано генерувати стенограми допитів свідків, потерпілих і підозрюваних, а також здійснювати аналітичну обробку звітів і документів, виділяючи ключові юридичні відомості. Це створює умови для більш ефективної підготовки матеріалів до суду, скорочує часові витрати на обробку великих обсягів інформації та забезпечує точність і системність документування.

Ураховуючи зазначене, актуальним є питання з'ясування правової природи, статусу та допустимості використання документів, створених або згенерованих із застосуванням ШІ, адже їхня технологічна специфіка може впливати на процедури фіксації фактів, оцінку доказів та юридичну відповідальність. Розгляд цього питання є необхідним для формування науково обґрунтованих підходів до регулювання застосування ШІ в правоохоронній і судовій практиці.

На нашу думку, ключовим аргументом на користь еквівалентності документів, створених із застосуванням систем штучного інтелекту (ШІ), та традиційних офіційних документів є їх спільна правова природа, функціональне призначення і процедурні засади створення. Обидва види документів мають на меті фіксацію юридично значущих фактів, які породжують, змінюють або припиняють певні правовідносини. Використання ШІ у цьому процесі не трансформує його сутності, а лише модернізує техніко-організаційний аспект документообігу, підвищуючи ефективність, точність і швидкість обробки даних. Таким чином, штучно-інтелектуальні системи виступають не заміною людського суб’єкта, а інструментом підвищення раціональності управлінських і правоохоронних процедур, що узгоджується з принципами належного урядування та цифрової трансформації публічного сектору.

У цьому контексті актуалізується питання визначення правового статусу документів, створених або модифікованих за допомогою алгоритмічних технологій, а також їх юридичної сили та допустимості як доказів у процесуальній діяльності правоохоронних органів. Зарубіжні дослідники

(A. Etzioni, R. Calo, F. Pasquale та ін.) пропонують розглядати такі документи як нову категорію правової інформації – «algorithmically generated legal documents», що потребує окремого нормативного врегулювання, з урахуванням принципів прозорості, верифікованості та підконтрольності людині.

Так, американський фахівець Philip Lukens пропонує впровадити нову термінологію для матеріалів, створених із використанням технологій ШІ, зокрема на основі записів натільних камер поліцейських. На його думку, такі матеріали слід позначати як *«транскрипцію сцени»* (*scene transcription*) – тобто достовірний, дослівний запис мови та звуків, зафіксованих технічним засобом, без будь-якої інтерпретації, аналітичної оцінки чи суб'єктивних суджень. Використання цього поняття, на думку вченого, дозволить уникнути плутанини між традиційними звітами, що містять аналітичну інтерпретацію, та інформацією, автоматично згенерованою штучним інтелектом [150].

Поступово у науковому дискурсі формується підхід, згідно з яким інформація, створена технічними засобами, що працюють у режимі автономності або з використанням алгоритмів штучного інтелекту, має отримати специфічний правовий статус. Це необхідно для забезпечення належного рівня достовірності, допустимості та правової визначеності таких даних у діяльності правоохоронних органів.

Вважаємо слушною пропозицію щодо виокремлення документів, згенерованих штучним інтелектом, в окрему категорію, оскільки кожен офіційний документ традиційно має свого автора (виконавця) – фізичну особу, яка несе юридичну відповідальність за його зміст і форму. Натомість документ, створений автономною системою, позбавлений такого суб'єкта, що актуалізує проблему визначення правових наслідків його створення, обігу та використання. Відповідно, необхідним є нормативне врегулювання статусу таких документів у національному законодавстві.

З огляду на це, доцільним є проведення класифікації документів, створених із використанням ШІ, за критерієм ступеня автономності системи у процесі їх формування:

1. Документи першої групи (автоматизовані або відтворювальні). Це документи, які можуть використовуватись у тому вигляді, в якому вони були згенеровані системою. Йдеться про інформаційні продукти, що формуються на основі офіційних джерел, державних реєстрів чи баз даних – наприклад, довідки, статистичні звіти, витяги з реєстрів або копії документів. У цьому випадку штучний інтелект виконує допоміжну функцію: він здійснює пошук, систематизацію та форматування інформації без зміни її змісту. За своєю формою і змістом отриманий документ нічим не відрізняється від документа, складеного людиною-посадовою особою відповідного державного органу, і може за своїм статусом прирівнюватись до електронного документу, визначеному Законом України «Про електронні документи та електронний документообіг» [151]. Такі матеріали можуть визнаватися документами «прямої дії», адже вони містять достовірні відомості з офіційно перевірених джерел і можуть бути використані у цивільних, адміністративних чи кримінальних провадженнях без додаткової експертизи.

2. Документи другої групи (аналітичні або когнітивні). Ця категорія охоплює документи, які створюються шляхом аналітичної, когнітивної чи прогностичної обробки даних. Прикладами є аналітичні звіти, ідентифікаційні профілі, результати відеоаналітики, патерн-розпізнавання або прогнози криміногенної ситуації. Такі документи мають інтелектуально-похідний характер, оскільки результат формується внаслідок алгоритмічного аналізу та узагальнення даних, отриманих з різних джерел – як офіційних, так і публічних (ЗМІ, соціальні мережі, відкриті бази даних). У цьому випадку технології машинного навчання функціонують частково автономно, моделюючи процеси людського мислення, що потребує обов’язкової перевірки (верифікації) результатів людиною.

З огляду на певну автономність і квазісуб’єктність ШІ у процесі генерування інформації, принцип обов’язкової людської перевірки має бути закріплений на законодавчому рівні. Цей принцип є ключовим у Рекомендаціях Ради Європи щодо етичних аспектів використання ШІ в правосудді [152], де наголошено, що будь-яке застосування автоматизованих систем у сфері правозастосування має

гарантувати збереження людської відповідальності, нагляду та можливості перегляду рішень. Аналогічний підхід закріплено у статті 14 Європейського акту про штучний інтелект [153], яка передбачає, що системи високого ризику, до яких належать правоохоронні алгоритми, можуть використовуватись лише за умови «належного людського контролю, який забезпечує зрозумілість і відтворюваність результатів». Це положення відповідає вимогам щодо запобігання маніпуляціям і забезпечення підзвітності суб'єктів, які використовують автоматизовані системи.

Отже, юридична сила таких документів повинна бути похідною від рішення уповноваженої посадової особи, яка засвідчує їх достовірність.

Оскільки документи, створені автономними алгоритмічними системами, не мають автора у класичному праворозумінні, виникає необхідність нормативного визначення суб'єкта юридичної відповідальності за їх створення, перевірку і використання. Таким суб'єктом може бути оператор, адміністратор або орган, який експлуатує систему, адже саме він приймає кінцеве рішення щодо використання отриманих результатів.

У контексті кримінального процесуального права така позиція узгоджується з положеннями статей 84 та 99 Кримінального процесуального кодексу України [154], які визначають вимоги до доказів і документів як їх джерел. Документ, створений із застосуванням ШІ, може бути визнаний доказом лише за умови, що він отриманий у передбаченому законом порядку та містить достовірні дані, підтверджені компетентною особою.

Крім того, аналітичні документи, створені за допомогою ШІ, мають містити відомості про алгоритм формування результатів, рівень похибки, а також межі достовірності висновків, якщо вони ґрунтуються на імовірнісних або прогнозних методах. Така вимога випливає із принципу надійності та обґрунтованості доказової інформації, який має конституційне підґрунтя у ст. 62 Конституції України (презумпція невинуватості).

Відповідно, в рамках національного законодавства повинна бути визначена посадова особа, яка здійснює контроль за достовірністю документів,

згенерованих ШІ, та ухвалює рішення про їхнє використання в офіційних цілях. Вона повинна засвідчувати достовірність, повноту та відповідність таких документів нормативним вимогам.

Крім того, доцільно законодавчо встановити обов'язкове маркування документів, створених або оброблених із застосуванням технологій ШІ. Це узгоджується з положеннями міжнародного документу «Керівні принципи щодо штучного інтелекту» Ради Організації економічного співробітництва та розвитку (ОЕСР), згідно з якими користувачі повинні бути поінформовані, коли взаємодіють із системами штучного інтелекту, а інформаційні продукти таких систем мають бути ідентифіковані й відокремлені від людських результатів [155].

Маркування є особливо важливим у випадках, коли системи машинного навчання здатні імітувати когнітивні й комунікативні особливості людини, через що створені ними документи (звіти, аналітичні огляди, інтерпретації тощо) можуть бути майже невідрізними від людських. Наприклад, підготовка звіту вимагає аналітичного осмислення, критичного мислення, оцінки та узагальнення фактів, що притаманно людині, але не машині. Тому використання таких матеріалів у діяльності правоохоронних органів можливе лише після перевірки їх змісту на відповідність фактам та правовим критеріям, із зазначенням відповідальної особи, що підтвердила достовірність даних.

Таким чином, запровадження чіткої системи контролю, маркування та юридичного визнання документів, створених із використанням ШІ, сприятиме забезпеченню принципів законності, прозорості, підзвітності та надійності, передбачених як міжнародними актами, так і національною правовою системою України.

Однією із сучасних технологій, яка допомагає правоохоронцям створити документ, є *ШІ-транскрипція* – це автоматизований процес перетворення аудіо- чи відеозаписів у письмовий текст за допомогою алгоритмів штучного інтелекту. ШІ-транскрипція являє собою значний крок вперед у здатності технології подолати розрив між усною мовою та письмовим текстом. Її сутність полягає в автоматизованому перетворенні аудіо- та відеозаписів у текстовий формат

шляхом аналізу усного мовлення та створення точного письмового відтворення змісту. Такі системи функціонують на основі моделей машинного навчання, які навчаються на великих масивах даних, зокрема аудіозаписах, що дозволяє розпізнавати мовні шаблони, словникові конструкції та граматичні закономірності [156].

Застосовуючи технології автоматичного розпізнавання мовлення (ASR), ШІ-транскриптори здатні точно передавати зміст сказаного, фіксуючи не лише слова, а й контекст їх уживання. На відміну від традиційних поліцейських звітів, транскрипція не передбачає інтерпретації чи суб'єктивного аналізу, а спрямована на максимально точне відтворення оригінального висловлювання. У поєднанні з методами обробки природної мови (NLP) такі системи забезпечують граматичну правильність, розуміння змісту фраз і передавання мовних відтінків.

У правоохоронній діяльності застосування технологій штучного інтелекту для транскрипції аудіо- та відеоматеріалів відкриває нові можливості для оптимізації процесів документування слідчих дій, зокрема допитів, показань і доказів. Використання ШІ-транскрипції дозволяє автоматизувати створення стенограм, що, у свою чергу, суттєво прискорює роботу секретаріату, підвищує точність процесу фіксації інформації та забезпечує ефективний пошук у базах даних. Для правоохоронців це створює умови для більш ґрунтовного аналізу матеріалів справ, формування аргументаційної бази та підвищення якості адміністративного й кримінального провадження.

В Україні ця технологія офіційно застосовується у сфері здійснення правосуддя. Так, у «Концепції єдиної судової інформаційно-телекомунікаційної системи», затвердженій наказом Державної судової адміністрації України № 178 від 30 квітня 2025 року, передбачено застосування ШІ для автоматичного створення стенограм судових засідань і перетворення мовлення в текст на запит користувача, а також генерації проектів рішень [157].

Отже, правоохоронні органи можуть ефективно застосовувати ШІ-транскрипцію під час допитів, аналізу свідчень або відтворення записів із місця події, що сприяє збереженню доказової бази та підвищенню якості розслідувань.

У зарубіжній літературі розрізняють типи ШІ-транскрипції: повністю автоматизована та ШІ-транскрипція за допомогою людини [158], [159]. Повністю автоматизована транскрипція штучного інтелекту передбачає транскрибування аудіо- та відеовмісту за допомогою передових технологій розпізнавання мовлення та обробки природної мови без втручання людини. Цей тип транскрипції є повністю автоматизованим і забезпечує швидкий час виконання. Він підходить для ситуацій, коли швидкість і ефективність є вирішальними, наприклад, для обробки великих аудіо- чи відеозаписів. Транскрипція штучного інтелекту за допомогою людини поєднує потужність технологій ШІ з досвідом людини. У цьому підході системи ШІ генерують початкові транскрипції, які люди-транскриптори потім переглядають і редагують. Допомога людини допомагає підвищити точність і якість транскрипції, особливо у випадках, коли вміст складний, вимагає знань у певній області або має складні звукові умови. ШІ-транскрипція за допомогою людини забезпечує вищу точність і може бути адаптована до конкретних вимог [158]. Таким чином, ШІ-транскрипція в правоохоронній сфері – це процес автоматизованого перетворення усного аудіо- та відеоконтенту, отриманого в ході слідчих дій, допитів свідків або потерпілих, у письмову форму за допомогою алгоритмів штучного інтелекту, при якому зберігається точність і зміст оригінальних висловлювань, без їх інтерпретації або оцінки, з метою забезпечення оперативного, системного та об’єктивного документування інформації для використання в досудовому та судовому провадженні.

Це технологічний прогрес, який використовує потужність штучного інтелекту, зокрема машинне навчання та методи обробки природної мови, для точної та ефективної транскрипції усного вмісту. Звісно, впровадження такої технології в роботу державного органу потребує вироблення чітких критеріїв і стандартів, а також сертифікації відповідного програмного забезпечення. При використанні ШІ-транскрипції, необхідно робити відповідну відмітку на такому документі, щоб відрізняти його від документів, створених людиною. Така відмітка надає можливість:

– уникнути помилкового враження, що документи ШІ є офіційною точкою зору поліцейського, слідчого чи експерта;

– підкреслити, що документи є результатом обробки джерел інформації, а не аналізом або думкою посадових осіб, і потребують додаткової перевірки;

– спонукати правоохоронців редагувати та доповнювати ШІ-документи власними спостереженнями, аналізом та вказувати джерела;

– визнати обмеження ШІ (помилки розпізнавання мови та зображень, шум, діалекти, сленг), що стимулює покращення системи та її точності.

Отже, для забезпечення юридичної визначеності у сфері використання ШІ в правоохоронній діяльності вітчизняне законодавство має бути доповнено нормами, що визначають правовий статус документів, згенерованих штучним інтелектом, і матеріалів, отриманих за допомогою ШІ, а саме:

– нормативне закріплення класифікації документів, створених із застосуванням ШІ;

– встановлення чітких критеріїв їх юридичної сили та допустимості у процесуальних відносинах;

– визначення суб’єкта відповідальності за перевірку, засвідчення й використання таких документів;

– упровадження механізмів контролю достовірності, маркування та аудиту алгоритмічних систем, що формують інформаційні матеріали, які мають юридичне значення.

2.2 Мережа Інтернет в інформаційно-аналітичній діяльності правоохоронного органу

Глобальне Інтернет-середовище розвивається «зі швидкістю думки», даруючи Інтернет-спільноті все нові й нові можливості спілкування. З огляду на те, що чисельність інтернет-користувачів у світовій спільноті зростає за експонентою, можна стверджувати, що людство загалом дедалі більше занурюється в інформаційно-комунікаційні глибини. Інтернет є конденсованим

вираженням глобального полікультурного соціуму в добу глобальної комунікації, яка продукує і транслює нові або оновлені смисли надшвидкими темпами [160]. Інтернет-середовище є майже стовідсотковим відображенням суспільного і приватного життя сучасної людини. Економіка, фінанси, комерція, освіта, культура, дозвілля, торгівля, державні послуги – це не повний перелік відносин, які відбуваються у мережі Інтернет, або за її допомогою. Сфери, які не мають свого «втілення» в цифровому вигляді можна перерахувати на пальцях. На жаль, як і в матеріальному світі, разом з можливостями і благами, які отримали люди з появою цієї мережі, з'явилися і відповідні загрози, пов'язані з порушеннями встановлених правил і норм. Таким чином, правове регулювання функціонування мережі Інтернет, а також правових відносин, які відбуваються за її допомогою, є вже давно предметом уваги законодавців як національних урядів, так і міжнародних інституцій.

Відповідно до Закону України «Про електронні комунікації»: «мережа Інтернет (Інтернет) – глобальна електронна комунікаційна мережа, що призначена для передачі даних та складається з фізично та логічно взаємоз'єднаних окремих електронних комунікаційних мереж, взаємодія яких базується на використанні єдиного адресного простору та на використанні інтернет-протоколів, визначених міжнародними стандартами».

Інтернет і трансформована ним злочинна діяльність (кіберзлочинність) становлять серйозний виклик для правоохоронних органів і підтримки правопорядку, оскільки правопорушення, скоєні за допомогою мережі Інтернет, мають глобальний характер, тоді як кримінальне законодавство здебільшого обмежене національними рамками. Для підтримки інформаційно-аналітичної діяльності правоохоронних органів, в їх структурі в різні часи було створено різноманітні підрозділи і служби. Так, в 2015 році в структурі Національної поліції України було створено Департамент інформаційного забезпечення та координації діяльності поліції «102», який організовував і реалізовував передбачені законодавством України заходи, спрямовані на інформаційно-аналітичне та інформаційно-пошукове забезпечення правоохоронної діяльності і

захист персональних даних при їх обробці в структурних підрозділах Національної поліції України. Пізніше його було реорганізовано в Департамент інформаційно-аналітичної підтримки, основними напрямами якого стало: забезпечення інформаційно-пошукової та інформаційно-аналітичної роботи; участь у розробці проєктів нормативно-правових актів Міністерства внутрішніх справ з питань, що належать до компетенції поліції і пов'язаних з інформаційно-аналітичним забезпеченням, а також оброблення персональних даних в органах і підрозділах поліції. Згідно звіту Національної поліції України про результати роботи у 2024 році, лінією екстреного виклику «102» опрацьовано майже 7,5 млн викликів (у 2023 році – 6,8 млн) [139].

В тому ж 2015 році прийнято Закон України «Про Національну поліцію», де в статті 26 визначено вичерпний перелік реєстрів та баз (банків) даних, що входять до Єдиної інформаційної системи МВС, які поліція наповнює та підтримує в актуальному стані засобами інформаційно-комунікаційної системи.

У наступні роки нормативно-правове забезпечення використання можливостей інформаційної підтримки правоохоронних органів значно покращилося. Так, у 2017 році було затверджено Положення про інформаційно-комунікаційну систему «Інформаційний портал Національної поліції України» та Положення про систему Інтернет у телекомунікаційній мережі Національної поліції України. Наступного року прийнято Положення про єдину інформаційну систему Міністерства внутрішніх справ. У 2020 році прийнято спільний Наказ Міністерства внутрішніх справ України, Офісу Генерального прокурора, Національного антикорупційного бюро України, Служби безпеки України, Державного бюро розслідувань, Міністерства фінансів України, Міністерства юстиції України «Про затвердження Інструкції про порядок використання правоохоронними органами України інформаційної системи Міжнародної організації кримінальної поліції – Інтерпол, зареєстрований в Міністерстві юстиції України», зареєстрований в Міністерстві юстиції України 04 вересня 2020 р. за № 849/35132.

В діяльності правоохоронних органів, мережа Інтернет виконує подвійну функцію, поєднуючи оперативно-розшукові та організаційно-комунікативні аспекти. Його роль у забезпеченні правопорядку та реалізації правоохоронної функції держави постійно зростає у зв'язку з цифровізацією суспільних відносин і зростанням обсягів інформаційних потоків. З одного боку, Інтернет є важливим джерелом доказової та аналітичної інформації, що сприяє розкриттю і розслідуванню злочинів. Використання цифрових даних, отриманих із відкритих джерел, платформ соціальних мереж або мережевої активності, дозволяє слідчим формувати доказову базу, оптимізувати оперативно-розшукові заходи та підвищувати ефективність криміналістичних досліджень.

З іншого боку, мережа виступає інструментом організаційно-управлінської діяльності правоохоронних органів, забезпечуючи комунікацію з громадськістю, надання адміністративних послуг у цифровій формі та інформування населення про результати діяльності поліції. Через офіційні вебпортали та соціальні медіа державні органи можуть здійснювати превентивну діяльність, підвищувати довіру громадян і забезпечувати прозорість у сфері публічної безпеки.

Реалізовуючи свої професійні функції, правоохоронні органи, як і будь-який орган владних повноважень, відповідно до Закону України «Про доступ до публічної інформації» зобов'язані інформувати суспільство про свою діяльність. Такий доступ, згідно з Законом, забезпечується шляхом:

1) систематичного та оперативного оприлюднення інформації: в офіційних друкованих виданнях; на офіційних веб-сайтах в мережі Інтернет; на єдиному державному веб-порталі відкритих даних; на інформаційних стендах; будь-яким іншим способом;

2) надання інформації за запитами на інформацію.

Конкретизація норм згаданого Закону відбувається в таких підзаконних актах, як: Указ Президента України від 05 травня 2011 року № 547 «Питання забезпечення органами виконавчої влади доступу до публічної інформації»; Наказ Міністерства внутрішніх справ України «Про Порядок прийому, реєстрації і розгляду запитів на публічну інформацію, розпорядником якої є Національна

поліція України, та відшкодування запитувачами фактичних витрат на копіювання і друк документів у Національній поліції України» від 07.02.2017 № 95; Наказ Міністерства внутрішніх справ «Про організацію роботи із запитами на публічну інформацію в Національній поліції України» від 07.02.2017 № 95.

Так, за даними, оприлюдненими на офіційних сайтах відповідних структур, загальна кількість отриманих запитів на інформацію в 2025 році Національною поліцією України склала 18339 штук; органами прокуратури – 12811. Загальна кількість звернень, що надійшли у 2024 році до ДБР – 48825 заяв/клопотань та 1655 інформаційних запитів. За 2024 рік співробітниками Приймальні СБУ опрацювали 976 (у 2023 – 858) запитів на інформацію, а саме: індивідуальних – 920 (у 2023 – 850); колективних – 56 (у 2023 – 8) [161]. (інформація за 2025 рік ДБР та СБУ поки відсутня).

Аналіз чинного законодавства, яке регулює доступ до публічної інформації, дозволяє стверджувати, що обов'язок правоохоронних органів інформувати суспільство про свою діяльність є невід'ємним елементом принципу відкритості та підзвітності державної влади. Відповідно до положень Закону України «Про доступ до публічної інформації», правоохоронні органи повинні функціонувати не лише як суб'єкти владних повноважень, а й як інститути публічної довіри, які забезпечують прозорість власної діяльності та створюють умови для громадського контролю за реалізацією своїх повноважень. У цьому контексті мережа Інтернет відіграє ключову роль у забезпеченні ефективної комунікації між державою та громадськістю. Вона виступає головним інструментом оперативного оприлюднення інформації, створює умови для електронної взаємодії між громадянами та правоохоронними органами, а також сприяє реалізації принципу публічності у діяльності органів влади. Так, ДБР на офіційному вебсайті у 2024 році опубліковано понад тисячу інформаційних повідомлень про діяльність Бюро [162]. Висвітлення діяльності органів прокуратури у 2025 році відбувалось шляхом надання інформації в органи влади, виступи в медіа, підготовлення програм, загальною кількістю 122 033 повідомлень [163].

Таким чином, інформування суспільства через Інтернет є не лише технічним засобом реалізації законодавчих вимог, а й важливим елементом демократичного управління, що забезпечує прозорість, довіру та підзвітність у системі публічної безпеки.

Що стосується використання мережі Інтернет як джерела інформації для здійснення аналітичної, пошукової, розвідувальної діяльності правоохоронним органом, то нормативно-правове регулювання тут стикається з певними труднощами і обмеженнями. Цифрове середовище представляє собою складне різнобарвне явище, а інтернет-відносини, в силу глобалізації, не завжди підпадають під дію національних норм.

В рамках цієї роботи ми зможемо розглянути лише окремі питання правового регулювання пошуку, накопичення, аналітики і використання інформації, розміщеної в мережі Інтернет в інтересах правоохоронних органів.

В епоху цифрової трансформації аналіз даних став незамінним інструментом у різних сферах, і правоохоронні органи не є винятком. Одним із таких інструментів є програмне забезпечення для аналізу посилань, яке відіграє ключову роль у виявленні прихованих зв’язків у поліцейських розслідуваннях. Аналіз зв’язків – це метод аналізу даних, який використовується для оцінки зв’язків (з’єднань) між вузлами. Ці вузли можуть представляти людей, організації або навіть події в контексті поліцейської діяльності. Відносини або зв’язки між вузлами представлені зв’язками. Програмне забезпечення для аналізу зв’язків забезпечує візуальне представлення даних, що полегшує виявлення зв’язків, які можуть бути не відразу помітними в необроблених даних

Програмне забезпечення для аналізу посилань прискорило проведення розслідувань правоохоронними органами, дозволяючи їм швидко аналізувати бази даних і виявляти взаємозв’язки між об’єктами, як-от місця, люди, події, транспортні засоби тощо. Так, за даними Департаменту кіберполіції Національної поліції України (ДКП) у 2024 році зареєстровано 50,2 тис. кримінальних правопорушень у сфері високих інформаційних технологій (далі –

кіберзлочини), зокрема у сфері телекомунікацій та протиправного контенту – 2,3 тис., що у 5,7 рази більше, ніж у 2023 році [164].

Слід зауважити, що за час дії воєнного стану зловмисники підлаштовувалися під тренди суспільства, тому набули поширення заволодіння коштами громадян під виглядом надання послуг з оформлення документів для чоловіків призовного віку, незаконного перетину кордону, шахрайства, пов'язані із продажем військового спорядження та наданням волонтерської допомоги, оренди квартир для внутрішньо переміщених осіб, їх перевезень в безпечні регіони. Окрема увага підрозділів ДКП була спрямовна на протидію найбільш поширеним різновидам шахрайств – дзвінкам від імені працівників банківських установ та фішингу. Треба зазначити, що більша половина від загальної кількості таких злочинів учинено шляхом незаконних операцій з використанням електронно-обчислювальної техніки (онлайн-шахрайства) – майже 35 тис. з 64,7 тис. У співпраці з фахівцями Національного банку України та Національного центру оперативно-технічного управління мережами телекомунікацій Адміністрації Держспецзв'язку у 2024 році обмежено доступ до майже 45 тис. доменних імен, які зловмисники масово використовували в протиправній діяльності, зокрема для створення фішингових посилань [139]. Підрозділи кіберполіції здійснюють постійний моніторинг національних електронних комунікаційних мереж та інформаційних ресурсів, аналіз вторгнень у ці мережі та ресурси, а також виявлення в режимі реального часу недоліків їх функціонування. Зокрема, для забезпечення захисту сервісів ДКП впроваджуються та використовуються сучасні програмно-технологічні рішення [164].

Департамент кібербезпеки СБУ з перших днів повномасштабної війни запровадив один із ключових інструментів протидії агресору – телеграм-бот @stop_russian_war_bot, через який громадяни передавали й продовжують передавати оперативні відомості про переміщення ворожих військ. У межах захисту інформаційного простору держави кіберфахівці СБУ за період повномасштабного вторгнення нейтралізували 9 829 кібератак і кіберінцидентів, блоковано спроби російського хакерського угруповання Sandworm проникнути в

українські військові мережі та організувати збір розвідданих. Виявлено десять ворожих шпигунських програм, також заблокували 80 ботоферм і численні антиукраїнські YouTube-канали, а також викрили та притягнули до відповідальності сотні інтернет-агітаторів, що поширювали ворожі фейки та пропагандистські наративи [165].

У сучасних умовах цифровізації дедалі частіше правоохоронні органи використовують розвідувальну інформацію, отриману з відкритих джерел, за допомогою таких технологій, як OSINT (Open Source Intelligence) та SOCMINT (Social Media Intelligence).

Пошук інформації і аналітика на основі відкритих OSINT являє собою технологію збору, обробки та аналізу військової, політичної, економічної чи іншої суспільно значущої інформації, яка є публічно доступною. Такий тип розвідки може застосовуватись будь-якою особою, що володіє відповідними технічними знаннями та програмними інструментами.

Разом із тим, у контексті правоохоронної діяльності використання OSINT передбачає підвищену правову відповідальність і дотримання принципів демократичної держави, зокрема гарантій додержання прав і свобод людини. Збір та обробка інформації навіть із відкритих джерел може за певних умов розглядатися як втручання в приватне життя особи, що вимагає правового обґрунтування та процесуальних гарантій.

Відповідна правова позиція закріплена у практиці Європейського суду з прав людини. Так, у справі *«С. Віберг проти Швеції»* (S. Wiberg v. Sweden, рішення від 6 червня 2006 р.) Суд визнав, що дії правоохоронних органів щодо збору інформації, доступної для користувачів мережі Інтернет, можуть бути кваліфіковані як порушення права на повагу до приватного і сімейного життя, гарантованого статтею 8 Конвенції про захист прав людини і основоположних свобод [166]. Це рішення підкреслює необхідність балансу між інтересами державної безпеки та захистом приватності особи, навіть у випадках, коли йдеться про публічно доступну інформацію.

З огляду на це, доцільним видається розмежування інструментів правоохоронного моніторингу на спеціальні технічні засоби, використання яких потребує нормативного регулювання, та загальнодоступні інструменти, застосування яких не порушує принципів приватності та інформаційної безпеки громадян. Збір персоніфікованих даних із відкритих джерел може бути допустимим лише в межах, визначених законом, і з виключною метою протидії злочинності. Такий підхід відповідає положенням статті 9 Закону України «Про оперативно-розшукову діяльність», якою встановлено загальну заборону на проведення оперативно-розшукових заходів без заведення оперативно-розшукової справи.

Важливою технологією збору та аналізу інформації в цифровому середовищі є SOCMINT (скорочено від *Social Media Intelligence*), що позначає розвідку на основі соціальних медіа. Ця технологія охоплює процеси збору, обробки та аналітичного опрацювання даних, розміщених у соціальних мережах, з метою забезпечення національної безпеки, підтримання громадського порядку та запобігання злочинності. SOCMINT передбачає моніторинг відкритого контенту соціальних медіа, включно з публікаціями, коментарями, мультимедійними матеріалами та поведінковими патернами користувачів, з метою формування аналітичних висновків, виявлення потенційних загроз, а також визначення соціальних і поведінкових тенденцій у цифровому просторі. У цьому контексті правоохоронні органи використовують SOCMINT як інструмент розслідування та попередження злочинів, що дозволяє підвищити ефективність оперативно-розшукової діяльності, встановлювати коло осіб, причетних до злочинних дій, та виявляти джерела деструктивної інформації.

Використання SOCMINT у правоохоронній діяльності ґрунтується на спеціалізованих програмних засобах, здатних здійснювати автоматизований збір, класифікацію та аналіз великомасштабних масивів даних із соціальних платформ (таких як X, Facebook, Instagram, Telegram тощо).

Так, на сайті поліції Києва у Фейсбуці, було опубліковано повідомлення щодо виявлення правопорушення, передбаченого ст. 184-3 КУпАП: «Порушення

правоохоронці виявили під час моніторингу мережі Інтернет. На оприлюдненому відео 28-річний користувач соцмереж, який має десятки тисяч підписників, вів стрім, будучи одягнутий в поліцейський однострій. Порушник, видаючи себе за співробітника кіберполіції, поводив себе зухвало та вживав нецензурну лексику. Працівники управління кримінального аналізу главку поліції встановили особу блогера та склали у відношенні правопорушника адміністративний матеріал за ч. 1 ст. 184-3 КУпАП - незаконне використання фізичною особою ознак належності до Національної поліції» [167].

Особливу увагу SOCMINT приділяє виявленню ознак радикалізації у віртуальних спільнотах, а також моніторингу потенційно небезпечних осіб або груп, які поширюють ідеї насильства, ненависті чи тероризму. Таким чином, SOCMINT є важливим елементом системи превентивного реагування на загрози у кіберпросторі, забезпечуючи можливість раннього виявлення деструктивних тенденцій та їх правової кваліфікації [168].

Так, Служба безпеки України викрила у Києві групу осіб, які «обслуговували» ботоферму, що поширювала антиукраїнський контент. Зловмисники управляли майже 6 тисячами ботів. Для підвищення рівня довіри зловмисники поширювали інформацію із «верифікованих акаунтів», використовуючи підроблені документи громадян України. Фальшивки давали службі підтримки Facebook для підтвердження «справжності особи». Потім «верифіковані» таким чином акаунти використовували для поширення публікацій та коментарів на замовлення третіх осіб. Здебільшого це контент, спрямований на посилення протестних настроїв в Україні, у тому числі антивакцинаторських. Заходи із викриття та документування протиправної діяльності здійснювали співробітники ГУ СБУ у м. Києві та Київській області за процесуального керівництва Святошинської окружної прокуратури [169].

Отже, правоохоронний моніторинг соціальних мереж набуває дедалі більшого значення в умовах цифровізації суспільних відносин. Водночас у сучасній правовій доктрині та нормативно-правовій базі України ця категорія перебуває на етапі теоретичного осмислення і не має чіткого юридичного

закріплення. Правоохоронний моніторинг соціальних мереж розглядається науковцями як інноваційний напрям діяльності державних органів, що підлягає нормативному оформленню у вигляді спеціального правового інституту, спрямованого на реалізацію правоохоронної функції держави в інформаційному середовищі [170].

Потреба у формуванні правових засад такого моніторингу зумовлює необхідність визначення кола суб'єктів, уповноважених на його здійснення, а також закріплення їхніх прав, обов'язків і меж компетенції. Саме відповідні структурні підрозділи державних органів повинні виступати носіями владних повноважень щодо проведення моніторингу, що зумовлює потребу у чіткій правовій регламентації їхньої діяльності.

Так, В. Д. Гавловський вважає, що «суб'єктами правоохоронного моніторингу можуть бути лише ті органи, що мають повноваження здійснювати пошук інформації про протиправні діяння певних осіб і груп, уповноважені збирати конфіденційну інформацію про особу без її згоди. Тому правоохоронний моніторинг потрібно зарахувати до компетенції лише тих правоохоронних органів, підрозділи яких уповноважені провадити оперативно-розшукову діяльність та (або) негласні слідчі дії. У системі МВС України здійснення правоохоронного моніторингу необхідно покласти на оперативні підрозділи, а в подальшому – на єдину розвідувальну поліцейську структуру, до повноважень якої слід віднести візуальне спостереження, оперативну установку, оперативно-технічні заходи, аналітичну розвідку та профілактичний пошук. Профілактично-пошукові заходи такої структури здійснюватимуться не лише на певних територіях, а у соціальних мережах та у Інтернеті загалом» [171, с. 24].

Визначення суб'єктами правоохоронного моніторингу оперативних підрозділів МВС та СБУ викликає необхідність конкретизації їх прав і обов'язків у цій сфері, а також закріплення організаційно-правових засад такої діяльності.

Вітчизняні і зарубіжні науковці зазначають, що: «відсутність законодавчої бази, що регулює використання поліцією соціальних мереж, залишає правоохоронні органи без достатньої інформації про їхні права та обов'язки. Їм

доводиться користуватися нормативними актами, створеними для офлайн-діяльності, і застосовувати їх у контексті онлайн-розслідувань. Крім того, оскільки не існує стандартизованих методів збору даних в Інтернеті, органи влади часто застосовують різні підходи та різні інструменти, що може призвести до розбіжностей. Обсяг інформації, доступної на платформах соціальних мереж, також є значною проблемою, оскільки поліцейські підрозділи не мають достатньої кількості персоналу для аналізу величезних обсягів даних, які вони надають [172].

На наш погляд, правовою основою моніторингу соціальних медіа з боку правоохоронних органів, можна вважати наступні нормативні акти: Закон України «Про Національну поліцію», де в ст. 40 «Застосування технічних приладів, технічних засобів та спеціалізованого програмного забезпечення» передбачена можливість поліції застосовувати спеціалізоване програмне забезпечення для здійснення аналітичної обробки фото- і відеоінформації для виконання покладених на неї завдань та здійснення повноважень, визначених законом. Закон України «Про оперативно-розшукову діяльність», надає право оперативним підрозділам для виконання завдань оперативно-розшукової діяльності, серед інших: «здійснювати аудіо-, відеоконтроль особи, зняття інформації з електронних комунікаційних мереж, електронних інформаційних мереж згідно з положеннями статей 260, 263-265 Кримінального процесуального кодексу України». Крім того, Інструкція «Про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні», затверджена наказом Генеральної прокуратури України, Міністерства внутрішніх справ України, Служби безпеки України, Адміністрації Державної прикордонної служби України, Міністерства фінансів України, Міністерства юстиції України від 16.11.2012 визначає види негласних слідчих (розшукових) дій, які проводяться виключно у кримінальному провадженні щодо тяжких або особливо тяжких злочинів. Серед них є: «Зняття інформації з транспортних телекомунікаційних мереж, яке полягає в негласному проведенні із застосуванням відповідних технічних засобів спостереження, відбору та

фіксації змісту інформації, яка передається особою, а також одержанні, перетворенні і фіксації різних видів сигналів, що передаються каналами зв'язку (знаки, сигнали, письмовий текст, зображення, звуки, повідомлення будь-якого виду)» [173].

Також в Інструкції визначено перелік негласних слідчих (розшукових) дій, які проводяться незалежно від тяжкості злочину, зокрема: «Зняття інформації з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або утримувачем чи не пов'язаний з подоланням системи логічного захисту (ч. 2 ст. 264 КПК України), полягає в одержанні інформації з електронних інформаційних систем, що містять відповідну інформацію, у тому числі із застосуванням технічного обладнання» [173].

Отже, аналіз змісту Інструкції дозволяє зробити висновок, що негласний моніторинг соціальних медіа має проводитись у випадках відкритого кримінального провадження з дотриманням визначеної процедури і належної фіксації. Важливо зазначити, що п.6.1 Інструкції встановлює обов’язок знищення інформації, яка втратила актуальність або немає відношення до кримінального провадження: «Відомості, речі та документи, отримані в результаті проведення негласної слідчої (розшукової) дії, які прокурор не визнає необхідними для подальшого проведення досудового розслідування, повинні бути негайно знищені на підставі його рішення, викладеного в постанові (ст. 255 КПК України)». Крім того, важливим є дотримання конституційного права особи на інформацію щодо проведення стосовно неї негласних слідчих (розшукових) дій. Так, п.7.1.3. Інструкції говорить, що «повідомлення про факт і результати негласної слідчої (розшукової) дії повинне бути здійснене протягом дванадцяти місяців з дня припинення таких дій, але не пізніше звернення до суду з обвинувальним актом».

Аналіз нормативно-правових актів і наукових джерел дозволяє сформулювати узагальнені положення щодо правового регулювання моніторингу соціальних медіа правоохоронними органами. По-перше, такий моніторинг має

здійснюватися лише за наявності обґрунтованих підстав та з дотриманням принципів доцільності і необхідності. Інформацію зі соціальних мереж слід збирати тоді, коли існують конкретні факти, які свідчать про її релевантність та суттєвість для поточного кримінального провадження. По-друге, зібрані дані мають бути належним чином задокументовані, включати опис пошукових запитів, критерії відбору інформації та підстави для моніторингу, а також оцінені на предмет достовірності та надійності перед використанням у слідчих діях. Крім того, інформація, що стосується інших органів або осіб, не може передаватися без юридично обґрунтованих підстав, наприклад, у випадку, якщо вона містить докази злочинної діяльності, що належить до компетенції іншого органу, або безпосередньо стосується поточного розслідування.

Особливу увагу необхідно приділяти використанню таємних облікових записів правоохоронцями під час розслідувань у соціальних мережах. Створення таких облікових записів повинно здійснюватися лише у межах санкціонованого розслідування та за попередньої згоди особи, яку видають за іншу. Дії офіцерів мають бути чітко обмежені рамками завдань розслідування, документовані та підконтрольні, без втручання в персональні дані або змін інформації у чужому обліковому записі поза визначеними цілями [174].

Запровадження таких правил дозволяє збалансувати ефективність правоохоронних дій та захист прав і свобод людини, а також створює основу для розроблення національної методики правового моніторингу соціальних медіа та правових засад використання його результатів у кримінальному процесі.

Можливості мережі Інтернет не вичерпуються лише розміщенням у ній певної інформації. Вона слугує також інструментом об’єднання, злагодження, з’єднання і синхронізації роботи багатьох технічних приладів. Це явище отримало назву *«Інтернет речей» (IoT)*. Використання технології Інтернету речей швидко трансформує різні галузі, і правоохоронні органи не є винятком. Інтернет речей має потенціал для революції в поліцейській діяльності, надаючи нові інструменти та можливості, які можуть покращити спостереження, покращити зв’язок і дозволити приймати рішення на основі отриманих даних.

З розвитком технологій і ІТ-відносин розвивається і визначення поняття «Інтернет речей» (IoT) і на сьогодні активно застосовуються наступні варіанти дефініції:

– це пристрої, транспортні засоби, будови та інші предмети, вбудовані в електроніку, програмне забезпечення, датчики та мережеве підключення, що дозволяє цим об'єктам збирати та обмінюватися даними [175];

– сукупність взаємодіючих технічних систем і комплексів, що складаються з мікропроцесорів, сенсорів, пристроїв, систем передачі даних, локальних і/або розподілених обчислювальних ресурсів і програмних засобів, у тому числі програм штучного інтелекту, на основі використання величезної кількості даних і мережі Інтернет та призначених для здійснення суспільних відносин, зокрема, пов'язаних із наданням послуг або проведенням робіт за безпосередньою участю або без участі суб'єктів цих відносин (юридичних або фізичних осіб) [176];

– глобальна інфраструктура для інформаційного суспільства, яка надає передові послуги шляхом взаємозв'язку (фізичних та віртуальних) речей на основі наявних та розвинутих взаємодіючих інформаційно-комунікаційних технологій [177];

– Інтернет речей можна визначити як інформаційно-технологічну концепцію побудови інформаційних і комунікаційних інфраструктур на основі обчислювальної мережі, яка з'єднує речі (фізичні об'єкти), оснащені інформаційними технологіями для здійснення комунікаційного обміну один з одним і глобальною інформаційно-комунікаційною інфраструктурою або безпосередньо, або через інтегровані з ними інші пристрої, які мають адресу протоколу Інтернет (IP) без участі людини з метою збору, передачі, накопичення та обробки інформації [178].

Отже, технічні пристрої, що входять в мережу IoT можуть варіюватися від простих датчиків і камер до більш складних систем, таких як дрони та мережі спостереження. Аналізуючи дані з різних джерел, таких як соціальні медіа, матеріали з камер відеоспостереження, GPS-навігаторів, а також історичні моделі злочинності, правоохоронні органи можуть визначити потенційні «гарячі точки»

злочинності та відповідно розподілити ресурси. Крім того, IoT може допомогти у запобіганні злочинності за допомогою прогнозної аналітики. Цей проактивний підхід може допомогти стримувати злочинну діяльність і покращити громадську безпеку.

Цікавим для України є варіант використання IoT у сфері безпеки. Зокрема, сьогоднішні технічні можливості виявлення супротивника і наявність високоточного озброєння змушують до високої мобільності та швидкого прийняття рішень. Це можливо лише за умови оперативного отримання інформації з різних джерел у режимі реального часу усіма задіяними в операції підрозділами. Одним зі способів вирішення цієї проблеми стало застосування рішень, які отримали назву «Інтернет бойових речей» (Internet of Battle Things, IoBT). Можливості Інтернету бойових речей охоплюють збирання та обробку будь-якої корисної інформації; вона виступає у ролі агентів, які допомагають здійснити скоординовані оборонні дії; забезпечують керування та логістичну підтримку комбінованих операцій; здійснюють контроль стану транспортних засобів, моніторинг навколишнього середовища. Методика інноваційна і перебуває ще на стадії апробації в деяких країнах західної Європи. Наприклад, що у 2016 році Нідерланди стали першою країною світу, яка повністю покрила себе національною мережею для Інтернету речей. В основі ідеї лежить створення енергоефективної мережі, яка б дозволила передавати невеликі обсяги інформації на значні відстані [179, с. 297].

Використання Інтернету речей може забезпечити також якісно новий рівень запобігання злочинності. Правоохоронні органи почали використовувати пристрої IoT, щоб революціонізувати свою роботу. Камери, які носять на тілі, стали основним приладом поліцейських, що дозволяє їм знімати відео-докази та забезпечувати прозорість у їхній взаємодії з громадськістю. Ці пристрої не тільки захищають правоохоронців від неправдивих звинувачень, але й притягують їх до відповідальності в разі службових порушень.

Найбільш поширеними елементами в системах IoT, що застосовуються правоохоронцями є відеоспостереження і GPS-трекери. Інтелектуальні системи

відеоспостереження також були інтегровані в стратегії правоохоронних органів, пропонуючи більш ефективний і ефективний спосіб моніторингу громадських місць. Ці системи використовують передову аналітику та технології розпізнавання облич для виявлення потенційних загроз або розшукуваних осіб, що дозволяє правоохоронним органам швидко реагувати та запобігати злочинній діяльності. GPS-трекери виявилися безцінними інструментами в операціях правоохоронних органів. Прикріплюючи ці пристрої до транспортних засобів або активів, правоохоронці можуть відстежувати їх місцезнаходження в режимі реального часу, допомагаючи у вилученні викраденого майна та затриманні підозрюваних. Крім того, GPS-трекери відіграють важливу роль у моніторингу переміщень відомих злочинців, дозволяючи правоохоронним органам збирати докази та будувати проти них вагомі докази.

Ще одним інноваційним пристроєм Інтернету речей, який активно поширюється у правоохоронних органах, є датчики виявлення пострілів. Ці датчики при розміщенні в районах з високим рівнем злочинності можуть миттєво виявляти звук пострілів, сповіщаючи правоохоронні органи про місце події. Ця технологія здатна скоротити час реагування на подію, потенційно рятуючи життя та збільшуючи шанси на затримання злочинців.

Новим напрямком правового регулювання у сфері Інтернету речей (IoT) є управління ідентифікацією даних та користувачів, а також інтеграція штучного інтелекту (ШІ) у процеси ідентифікації. Сучасні дослідження показують, що ідентифікація фізичної особи в цифровому середовищі може здійснюватися за допомогою різноманітних технологій. Наразі єдиною загальновизнаною системою електронної ідентифікації є інфраструктура відкритих ключів (PKI), яка базується на криптографічних методах і передбачає персональну ідентифікацію користувача або власника цифрового підпису на момент створення особистого ключа.

Водночас сучасне IoT-середовище характеризується високою неоднорідністю як у механізмах ідентифікації, так і в універсальних ідентифікаційних системах. Подібна неоднорідність спостерігається і у підходах

до нормативно-правового регулювання цієї сфери, що ускладнює формування чітких стандартів та визначень. Науковці не досягли консенсусу щодо класифікації ідентифікаційних та персональних даних, їх деталізації та однозначності дефініцій. Як зазначає О. В. Бугера: «з метою підвищення безпеки у сфері IoT доцільним є концептуальне обґрунтування використання можливостей Інтернету речей для запобігання злочинності. Зокрема, ефективне застосування IoT у кримінологічному контексті можливе через створення комплексної системи збору та аналізу інформації, що має кримінологічне значення, із використанням звукових датчиків, відеокамер, безпілотних літальних апаратів та інших технологічних засобів [179, с. 297].

Отже, необхідно враховувати потенційні проблеми, пов’язані із застосуванням технологій Інтернету речей (IoT) у діяльності правоохоронних органів. Експерти наголошують на необхідності формування цілісного законодавчого підходу до управління ідентифікаційними даними у контексті застосування IoT і ШІ. До ключових заходів зменшення ризиків у цій сфері відносять впровадження ефективної політики захисту даних, забезпечення прозорості процесів та механізмів підзвітності, що створює правову основу для безпечного та законного використання технологій IoT у правоохоронній діяльності.

Треба зазначити, що стрімкий розвиток технологій випереджає можливості правової системи, тому законодавство нового покоління має закладати універсальні принципи, етичні норми та вимоги, які будуть дійсні незалежно від появи конкретних технологій. Національне законодавство, зокрема закони України «Про захист персональних даних» та «Про інформацію», а також Розпорядження Кабінету Міністрів України «Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки» (від 17.01.2018 № 67-р), містять загальні положення щодо конфіденційності та інформаційної безпеки, але недостатньо адаптовані до специфіки IoT та новітніх цифрових реалій. Відсутність уніфікованих стандартів і сертифікаційних протоколів для користувачів і розробників створює ризики правопорушень і зловживань,

оскільки виробники часто не несуть обов’язку забезпечувати безпеку продуктів, а користувачі не завжди мають повне розуміння своїх прав.

Ще однією суттєвою проблемою у сфері Інтернету речей (IoT) залишається невизначеність юрисдикції, що охоплює як суб’єктів, так і об’єкти цих правовідносин. Це стосується, зокрема, встановлення застосовного права, територіальної дії законодавства, персонального кола його дії, а також місця вирішення спорів. Така ситуація зумовлює потребу у подальшому вдосконаленні приватно-правового регулювання на міжнародному та доктринальному рівнях.

Вважається доцільним у галузі IoT та ШІ визначити уповноваженого державного суб’єкта права, на якого покласти завдання розробки правових регуляторних актів і формування вітчизняного глосарію технічних та техніко-юридичних визначень, дефініцій і законодавчих положень. Також доцільно розробити відкриту онлайн-платформу для залучення розробників робототехніки та штучного інтелекту до державних програм цифровізації країни, а також для забезпечення їх державної фінансової підтримки та правового захисту.

2.3 Використання новітніх технологій для підвищення особистої безпеки та професійної компетентності працівників правоохоронних органів

Як уже зазначалося у попередніх підрозділах, штучний інтелект є потужним технологічним інструментом, здатним розширювати людські можливості, автоматизувати трудомісткі процеси та генерувати нові ідеї на основі аналізу великих обсягів даних. Його потенціал трансформувати різні сфери суспільного життя, зокрема правоохоронну діяльність, є надзвичайно високим. У сфері поліцейської роботи ШІ може автоматизувати низку завдань, що зменшує навантаження на персонал і знижує ймовірність людських помилок, особливо під час виконання рутинних, повторюваних або виснажливих дій. До прикладу, системи на основі ШІ здатні забезпечити автоматичне розшифрування, структурування та аналіз поліцейських звітів, допитів та доказової бази.

Штучний інтелект має потенціал не лише для автоматизації рутинних процесів, а й для підвищення професійної спроможності правоохоронців. Завдяки аналітичним інструментам і алгоритмам підтримки рішень, технології ШІ допомагають оперативно оцінювати ризики, формувати прогностичні моделі та забезпечувати більш зважене реагування на складні ситуації. Це сприяє зростанню ефективності управлінської діяльності, оптимізації використання ресурсів і підвищенню рівня ситуаційної обізнаності працівників правоохоронних органів.

Окрім того, технології ШІ відкривають нові можливості для професійного навчання та розвитку кадрів. Використання інтелектуальних навчальних платформ, симуляцій і систем адаптивного навчання дозволяє формувати індивідуальні траєкторії підготовки, моделювати оперативні ситуації та отримувати аналітичний зворотний зв'язок у реальному часі. Таким чином, важливими напрямами впровадження ШІ в діяльність правоохоронних органів є управління, професійна освіта та забезпечення особистої безпеки правоохоронців, що сприяє формуванню сучасної, ефективної та технологічно орієнтованої системи правоохоронної діяльності.

Оскільки все частіше цифрові технології застосовуються на робочому місці, набуття та підтримка цифрових навичок стає все більш важливим для переважної більшості працівників. За даними Європейської комісії, попит на працівників зі спеціалізованими цифровими навичками зростає приблизно на 4% щороку [180]. Оскільки робоче місце продовжує зазнавати суттєвої реструктуризації у відповідь на впровадження ШІ та ІКТ, багато цифрових навичок швидко застаріють. Проблема змін у сфері ринку праці і робочої сили, викликана впровадженням технологій, є предметом підвищеної уваги Міжнародної організації праці. Ця міжнародна інституція за останні 10 років провела десятки досліджень у цій сфері. Наприклад, у 2018 році була опублікована Доповідь «Global Skills Trends, Training Needs and Lifelong Learning Strategies for the Future of Work», підготовлена МОП та OECD для Робочої групи G20 з питань зайнятості. Серед іншого, в ній зазначається, що первинне отримання

професійних навичок через початкову підготовку для єдиної довічної кваліфікації вже недостатнє і малоефективне, бо все частіше піддається ризикам в контексті швидкої зміни потреб у навичках [181].

Таким чином, щоб залишатися конкурентоспроможними, працівникам необхідно буде постійно підтримувати свою професійність шляхом набуття нових або вдосконалення наявних навичок. Це вимагає від працівника гнучкості, позитивного ставлення до навчання впродовж життя та допитливості. Широкий вплив роботизації і штучного інтелекту на кваліфікацію кадрів свідчить про те, що науковцям і практикам необхідно переосмислити професійне навчання на рівні держави [182]. Так, за даними Тренінгового центру прокурорів України у 2025 році 7245 прокурорів підвищили свою кваліфікацію за 29 навчальними програмами, серед яких: тренінг «Електронні докази, пошук, перевірка та фіксація даних з Інтернету», тренінг «Використання технологій Штучного інтелекту в професійній діяльності прокурора», тренінг «Оброблення та захист персональних даних в інформаційних системах органів прокуратури», курс «Цифрова грамотність прокурора» тощо [183] за даними ДБР у 2024 році пройшли підвищення кваліфікації 965 осіб рядового і начальницького складу. Працівники ДБР брали участь у семінарах з питань діяльності правоохоронних органів України під час війни та у повоєнний період, інноваційної криміналістики в умовах війни, протидії злочинному порушенню законів і звичаїв війни, боротьби з фінансовими злочинами, проведення негласних (слідчих) розшукових дій, розслідування кримінальних правопорушень за фактами катування та інших [162].

Потужна програма підготовки та підвищення кваліфікації співробітників запроваджується в останні роки Службою безпеки України. Так, при Національній академії СБУ функціонує Навчальний ситуаційний центр кібербезпеки об’єкта критичної інфраструктури, де готують майбутніх кіберфахівців СБУ. Також в Україні започатковано міжвідомчу освітню платформу «Взаємодія заради Перемоги» для представників сектору безпеки і оборони. На її основі реалізовано сертифікатні програми боротьби з тероризмом,

переговірної діяльності, захисту об’єктів критичної інфраструктури, методів і засобів OSINT-технологій, оперативної психології [184].

Погоджуючись із підходом, обґрунтованим у дослідженні Д. Денищука щодо контролю знань працівників ДКВС України, вважаємо можливим екстраполювати його висновки на діяльність усіх правоохоронних органів. Контроль цифрових навичок повинен мати систематичний характер, здійснюватися на постійній основі через сукупність організаційних, навчальних і перевірочних заходів та не обмежуватися вичерпним переліком форм [185, с. 369]. Він має охоплювати всіх співробітників, допущених до роботи з інформаційними джерелами та ІКТ, тоді як контроль рівня знань керівника забезпечується суб’єктом, у сфері управління чи підпорядкування якого він перебуває. Таким чином, відповідний підхід слід розглядати як універсальну модель організації контролю знань у сфері використання інформаційно-комунікаційних технологій в системі правоохоронних органів України.

Питання особистої безпеки під час виконання професійних обов'язків, а також підтримка фізичного і ментального здоров'я співробітника правоохоронного органу мають надважливе значення, як для самого поліцейського, так і для суспільства на благо якого він працює. У цьому контексті цікавими є наробки зарубіжних компаній і правоохоронних структур щодо застосування технологій штучного інтелекту у сфері охорони праці, а саме – моніторинг фізичного стану співробітників при виконанні службових обов’язків.

Як відомо, у повсякденній роботі правоохоронці стикаються з високим рівнем стресу, травм і фізичного ризику. Ці фактори можуть вплинути на їхнє здоров’я, продуктивність і прийняття рішень. Сьогодні носимі пристрої, які фіксують фізичний стан людини, широко застосовуються роботодавцями в різних сферах господарства. Здебільшого це стосується працівників, які залучаються до робіт зі шкідливими або небезпечними умовами праці (будівельники, рятувальники, хімічні підприємства, атомна енергетика тощо). Зважаючи на те, що до 2030 року світове зростання обсягів носимих технологій оцінюється на 14,6% (Звіт про частку ринку та тенденції носимих технологій,

2030) [186], багато компаній зараз інвестують у носимі технології для своїх співробітників. Для працівників поліції та інших правоохоронних органів, залучених до виконання завдань, що супроводжуються ризиками особистої небезпеки, використання відповідних пристроїв також є нагальною необхідністю.

Найбільш розповсюдженою в зарубіжній поліцейській практиці є технологія моніторингу та аналізу поведінки водія. На сьогодні існують технології для аналізу поведінки, уваги та пильності водія в реальному часі. Наприклад, технологія SOLO AI використовується для діагностики стану поліцейського при патрулюванні вулиць на автомобілі [187]. Вона базується на останніх дослідженнях і розробках у сфері виявлення втоми водія, аналізу поведінки водія та навчання водіїв. При цьому використовується камера, яка встановлена на лобовому склі або панелі приладів автомобіля, і програмне забезпечення, яке обробляє зображення та відео, зняті камерою. Технологія може виявляти різні ознаки втоми водія, такі як заплющення очей, поза голови, позіхання, кліпання та вираз обличчя. Ця технологія також може вимірювати когнітивне навантаження, відволікання та залучення водія, аналізуючи напрямок погляду водія, розширення зіниці та рухи очей. На основі аналізу поведінки, уваги та пильності водія штучний інтелект може надати своєчасний і персоналізований зворотний зв’язок, попередження та втручання водієві, а також диспетчерам і супервайзерам, щоб допомогти їм керувати втомою водія та покращити самопочуття офіцера. При цьому використовується хмарна платформа, яка збирає та аналізує дані з камер і сенсорів, визначає закономірності поведінки водія та формує звіти й інформаційні панелі щодо рівня втоми, навичок керування та стану здоров’я. Платформа застосовує методи машинного та глибокого навчання для оцінки даних, створення індивідуалізованих навчальних програм, порівняння показників водія з даними інших користувачів та формування рейтингових контрольних показників для мотивації підвищення ефективності водіння. Крім того, система передає інформацію керівникам і диспетчерам для ухвалення

обґрунтованих рішень і розробки політик, спрямованих на підвищення безпеки та здоров’я офіцерів.

SOLO AI не є єдиною технологією, яку можна застосовувати для моніторингу та аналізу поведінки водія, а також для надання зворотного зв’язку й інструктажу. На сучасному ринку існують інші системи, які виконують аналогічні функції та забезпечують безпеку і ефективність керування. Серед них технологія моніторингу стану водія (DSM), розроблена компанією Seeing Machines, яка використовує камеру та інфрачервоний датчик для відстеження очей, положення голови та виразу обличчя водія, а також для виявлення ознак втоми, відволікання чи погіршення самопочуття, при цьому надаючи сповіщення та втручання в реальному часі. Подібним чином функціонує Driver Attention Monitor (DAM) компанії Denso, яка застосовує камеру та радарні сенсори для оцінки стану водія і забезпечує оперативні рекомендації для запобігання аварійним ситуаціям. Технологія DriverFocus від Subaru використовує камеру та програмне забезпечення для розпізнавання обличчя з метою відстеження очей, голови та виразу обличчя, а також для своєчасного попередження про ознаки втоми чи відволікання. Аналіз поведінки водія (DBA), розроблений компанією Affectiva, інтегрує камеру та динамік для оцінки очей, голови, виразу обличчя та голосових сигналів водія, що дозволяє виявляти ознаки втоми, відволікання, порушень, настрою та емоцій, і надавати індивідуальний зворотний зв’язок і рекомендації щодо підвищення продуктивності водіння. Система навчання водіїв (DCS) компанії GreenRoad також використовує камеру та динамік для комплексного відстеження очей, голови, виразу обличчя та голосу водія, а додатково вимірює швидкість, гальмування, прискорення та зміну смуги руху, що дозволяє формувати програми корекції поведінки та підвищувати безпеку руху.

Усі ці технології інтегрують елементи машинного навчання та глибокого навчання для аналізу великих обсягів даних, виявлення закономірностей і тенденцій у поведінці водія, формування контрольних показників та рейтингових систем для мотивації та вдосконалення навичок керування. Водночас вони можуть забезпечувати обмін даними та аналітикою з керівниками та

диспетчерами, що дозволяє приймати обґрунтовані управлінські рішення та формувати політику щодо безпеки та здоров'я персоналу. Таким чином, інтеграція цих технологій у професійну діяльність створює комплексну систему контролю та підвищення ефективності водіння, що поєднує технічні, поведінкові та навчально-методичні аспекти.

Ще одна новітня розробка, яка проходить тестування і активно обговорюється в зарубіжних джерелах – «електронна шкіра» була розроблена для різних застосувань, таких як робототехніка, протезування, медицина та розваги. Однак одним із найбільш перспективних і нових її застосувань є моніторинг здоров'я та діагностика. Технологія повторює охорони здоров'я астронавтів NASA [188]. Електронна шкіра – це гнучкий і тонкий матеріал, який може імітувати властивості та функції шкіри людини. Він може відчувати різні подразники, такі як тиск, температура, вологість і хімічні речовини, і передавати сигнали на пристрій або систему для обробки та інтерпретації.

Завдяки інтеграції електронної шкіри зі штучним інтелектом можна аналізувати дані, зібрані датчиками, і надавати в режимі реального часу зворотний зв'язок і рекомендації, наприклад, поліцейським і їхнім керівникам. Наприклад, штучний інтелект може інформувати поліцейських про їхній рівень стресу та запропонувати їм зробити перерву, потренуватися або звернутися за консультацією; він також може попередити про підвищений/знижений артеріальний тиск або рівень глюкози та порадити приймати ліки, займатися спортом або відвідати лікаря. ШІ також може сповіщати керівників про здоров'я та продуктивність співробітників і рекомендувати їм втрутитися або підтримати їх за потреби (наприклад, штучний інтелект може повідомити про офіцера, який виявляє ознаки втоми, відволікання чи агресії, і запропонувати їм призначити інше завдання, партнера чи відпустку).

Сучасні технології зі штучним інтелектом підвищують безпеку та ефективність роботи працівників правоохоронних органів, проте їхнє впровадження супроводжується низкою обмежень. Основні проблеми пов'язані з варіативністю точності та надійності алгоритмів залежно від якості відео, умов

освітлення та фізіологічних особливостей осіб; питаннями конфіденційності, безпеки та етики обробки даних; а також сприйняттям і довірою користувачів до зворотного зв’язку та попереджень, які генерує ШІ.

Вважаємо, що успішне впровадження таких технологій потребує системного підходу, що включає: ретельне тестування та оцінювання алгоритмів ШІ та комп’ютерного зору для забезпечення їхньої точності, надійності та усунення потенційних упереджень та технічних помилок; запровадження прозорих та регламентованих процедур обробки даних для гарантування конфіденційності, безпеки та етичності, а також забезпечення інформованої згоди учасників процесу; активне залучення всіх зацікавлених сторін – правоохоронців, диспетчерів, наглядачів та громадськості – до розробки, тестування та впровадження систем зворотного зв’язку та попереджень, що сприяє їхній прийнятності, підвищенню зручності та ефективності використання технологій, а також подоланню потенційного опору або недовіри до інновацій.

Як вбачається з вищесказаного, технології активно розвиваються і впроваджуються у професійну сферу правоохоронців. Не всі з них поки що мають достатній рівень розробки, але вектор заданий і визначений. Підвищення безпеки працівника при виконанні професійної діяльності, навчання цифровим навичкам, підтримка фізичного і ментального здоров'я, часткова або повна заміна людини при виконанні небезпечних завдань – мета, до якої мають прагнути розробники і керівники правоохоронних органів при залученні технологій штучного інтелекту у професійну діяльність.

Розвиток і впровадження технологій штучного інтелекту у професійну діяльність правоохоронців визначає нові вимоги до їхніх професійних компетентностей і рівня цифрової підготовки. Підвищення безпеки, підтримка фізичного та ментального здоров’я, а також ефективне використання технологій у складних чи небезпечних завданнях вимагає системного підходу до навчання та розвитку персоналу. Саме у цьому контексті важливо враховувати зарубіжний досвід для формування національної стратегії впровадження цифрових та інноваційних технологій у діяльність правоохоронних органів. Наприклад,

запозичення ефективних зарубіжних практик дозволяє враховувати перевірені підходи до підготовки персоналу, організації навчання, тестування та оцінки технологій, а також забезпечення етичних стандартів і захисту прав людини. На основі такого досвіду доцільно розробляти національні програми, які інтегрують підвищення цифрової компетентності, адаптацію до інноваційних рішень та створення безпечного й ефективного середовища для виконання професійних обов'язків правоохоронців. Зокрема, на рівні державної політики доцільним є: впровадження обов'язкових блоків цифрової підготовки у програми післядипломного навчання працівників поліції; регулярне оновлення навчальних матеріалів з урахуванням сучасних технологій та штучного інтелекту, а також створення механізмів оцінки ефективності таких навчальних програм.

На рівні організаційної та операційної практики пропонується: інтегрувати інтелектуальні системи автоматизації рутинних та аналітичних процесів, що дозволяє працівникам зосередитися на критично важливих аспектах оперативної діяльності; застосовувати алгоритми ШІ для зниження ризиків у реальному часі та підтримки прийняття рішень; впроваджувати персональні цифрові асистенти для підвищення ситуаційної обізнаності та контролю над небезпечними ситуаціями; використовувати аналітичні системи для об'єктивної оцінки професійних компетентностей, формування персоналізованих навчальних програм і надання якісного зворотного зв'язку.

Висновки до розділу 2

1. Розглянуто основні наукові підходи до дослідження технології штучного інтелекту, зокрема когнітивно-символічний, нейронний, філософсько-теоретичний, правовий і соціально-гуманітарний. Зроблено висновок про відсутність єдності в науковій літературі щодо визначення змісту та юридичної природи штучного інтелекту. Це обумовлює необхідність створення своєрідного «правового каркасу», який має визначати межі допустимого використання технологій ШІ у правоохоронній сфері, передбачати дієві механізми контролю,

нагляду й аудиту алгоритмічних систем, а також встановлювати обов'язковість попередньої оцінки їхнього впливу на права людини перед запровадженням у практику.

2. Проаналізовано особливості реалізації принципів ШІ у діяльності правоохоронних органів. Зазначено, що вони мають базуватися на загальноправових, галузевих та міжгалузевих принципах використання ІКТ правоохоронцями. Розглянуто зміст принципів конфіденційності, оспорюваності та відшкодування, верховенства інтересів людини з урахуванням специфіки застосування технології штучного інтелекту в правоохоронній сфері. Зроблено висновок що держава має забезпечити ефективні механізми контролю, аудиту та нагляду за збереженням конфіденційності персональних даних на всіх етапах життєвого циклу алгоритмів ШІ – від розробки до практичного застосування. Для цього необхідно впровадити систему моніторингу та перевірки алгоритмів на законність та дотримання діючого законодавства, а також встановити взаємну відповідальність розробників програмного забезпечення та правоохоронного органу за відповідні порушення.

3. Визначено коло суб'єктів використання штучного інтелекту в правоохоронній діяльності, які класифіковано за функціональним призначенням: 1) правоохоронні органи, уповноважені законом застосовувати ІКТ та ШІ у межах оперативно-розшукової та кримінально-процесуальної діяльності; 2) органи державного управління і регулювання, що формують державну політику та нормативне забезпечення у сфері ШІ; 3) інституції контролю, нагляду й захисту прав людини; 4) розробники та технічні адміністратори систем ШІ, відповідальні за їх безпеку і відповідність законодавству; 5) громадяни як користувачі та суб'єкти впливу алгоритмічних рішень.

4. Здійснено комплексний аналіз технологічного потенціалу та правового регулювання технології розпізнавання облич (Facial Recognition Technology, FRT) як елементу процесів збирання, накопичення, обробки й аналітичного використання інформації у діяльності правоохоронних органів. Обґрунтовано, що застосування FRT у режимі реального часу, яке передбачає збирання,

зіставлення та/або зберігання зображень облич для ідентифікації особи, становить втручання у право на захист персональних даних, гарантоване Законом України «Про захист персональних даних», а отже, має здійснюватися на засадах законності, цільової обумовленості та пропорційності. Доведено необхідність удосконалення чинного законодавства шляхом запровадження норм, що передбачають відповідальність як розробників технологій за порушення технічних регламентів, процедур тестування та впровадження, так і правоохоронних органів – за неправомірне або надмірне використання технології розпізнавання обличь.

5. Обґрунтовується позиція, що еквівалентність документів, створених із застосуванням систем штучного інтелекту та традиційних офіційних документів підтверджується їх спільною правовою природою, функціональним призначенням і процедурними засадами створення. Проведено класифікацію документів, створених із використанням ШІ, за критерієм ступеня автономності системи у процесі їх формування. Зроблено висновок, що оскільки документи, створені автономними алгоритмічними системами, не мають автора у класичному праворозумінні, виникає необхідність нормативного визначення суб’єкта юридичної відповідальності за їх створення, перевірку і використання. Таким суб’єктом може бути оператор, адміністратор або орган, який експлуатує систему, адже саме він приймає кінцеве рішення щодо використання отриманих результатів.

Визначено вимоги до документів згенерованих або створених за допомогою ШІ, а саме: а) обов’язкове маркування документів, створених або оброблених із застосуванням технологій ШІ; б) аналітичні документи, створені за допомогою ШІ, мають містити відомості про алгоритм формування результатів, рівень похибки, а також межі достовірності висновків, якщо вони ґрунтуються на імовірнісних або прогнозних методах; в) документ має містити інформацію про уповноважену особу, яка перевірила документ на відповідність і законність.

6. Зазначено, що відсутність законодавчої бази, що регулює використання поліцією соціальних мереж, залишає правоохоронні органи без достатньої

інформації про їхні права та обов'язки. Їм доводиться користуватися нормативними актами, створеними для офлайн-діяльності, і застосовувати їх у контексті онлайн-розслідувань. Крім того, оскільки не існує стандартизованих методів збору даних в Інтернеті, органи влади часто застосовують різні підходи та різні інструменти, що може призвести до розбіжностей. Тому постала необхідність конкретизації їх прав і обов’язків у цій сфері, визначення організаційно-правових засад такої діяльності.

7. Технології штучного інтелекту можливо використовувати у сфері безпеки і охорони праці працівників правоохоронного органу, а також професійного навчання. При використанні пристроїв з технологією ШІ для моніторингу фізичного стану працівника поліції під час виконання ним професійних обов’язків необхідне встановлення чіткої та прозорої політики та процедур для збору, зберігання та обміну даними, щоб забезпечити конфіденційність, безпеку та етику даних, а також отримати згоду та співпрацю водія, диспетчерів, наглядачів та громадськості. Технології ШІ мають потенціал позитивно впливати на професійний розвиток правоохоронців, надаючи можливості для персоналізованого навчання, тренувань та отримання зворотного зв’язку. Такі інструменти можуть сприяти як покращенню ефективності щоденної роботи, так і кар’єрному зростанню фахівців. Таким чином вважаємо доцільним впровадження в навчальні програми співробітників правоохоронних органів обов’язкового блоку, що підвищує цифрові навички, в тому числі ознайомлення та опрацювання новітніх технологій та програм з елементами штучного інтелекту.

РОЗДІЛ 3
МІЖНАРОДНЕ ЗАКОНОДАВСТВО ТА ДОСВІД ВИКОРИСТАННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ В ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ І МОЖЛИВОСТІ ЇХ АДАПТАЦІЇ В УКРАЇНІ

3.1 Європейські норми та стандарти використання інформаційно-комунікаційних технологій у правоохоронній сфері

Реформування правоохоронних органів України в контексті європейської інтеграції зумовлює потребу в комплексному оновленні підходів до організації їхньої діяльності, зокрема через упровадження сучасних інформаційно-комунікаційних технологій. Використання новітніх цифрових рішень сприяє підвищенню ефективності, прозорості та результативності правоохоронної діяльності, забезпечуючи належний рівень інформаційно-аналітичної підтримки управлінських рішень. У цьому зв’язку особливої актуальності набуває вивчення міжнародного досвіду застосування інформаційних технологій у діяльності правоохоронних органів, адаптація та імплементація його найкращих практик у вітчизняну правову систему.

Наразі інформаційне забезпечення діяльності правоохоронних органів України потребує суттєвого вдосконалення з метою забезпечення ефективної протидії злочинності у сферах національної безпеки, охорони життя та здоров’я людини, боротьби з незаконним обігом наркотиків, а також у економічній та екологічній сферах. Рівень розвитку інформаційно-аналітичних систем безпосередньо впливає на здатність держави забезпечувати громадську безпеку та правопорядок. Додаткових викликів у цьому контексті створює збройна агресія проти України, що супроводжується інформаційною війною та кібератаками, спрямованими на підрив національної безпеки. Ми вважаємо цілком справедливою думку науковців про те, що: «..міжнародне поліцейське співробітництво слідує розглядати сьогодні як один із компонентів взаємодії

держав у сфері боротьби зі злочинністю, що саме по собі є важливою частиною міжнародних відносин..». Це викликає необхідність інтеграції вітчизняних інформаційно-аналітичних систем у міжнародні, що зумовлює необхідність удосконалення цих систем відповідно до технологічного рівня вимог розвинутих країн і насамперед країн Європейського союзу [189].

Так, 4 грудня 2009 року у Києві Україна підписала Угоду з Європейським поліцейським офісом про стратегічному співробітництві, яка була ратифіковано 5 жовтня 2010 року. Метою цієї Угоди було посилення співробітництва держав – членів Європейського Союзу, які діють через Європол, з Україною в запобіганні серйозним формам міжнародної злочинності, їхньому виявленні, припиненні та розслідуванні у сферах, зокрема шляхом обміну стратегічною й технічною інформацією. Стратегічна інформація включає заходи правоохоронного характеру, які можуть бути корисними для припинення злочинів; нові способи скоєння злочинів; спостереження та дані, отримані в результаті успішного застосування нових правоохоронних методів та засобів; маршрути, які використовуються контрабандистами або особами, причетними до злочинів, пов'язаних із торгівлею людьми та змінами цих маршрутів і так далі. Однак ця угода не давала повноважень на передачу даних, що належать до встановлення осіб, які вчинили злочини [190]. Документ втратив чинність у 2017 році у зв’язку з підписанням нової угоди «Про оперативне та стратегічне співробітництво», яка робить акцент на захисті персональних даних при їх передачі чи обробці. Крім того, стаття 4 цієї Угоди зазначає, що: «…крім обміну інформацією, співробітництво може включати, відповідно до визначених Рішенням Ради Європолу завдань Європолу, обмін спеціальними знаннями, загальними зведеннями, результатами стратегічного аналізу, інформацією щодо процедур кримінальних розслідувань, інформацією про методи запобігання злочинності, участь у навчальних заходах, а також надання консультацій та підтримки в окремих кримінальних розслідуваннях» [191].

У 2002 році в рамках Європолу Державами, що входять до Європейського Союзу, було запроваджено єдину автоматизовану систему обліку кримінальних

відомостей. До складових комплексної інформаційно-аналітичної системи TECS (The Europol Computer System), крім власне AIC, також належать аналітичний центр та індексна підсистема. Комп'ютерна система TECS дозволяє одночасно обробити та проаналізувати майже мільйон записів. Вся інформація до системи надається безпосередньо державами-членами ЄС. Кожна з країн має власну організацію – представника у Гаазі, так звану ELOS. Тільки ці організації мають доступ до національних баз даних.

Інформаційні системи країн Європейського Союзу, як правило, утворені на загальнонаціональному рівні та забезпечують стратегічний аналіз даних, щодо функціонування злочинних угруповань. На центральному рівні ведуться обліки осіб, які вчинили правопорушення, самі злочини, готуються законодавчі пропозиції нормативного урегулювання роботи кримінальної поліції, підтримуються контакти з Інтерполом. Такий розподіл повноважень дозволяє краще спрямовувати та координувати зусилля, враховуючи розширення міжрегіональних та міжнародних контактів, а також міграцію організованих злочинців, що забезпечує більший рівень конспірації при значному вплив криміналітету на політичні, економічні, а нерідко і правоохоронні структури на місцях, особливо у невеликих містах.

У 2004 році Європейський Союз заснував Агентство з мережевої та інформаційної безпеки (ENISA) [192], яке стало експертним центром з кібербезпеки в Європі. Він тісно співпрацює з державами-членами ЄС та приватним сектором, щоб сприяти «розвитку культури, безпеки мережі та інформації у суспільстві та з метою підвищення обізнаності про NIS». ISACA (Асоціація аудиту та контролю інформаційних систем) вважає, що структура для сертифікації кібербезпеки продуктів і послуг ІКТ має бути регіональною, а не національною, і повинна використовувати існуючі глобальні стандарти та найкращі практики. Крім того, слід переконатися, що при розробці продуктів і послуг на початку процесу проектування враховується кібербезпека, щоб уникнути створення нових вразливостей. Нарешті, ЄС визнав, що усунення прогалини в навичках кібербезпеки є серйозною проблемою, і ISACA рішуче

підтримує заклик до промисловості посилити навчання організацій і персоналу з кібербезпеки.

В грудні 2018 року Європейська комісія з ефективності судочинства у складі Ради Європи затвердила «Етичну хартію щодо використання ШІ в судовій системі та її середовищі». Відповідно до тексту Документа, основною метою Хартії визначається підвищення ефективності та якості здійснення правосуддя шляхом опрацювання алгоритмами судових рішень і даних. При цьому окремо наголошується про обов'язковість дотримання основних прав і свобод людини, які гарантуються Європейською конвенцією з прав людини і Конвенцією Ради Європи про захист персональних даних. Крім іншого, Етична хартія щодо використання ШІ в судовій системі та її середовищі, визначає основні принципи використання штучного інтелекту під час здійснення правосуддя. А саме: «1) дотримання основних прав людини при використанні ШІ; 2) недискримінації (запобігання розвитку будь-якої дискримінації між окремими особами чи групами осіб); 3) якості та безпеки, який стосується обробки судових рішень і даних у безпечному технологічному середовищі; 4) прозорості; 5) неупередженості; 6) справедливості; 7) підконтрольності користувачеві» [152].

Підвищення продуктивності та широка доступність використання штучного інтелекту призвели до вироблення у 2021 році Проекту пропозиції Європейського парламенту та Ради до регламенту, що встановлює гармонізовані правила щодо штучного інтелекту, і який наразі був ухвалений Європейським парламентом 13 березня 2024 р. («Закон про ШІ») і набув чинності 1 серпня 2024 року [153]. Це перша в усьому світі законодавча база щодо штучного інтелекту, спрямована на сприяння розвитку та впровадження безпечних і надійних систем штучного інтелекту в ЄС, а також дотримання основних прав, безпеки та етичних принципів шляхом усунення ризиків потужних моделей штучного інтелекту.

В Законі передбачено наявність компетентного органу (EDPS) для нагляду за інституціями, органами, офісами та агенціями ЄС (EUI) які підпадають під дію цього документу. У цій якості EDPS має право накладати адміністративні штрафи, за певних умов, на тих, хто не виконує положення Закону.

Аналогічно, Європейський наглядовий орган із захисту даних (EDPS) у межах дії цього Закону виконує функції органу ринкового нагляду, а також нотифікуючого органу і нотифікуючого органу для інституцій ЄС. Ринковий нагляд охоплює діяльність уповноважених органів, спрямовану на перевірку відповідності продукції вимогам гармонізованого законодавства Європейського Союзу та на забезпечення захисту суспільних інтересів, які цим законодавством охороняються. У свою чергу, законодавство про штучний інтелект визначає уповноважений орган як орган з оцінки відповідності, який нотифікований згідно з цим регламентом та іншим релевантним законодавством ЄС. При цьому нотифікуючий орган – це національний орган влади, на який покладено повноваження щодо організації процедур оцінювання, призначення та офіційної нотифікації органів з оцінки відповідності, а також здійснення подальшого контролю за їх діяльністю. [193].

Впровадження аналогічної моделі в Україні, з урахуванням положень Регламенту (ЄС) 2019/1020 та принципів ринкового нагляду ЄС, дозволить посилити державний контроль за дотриманням вимог щодо безпечного й відповідального використання технологій ШІ, у тому числі в діяльності правоохоронних органів. Створення уповноваженого органу з питань ШІ сприятиме гармонізації національного законодавства з європейськими стандартами, підвищенню довіри громадян до використання інтелектуальних технологій у публічному секторі та формуванню правової культури цифрової доби.

Насьогодні Закон ЄС про штучний інтелект – це найповніше у світі законодавство щодо штучного інтелекту, орієнтоване на ризики і спрямоване на розвиток інновацій. Він є унікальним з багатьох причин: пропонує багаторівневу структуру класифікації ризиків для систем ШІ; спрямований на стандартизацію законодавства щодо штучного інтелекту в ЄС; створенню органів управління роботи з штучним інтелектом; сприяє орієнтованим на людину та надійним інноваціям у сфері ШІ, збереженню фундаментальних прав і демократичних

цінностей; сприяє міжнародній співпраці та забезпечення можливості безпечного тестування та перевірки систем ШІ перед розгортанням тощо.

Закон ЄС про штучний інтелект класифікує системи штучного інтелекту на основі ризик-орієнтованого підходу та передбачає чотири категорії ризику: неприйнятний, високий, обмежений і мінімальний.

Неприйнятний ризик становлять системи ШІ, які є забороненими. До них належить штучний інтелект, який маніпулює людською поведінкою, щоб обійти свободу волі користувачів (наприклад, підсвідомі методи чи експлуатація вразливих груп), здійснює оцінку чи класифікацію фізичних осіб на основі їхньої поведінки, біометрична ідентифікація в режимі реального часу в публічних місцях (з деякими виключеннями).

Високий ризик включає системи ШІ, які використовуються у критично важливих сферах життя. Наприклад, використання для віддаленої біометрії в реальному часі та постідентифікації фізичних осіб; використання правоохоронними органами в якості поліграфа для виявлення емоційного стану фізичної особи; оцінки достовірності доказів у кримінальному процесі тощо.

Обмежений ризик. До цієї категорії належать системи ШІ, які вимагають зобов'язань щодо прозорості. Наприклад, чат-боти мають бути розроблені таким чином, щоб користувачі знали, що вони взаємодіють із машиною.

Мінімальний ризик. Такі програми штучного інтелекту, як відеоігри чи фільтри спаму, вважаються мінімальним ризиком і можуть вільно розроблятися та використовуватися в межах ЄС [194].

Документ також містить конкретні норми, що встановлюють правила використання ШІ правоохоронцями. Так, у статті 5 вказаного Закону зазначено, що використання систем дистанційної біометричної ідентифікації «в реальному часі» правоохоронними органами зазвичай заборонено, за винятком вичерпно перелічених і вузько визначених ситуацій. Наприклад за умови дотримання суворих заходів безпеки і обмежень за часом і розташуванням, а також за умови спеціального попереднього судового або адміністративного дозволу. Такі види використання можуть включати, наприклад, цілеспрямований пошук (і)

конкретних жертв викрадення чи торгівлі людьми, (ii) запобігання конкретній, суттєвій та неминучій загрозі життю чи фізичній безпеці фізичних осіб, або (iii) локалізації чи ідентифікації особа, яка підозрюється у вчиненні кримінального правопорушення [195]. Також передбачені чіткі вимоги до впровадження і використання інших систем ШІ з високим рівнем ризику. Це обумовлено високою ймовірністю негативного впливу технологій на здоров'я людини, її безпеку, загрозою порушення основних прав і свобод, демократії та верховенства права, а також завдання шкоди навколишньому середовищу. Приклади використання штучного інтелекту з високим ризиком включають критичну інфраструктуру, освіту та професійну підготовку, працевлаштування, основні приватні та державні послуги (наприклад, охорона здоров'я, банки), певні системи правоохоронних органів, управління міграцією та кордонами, правосуддя та демократичні процеси (наприклад, вплив на вибори). Відповідно до Закону ЄС про штучний інтелект: «Такі системи повинні оцінювати та зменшувати ризики, вести журнали використання, бути прозорими та точними та забезпечувати нагляд з боку людини. Громадяни матимуть право подавати скарги на системи ШІ та отримувати пояснення щодо рішень, заснованих на системах високого ризику ШІ, які впливають на їхні права» [196].

Системи штучного інтелекту, цільове призначення яких, за визначенням провайдера, є правоохоронна діяльність або відправлення правосуддя, класифікуються як системи високого ризику згідно з Додатком III Закону. Як такі, вони підпадають під основні вимоги (управління ризиками, тестування управління ризиками, тестування, управління даними, технічна документація, прозорість, людський нагляд, прозорість, точність, надійність та кібербезпека) та зобов'язання (наприклад, системи управління якістю, технічна документація, відповідність системи управління якістю, технічна документація, оцінка відповідності, коригувальні дії, обов'язок інформування, обов'язки імпортерів та дистриб'юторів), а також стандарти та оцінки відповідності [193].

На європейському рівні Закон про ШІ засновує Європейську раду зі штучного інтелекту (EAIB). Подібно до існуючих європейських агентств, таких

як ESMA, EAIB, їй буде доручено координувати дії різних європейських компетентних органів у впровадженні Закону про штучний інтелект та надавати підтримку Комісії та національним наглядовим органам у тому, як аналізувати та реагувати до нових проблем у сфері ШІ.

Крім того, у Комісії створено Офіс штучного інтелекту, який здійснює нагляд за передовими моделями ШІ, сприяє розвитку стандартів і методики тестування та забезпечує виконання загальних правил у всіх державах-членах. Наукова група незалежних експертів консультуватиме Офіс щодо моделей GPAI, допомагаючи розробляти методології оцінки можливостей фундаментальних моделей, надавати рекомендації щодо впровадження моделей із високим потенційним впливом та відстежувати можливі ризики безпеки даних, пов’язані з такими моделями.

Отже, Закон про штучний інтелект має на меті створити довгострокову правову основу для використання штучного інтелекту. Цілями Закону про штучний інтелект є захист основних прав, гармонізація правового середовища для штучного інтелекту на європейському рівні і встановлення правових основ для застосування ШІ у правоохоронній діяльності. [197]

Наразі в ЄС немає спеціального закону, який регулює використання ШІ в правоохоронних органах. Однак існує кілька законодавчих актів, які можуть застосовуватися в процесі розробки та використання штучного інтелекту в цілому та діяльності правоохорониих органів. Ці документи можна поділити на групи відповідно до сфери правового захисту:

1. *Захист та управління даними.* Права на конфіденційність і захист персональних даних (ст. 8 Європейської конвенції з прав людини); ст. ст. 7-8 Хартії основних прав ЄС є кардинальними як для розробки, так і для використання додатків ШІ. Серед законів ЄС, які встановлюють правила захисту та керування даними, основна увага приділяється Регламенту 2016/679 (він же GDPR) [84] і Директиві 2016/680, 29 відомій як LED [146].

Для цілей захисту даних важливо розрізняти етап розробки інструментів аналітики злочинності на основі штучного інтелекту, який регулюється GDPR,

від етапу, коли правоохоронці застосовують такі інструменти в оперативних цілях. Останній регулюється LED у тій мірі, в якій відбувається обробка персональних даних. LED – хоча й має ту саму аксіологічну основу, що й GDPR, представляє різні нюанси щодо, наприклад, позовних прав суб'єктів даних або повноважень органів із захисту даних, пов'язаних із особливостями середовища поліції та кримінального правосуддя (див. пункти 10, 11). Це означає, що персональні дані мають оброблятися законно для цілей правоохоронних органів і що така обробка персональних даних також регулюється принципами обмеження мети, мінімізації даних, точності, обмеження зберігання, цілісності та конфіденційності (ст. 4 (1) LED). Однак, подібно до прав суб'єктів даних, ці принципи були адаптовані для забезпечення певного рівня гнучкості, щоб задовольнити особливі потреби, пов'язані з безпекою, і повсякденну правоохоронну практику.

Що стосується законності обробки персональних даних для правоохоронних цілей, LED є більш обмежувальним порівняно з GDPR та його правовими основами для обробки персональних даних. Так, ст. 8 (1) цього документу вказує, що:

Держави-члени повинні передбачати, що обробка є законною, лише в тій мірі, в якій обробка необхідна для виконання завдання, яке виконується компетентним органом для цілей, викладених у статті 1(1) (а саме запобігання, розслідування, виявлення або судове переслідування кримінальних правопорушень або виконання кримінальних покарань, включаючи захист від загроз громадській безпеці та їх запобігання), і якщо вона ґрунтується на законодавстві Союзу або держав-членів. Таким чином, обробка персональних даних є законною, лише якщо вона пов'язана із завданням у межах сфери дії Директиви, як зазначено у внутрішньому законодавстві, що її транспонує.

ст. 9 LED застосовується на етапі тестування додатків, керованих ШІ, коли правоохоронні органи використовують набори даних, доступні лише їм. Це передбачає, що персональні дані, зібрані компетентними органами з метою запобігання, розслідування, виявлення або переслідування кримінальних

правопорушень, або виконання кримінальних санкцій, можуть оброблятися лише для інших цілей, якщо така обробка дозволена законодавством Союзу або держав-членів. У цьому випадку застосовується GDPR, якщо обробка не здійснюється в рамках діяльності, яка виходить за межі законодавства Союзу (ст. 9 (1) LED). GDPR також застосовується, коли правоохоронні органи обробляють персональні дані, зокрема, для наукових цілей (ст. 9 (2) LED).

Крім того, правоохоронні органи, як контролери даних, зобов'язані проводити оцінку впливу на захист даних (DPIA), як того вимагає ст. 27 (1) LED «де тип обробки, зокрема, з використанням нових технологій, і враховуючи характер, обсяг, контекст і цілі обробки, ймовірно, призведе до високого ризику для прав і свобод фізичних осіб». Важливо, що формулювання LED робить DPIA обов'язковим, коли йдеться про використання нових технологій обробки персональних даних у правоохоронному середовищі.

Нарешті, збір і обробка неперсональних даних регулюється Регламентом ЄС 2018/1807, який «спрямований на забезпечення вільного потоку даних, крім персональних даних, у межах Союзу шляхом встановлення правил, що стосуються вимог до локалізації даних, доступності даних для компетентних органів і перенесення даних для професійних користувачів» (ст. 1). Вимоги щодо локалізації даних можуть встановлюватися з міркувань громадської безпеки (включаючи розслідування злочинів, розкриття та судове переслідування) відповідно до принципу пропорційності (ст. 4 (1)).

2. *Захист основних прав громадян*. Резолюція Європейського Парламенту від 6 жовтня 2021 року «Про штучний інтелект у кримінальному праві та його використання поліцією та судовими органами у кримінальних справах», яка підкреслює необхідність забезпечення дотримання основних прав людини, пропорційності та підзвітності при застосуванні технологій ШІ у правоохоронній сфері [198]. Документ визначає, що системи ШІ, що застосовуються в правоохоронних цілях, належать до високоризикових, оскільки їх використання пов'язане з потенційним дисбалансом повноважень між державними органами та громадянами, а також із ризиками дискримінації, упередженого ставлення та

порушення процесуальних гарантій. Такі ризики можуть виникати через недостатню якість даних, відсутність прозорості, зрозумілості та належної документації алгоритмів.

Закон ЄС про штучний інтелект [153] охоплює використання штучного інтелекту в правоохоронних органах у двох сценаріях. По-перше, він забороняє використання систем дистанційної біометричної ідентифікації в режимі реального часу в загальнодоступних місцях, окрім випадків, коли це є абсолютно необхідним для досягнення цілей, викладених у ст. 5 (1) літ. d. По-друге, класифікує інші системи штучного інтелекту, що використовуються для цілей правоохоронної діяльності, як високоризикові (ст. 6) та передбачає низку юридичних зобов'язань для їхніх постачальників. Зокрема, пункт 6 Додатка III до цього Закону вводить типологію високоризикових автоматизованих правоохоронних органів, включаючи системи штучного інтелекту, призначені для використання:

– для індивідуальної оцінки ризику фізичних осіб з метою оцінки ризику (рецидиву) правопорушень або ризику для потенційних жертв кримінальних правопорушень (пункт a);

– як поліграфи та аналогічні інструменти або для виявлення емоційного стану фізичної особи (літеру b);

– для виявлення глибоких фейків (літеру c);

– для оцінки достовірності доказів під час кримінального розслідування або кримінального переслідування (пункт d);

– для прогнозування (повторного) скоєння фактичного або потенційного злочину на основі профілювання фізичних осіб (стаття 3 (4) Директиви ЄС 2016/680) або оцінки рис особистості та характеристик чи минулої злочинної поведінки фізичних осіб та груп (літера e);

– для профілювання фізичних осіб під час розкриття злочинів, розслідування або кримінального переслідування (пункт f);

– для аналізу злочинів щодо фізичних осіб, надання правоохоронним органам можливості шукати складні пов’язані та непов’язані між собою великі набори даних, доступні в різних джерелах даних або в різних форматах даних, з метою виявлення невідомих закономірностей або виявлення прихованих зв’язків у даних (літера g).

Таким чином, автоматизовані програми правоохоронних органів мають відповідати певним вимогам, перш ніж їх можна буде розмістити на ринку або використовувати в ЄС. Зокрема, ці вимоги включають створення, впровадження, документування та підтримку системи управління ризиками, використання високоякісних наборів даних для навчання, валідації та тестування, технічну документацію, яка дає змогу оцінити відповідність системи штучного інтелекту вимогам, викладеним у Законі ЄС про штучний інтелект (ст. 11), можливості реєстрації, дизайн, що забезпечує інтерпретацію системи (ст. 13) та захист людського контролю (ст. 14), точність, надійність, кібербезпека (ст. 15). Це значні запобіжні заходи, які гарантують, що системи штучного інтелекту, які використовуються в правоохоронних органах, не сприяють упередженню чи дискримінації щодо певних осіб чи груп, є прозорими та справедливими та не завдають шкоди. У цьому сенсі ці вимоги є важливим кроком до забезпечення того, щоб автоматизовані додатки правоохоронних органів використовувалися відповідально та етично [199]**.** Вважаємо за доцільне врахувати цей європейський досвід при подальшій розрозбці та формування нормативної бази застосування ШІ в діяльності правоохоронних органів України.

У 2019 році міністри юстиції та внутрішніх справ ЄС доручили Європолу створити Лабораторію інновацій для підтримки правоохоронного співтовариства в галузі інновацій. Лабораторія спрямована на виявлення, просування і розробку конкретних інноваційних рішень на підтримку оперативної роботи держав-членів ЄС. Вони допоможуть слідчим і аналітикам максимально використовувати можливості, що надаються новими технологіями, щоб уникнути дублювання роботи, створити синергетичний ефект і об'єднати ресурси. Діяльність Лабораторії безпосередньо пов'язана зі стратегічними пріоритетами,

викладеними в Стратегії Європолу 2020+, в якій йдеться про те, що Європол має бути на передньому краї інновацій і досліджень у сфері правоохоронної діяльності.

Європейська клірингова рада з «Інструментів, методів та інновацій у сфері технічної підтримки операцій і розслідувань» (EuCB) була створена главами національних підрозділів Європолу (HENUs) на їхній зустрічі 5 листопада 2020 року. Вона складається з єдиних контактного центру (SPoCs) з Інноваційної лабораторії Європолу, всіх держав-членів ЄС і чотирьох країн, асоційованих із Шенгенською зоною. SPoCs регулярно зустрічаються на пленарних засіданнях, під час яких вони інформують один одного про інноваційні проєкти та інструменти й ухвалюють рішення про нові спільні заходи зі співробітництва.

Стратегічна група з технологій та етики була заснована 2021 року під егідою EuCB. Наразі до групи входять представники Австралії, Нідерландів, Норвегії, Словенії, Іспанії, Швеції та Великої Британії. Однією з цілей групи було створення справжніх керівних принципів «Оцінка технологій у правоохоронній діяльності: метод етичного прийняття рішень» для користі всіх членів EuCB [200]. Результати їх роботи, з деякими доповненнями викладені в *Таблиці 3.1*.

Таблиця 3.1

Оцінка технологій у правоохоронній діяльності: метод етичного прийняття рішень

№	Вид технології	Проблематика застосування	Висновки та шляхи вирішення
1.	**Технологія відеоаналітики** (доповнює існуючі можливості відеоспостереження, для пошуку певних об'єктів, осіб за описом, транспортних засобів тощо більш ефективно, ніж за допомогою поточного ручного аналізу. Технологія не передбачає розпізнавання/співставлення облич)	Баланс між правом людини на приватність проти занепокоєння щодо широкомасштабного моніторингу поведінки громадян поведінки громадян у громадських місцях	Запровадити відеоналатки тільки після періоду залучення громадськості, лише для визначених випадків використання та зі схвалення вищого керівництва (за умови, що громадськість значною мірою підтримує цю технологію)

2.	**Аналіз моделі відкритого коду збирання даних.** Часто крадуть електроінструменти перепродані на онлайн-ринках.	Чи є допустимим автоматизований аналіз інтернет-торгівлі з використанням інструментів «скрапінга»?	Оскільки автоматизовані розслідування порушують умови обслуговування, вилучення даних з відкритих джерел є неприйнятним.
3.	**Автоматизований аналіз великих та складних наборів даних.** Розглядає низку проблем, пов'язаних з аналізом великих та складних наборів даних.	Аналіз великих та складних наборів даних вразливий до зміни функцій, чутливої комбінації джерел та еволюції даних.	Прийнятно як щось середнє між «все дозволено» та «заборонено». Потрібні різні заходи в залежності від конкретної технології.
4.	**Вимірювання ризику повторного вчинення правопорушення у випадках ґендерного насильства.** Для вимірювання ризику використовується ШІ, але завжди проводиться людська перевірка навченим персоналом.	Проблеми прозорості, викликані побоюваннями щодо надійності, зрозумілості та справедливості.	Правильна розробка з багатьма випробуваннями та одночасним використанням з поточною системою. Прозоро взаємодіючи з громадськістю, вважається найкращим рішенням.
5.	**Використання чат-бота для запобігання сексуального насильства над дітьми.** Чат-бот виявляє сексуалізовану мову, вказує вік та стать, виконує аналіз настроїв та виявляє лінгвістичні відбитки, дозволяючи людині-оператору втрутитися.	Ризик надмірного спостереження як і всі дані чату на форумі оброблені. Тестування в реальному житті проблематично. Існує також проблема чорного ящика глибоке навчання.	Допустима обмежена версія чат-бота з великим віковим порогом (різницею у віці між співрозмовниками).

25 січня 2008 року Парламентською асамблеєю Ради Європи була прийнята резолюція щодо «Відеоспостереження в публічних місцях». Даною резолюцією передбачено, що в країнах-членах Ради Європи на законодавчому рівні необхідно врегулювати питання застосування систем відеоспостереження в публічних місцях і, зокрема, визначити механізми і поняття щодо:

– збирання, обробки і збереження даних, отриманих під час відеоспостереження;

– суворого врегулювання використання технічних можливостей з певними далекосяжними аспектами безперервного спостереження;

– визначення обмежень для встановлення устаткування і програмного забезпечення з функціями збільшення зображення з огляду на конкретне місце;

– законодавчого визначення поняття «приватні зони» і виключення їх з відеоспостереження за допомогою спеціалізованого програмного забезпечення;

– практики декодування записів відеоспостережень;

– прав громадян знати про прохід через зону відеоспостереження і мати доступ до всіх записів із своїм зображенням.

В більшості країн Європи питання впровадження, експлуатації, використання систем відеоспостереження врегульовано як технічними документами, так і законодавчими актами (Законами та інш.), які спираються на чисельні документи Європейського Парламенту, такі як:

– Правила (ЄС) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016р. «Про захист фізичних осіб стосовно обробки персональних даних та про вільне переміщення таких даних»;

– Директива (ЄС) 2016/680 Європейського Парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб у зв’язку з обробкою персональних даних компетентними органами з метою запобігання, розслідування, виявлення або кримінального переслідування правопорушень або виконання кримінальних покарань, а також щодо вільного переміщення таких даних і скасування Рамкового рішення Ради 2008/977/JHA;

– Конвенція Ради Європи №108 «Про захист осіб у зв’язку з автоматизованою обробкою персональних даних», яка ратифікована Законом України від 06.07.2010р. №2438-VI;

– Керівні принципи щодо захисту осіб відносно збору та обробки даних засобами відеоспостереження, які затверджені Європейським Комітетом з питань правової співпраці (ЄКПС) Ради Європи на 78-их зборах 20-23 травня 2003р.;

– Керівні принципи 3/2019 щодо обробки персональних даних за допомогою відеопристроїв, версія 2.0, прийняті 29 січня 2020 року Європейська рада із захисту даних (2020).

До прийняття Закону про штучний інтелект законодавство, політика та керівні принципи Європейського Союзу вже були орієнтовані на значне обмеження використання FRT у поліцейських і безпекових контекстах. Закон про ШІ з одного боку прояснює і конкретизує деякі аспекти, але також залишає значну свободу дій щодо розгортання FRT. Так, Закон про штучний інтелект визнав підстави використання FRT, які обговорювались вище, і вказав, що перевірка за допомогою FRT не вважається забороненою або високою небезпекою якщо «…системи штучного інтелекту, призначені для використання для біометричної перевірки, яка включає автентифікацію, єдиною метою якої є підтвердження того, що конкретна фізична особа є особою, за яку вона себе видає, і підтвердити особу фізичної особи з єдиною метою отримання доступу до послуги, розблокування пристрою або мати безпечний доступ до приміщень» (Закон ЄС про AI 2024, Декларативна частина»).

Переходячи до більш дискусійного питання біометричної ідентифікації в реальному часі (яка включає в себе FRT у прямому ефірі), попередня позиція Європейського Союзу була доволі стриманою щодо використання цієї технології. Наприклад, у «Керівних принципах 05/2022 щодо використання технології розпізнавання обличь у сфері правоохоронних органів» від 26 квітня 2023 року позиція Європейської Ради із захисту даних звучить таким чином: «дистанційна біометрична ідентифікація осіб у загальнодоступних місцях створює високий ризик втручання в приватне життя людей і не має місця в демократичній державі. суспільство, оскільки за своєю природою воно передбачає масове спостереження». У абзаці 73 зазначалось, що обробка даних є виключно необхідною тільки якщо альтернативні методи неможливі або були вже використані і повинні бути розглянуті (у параграфі 51) до прийняття рішення про використання FRT. Рада також підкреслила жахливий ефект масового стеження. Зокрема вони розрізняють терміни: «необхідна обробка», «сувора необхідність»,

«вкрай необхідна» тощо. Так, у сфері захисту персональних даних у правоохоронних цілях стаття 10 (1) Директиви «Про захист персональних даних» встановлює, що використання FRT повинно бути «суворо необхідним». Згідно зі статтею 29, це означає «передбачити точні та особливо вагомі обґрунтування для обробки таких даних». Отже, стаття 29 підкреслила різницю між вимогами необхідності, що містяться у статті 8(1) Директиви та вимогою суворої необхідності, викладеною у статті 10 Директиви. Згідно з останньою вимогою, необхідно продемонструвати, що мета обробки таких чутливих даних (у нашому випадку розслідування злочинів і застосування кримінального законодавства) не може бути досягнута менш інтрузивними заходами з точки зору основоположних прав людини.

Пропорційність також є виміром необхідності: FRT слід обирати, лише якщо мета не може бути розумно досягнута іншими засобами, які менш втручаються в основні права та свободи суб'єкта. Зрештою, має бути справедливий баланс між індивідуальними правами та цільовою метою [201].

Попередні версії тексту Закону про штучний інтелект мали більш обмежувальний підхід до розгортання FRT. Коаліція із 120 правозахисних груп у всьому Європейському Союзі рішуче виступала за повну заборону FRT, зокрема автоматизованого FRT у реальному часі (Організації громадянського суспільства 2021). Але остаточний текст відступив від цієї більш обмежувальної позиції. Дистанційна біометрична ідентифікація в реальному часі (зокрема FRT) буде дозволена з метою контролю та безпеки, але лише за суворих і вузько визначених умов, які включають попередній дозвіл і вимоги сповіщати та записувати використання. Використання повинно бути «суворо необхідним для досягнення суттєвих суспільних інтересів, важливість яких переважає ризики» (пункт 33 статті). Дозволеними умовами є:

– розшук окремих жертв злочинів, у тому числі зниклих безвісти;

– такі ситуації, як загрози життю чи фізичній безпеці фізичних осіб або терористичний напад;

– локалізація або ідентифікація осіб підозрюваних, звинувачених у злочинах, які караються триманням під вартою понад чотири роки, що включає низку перелічених злочинів, що завдають великої шкоди, таких як тероризм і сексуальна експлуатація дітей (Закон про AI ЄС 2024: Додаток II).

Крім того, згідно з Директивою (ЄС) 2016/680 Європейського Парламенту та Ради від 27 квітня 2016 року [146] (див. також статтю 5/1 GDPR), органи влади зобов'язані інформувати громадян про те, що вони підпадають під FRT і про пов'язані з цим ризики [202]. Право бути поінформованим є необхідною умовою для реалізації інших прав, таких як право запитувати доступ до збережених даних, право вимагати їх видалення або виправлення і право подати скаргу до наглядового органу та отримати ефективний засіб правового захисту. З огляду на право бути поінформованим, особи, які відстежуються за допомогою FRT, повинні бути попереджені про використання FRT і конкретні місця, де розташовані камери. Якщо це неможливо – наприклад, через таємницю, необхідну для деяких кримінальних розслідувань – особи повинні бути проінформовані *постфактум.* Щоб захистити поточні розслідування, слід запровадити механізми обмеження права на отримання інформації в певних ситуаціях, оскільки правоохоронним органам іноді доводиться розвивати свою роботу в таємниці, щоб зберегти кримінальні докази [145]. Українське законодавство, в свою чергу, встановлює підстави обробки персональних даних без згоди суб'єкта персональних даних лише як виключення з загального правила без конкретизації умов і обґрунтованості таких дій.

Відповідно до Директиви (ЄС) 2016/680: «Порушення персональних даних, якщо його не усунути належним чином і своєчасно, може призвести до фізичних, матеріальних або нематеріальних збитків для фізичних осіб, таких як втрата контролю над їхніми персональними даними або обмеження їхніх прав, дискримінація, крадіжка особистих даних або шахрайство, фінансові збитки, несанкціоноване скасування псевдонімізації, шкода репутації, втрата конфіденційності персональних даних, захищених професійною таємницею, або будь-яка інша значна економічна чи соціальна невигідність зацікавленій фізичній

особі» [146]. Завдяки масовому невибірковому нагляду за допомогою відеоспостереження в громадських місцях немає анонімності. Кожна людина може стати підозрюваною і навіть випадкова поведінка (наприклад, носіння великих сонцезахисних окулярів, ховання обличчя або погляд в землю) може вважатися підозрілою. З цього приводу Європейська мережа, спрямована на захист прав і свобод в Інтернеті (EDRI) висловилась наступним чином: «Захід, який передбачає постійне спостереження в режимі реального часу, особливо пов'язане з обробкою конфіденційних даних спеціальної категорії, таких як біометричні дані обличчя, у загальному або невибірковому порядку, сам по собі порушує суть основних прав, таких як приватність, гідність, свободу вираження думок і свободу асоціацій і, таким чином, буде несумісним із законодавством ЄС (…) Масове стеження за своєю природою є фундаментальним порушенням основних прав: це зазіхає на саму суть конфіденційності, захисту даних та інших прав» [203]. З цих причин втручання в конфіденційність, які впроваджують (або можуть перерости в) масове стеження, неодноразово відхилялися в ЄС.

Закон про штучний інтелект ЄС також ретельно розрізняє живу біометричну ідентифікацію від ретроспективних систем, щоб запобігти підриву правил. У ньому зазначено (у параграфі 17), що системи «в реальному часі» включають використання «живого» або «майже живого» матеріалу, такого як відеоматеріал, згенерований камерою або іншим пристроєм із подібними функціями. У випадку з «поштовими» системами, на відміну від цього, біометричні дані вже зібрано, і відбувається порівняння та ідентифікація. Це включає дані, зібрані з «обмеженими короткими затримками» (стаття 3) [42]. Крім того, остаточний текст Закону про ШІ також дозволяє поліції та службам безпеки використовувати біометричну ідентифікацію в контексті безпеки кордону та надання притулку, зокрема, якщо особа відмовляється бути ідентифікованою або не може ідентифікувати себе (пункт 33). Консультативний комітет Конвенції про захист осіб щодо автоматизованої обробки персональних даних висуває відповідний результат використання технології FRT як критерій для встановлення різних часових рамок для зберігання шаблонів, отриманих у результаті громадського

спостереження (так зване неконтрольоване середовище). Відповідно до цього критерію, якщо збігів немає, біометричні шаблони людей, що проходять повз, повинні бути автоматично знищені при негативному результаті; навпаки, якщо є збіг, біометричний шаблон може зберігатися протягом періоду, строго необхідного для проведення відповідного поліцейського розслідування [204].

Що стосується параметрів баз даних еталонних зображень, системи штучного інтелекту, які «створюють або розширюють бази даних розпізнавання обличь за допомогою нецільового копіювання зображень обличь з Інтернету або записів із камер відеоспостереження», заборонені через можливість «грубих порушень» конфіденційності [153].

Хоча Закон про ШІ надав більш чіткого нормативного режиму для використання FRT у поліцейській діяльності та безпеці в законодавстві Європейського Союзу, у правовому полі все ще існує значна невизначеність щодо того, як будуть реалізовані винятки з нього. В першу чергу це стосується питань захисту прав на приватне життя та свободу вираження поглядів. В теперішній час країни-члени все ще вирішують питання чи почати використовувати або продовжувати використовувати ці технології. Очевидно, що сфера і межи застосування цих технологій суттєво відрізнятимуться як між державами-членами Європейського Союзу, так і в межах цих юрисдикцій.

Останнім викликом для поліції та безпекових структур є те, що застосування штучного інтелекту у сфері оборони, військових операцій і національної безпеки повністю виключено з-під дії регулювання Закону ЄС про штучний інтелект. Сфера оборони та діяльність збройних сил не регулюється цим законом як частина ширшого підходу ЄС до цих галузей, натомість їхнє використання визначається нормами міжнародного публічного права. Питання національної безпеки належить до виключної компетенції держав-членів, що і стало підставою для виключення. Основна складність у реалізації полягає в тому, що межа між національною безпекою та правоохоронною діяльністю часто є нечіткою, особливо у контексті боротьби з тероризмом, кіберзлочинністю, фінансовими злочинами, відмиванням коштів та транснаціональною організованою

злочинністю. Хоча в Законі прямо зазначено, що оборонні та військові технології, які використовуються у правоохоронних чи інших цілях – постійно або тимчасово – підпадають під його дію, на практиці це дуже важко проконтролювати. Наприклад, у Законі зазначено, що правоохоронна діяльність включає «захист і запобігання загрозам громадській безпеці» (стаття 3), що на практиці майже неможливо чітко відмежувати від функцій систем національної безпеки спостереження [205].

Отже, європейське законодавство щодо меж і стандартів використання ШІ у правоохоронній сфері знаходиться в процесі становлення. Водночас, необхідно зазначити, що дослідження динаміки та змісту наукових публікацій за 2021-1023 рр. у ЄС за напрямом «Соціальні, економічні та екологічні виміри ШІ» свідчить про зростання наукової активності, що корелює з посиленням значення првової визначеності принципів ШІ, розвитком цифрового врядування та реалізацією Цілей сталого розвитку ООН. Проблематика сталості й цифровізації формує концептуальний зв'язок між правовими та технологічними дослідженнями, акцентуючи увагу на інтеграційному характері розвитку і регулювання штучного інтелекту. Зазначена тенденція підтверджує припущення про те, що правовий дискурс ШІ функціонує в межах сталої міждисциплінарної парадигми, яка поєднує правові, технологічні, етичні, соціальні та управлінські аспекти його регулювання і є надзвичайно актуальною для європейського регіону [206].

3.2 Аналіз міжнародного досвіду використання інформаційно-комунікаційних технологій в правоохоронній сфері та перспективи його впровадження в Україні

Сучасні тенденції цифрової трансформації свідчать про стрімке зростання ролі штучного інтелекту та інформаційно-комунікаційних технологій у правоохоронній діяльності, що зумовлює необхідність вивчення зарубіжного досвіду їх упровадження. У контексті глобалізації злочинності – кіберзлочинів, тероризму, відмивання коштів, торгівлі людьми та інших транснаціональних

загроз – правоохоронні органи різних держав дедалі активніше інтегрують інтелектуальні системи в аналітичну, оперативно-розшукову та управлінську діяльність.

Використання ШІ у провідних країнах світу охоплює широкий спектр напрямів – від прогнозування злочинності та аналізу великих масивів даних до автоматизації процесів розслідування, цифрової криміналістики та підвищення ефективності адміністративного управління. Такі технології забезпечують своєчасне виявлення загроз, оптимізацію ресурсів і зменшення ризику людських помилок у прийнятті рішень.

Разом із тим, активне впровадження ШІ у правоохоронну сферу вимагає належного правового регулювання. Без чітко визначених міжнародних і національних норм виникають ризики зловживань, порушення прав людини, непрозорості алгоритмів і невизначеності правової відповідальності. Саме тому вивчення досвіду зарубіжних країн і міжнародних правоохоронних організаій є надзвичайно важливим для України – воно дозволяє адаптувати найкращі практики, уникнути системних помилок і сформувати ефективну модель використання ШІ у правоохоронній діяльності на засадах законності, етики та підзвітності.

Ключову роль у впровадженні інновацій у сфері міжнародного правопорядку та боротьби з транснаціональною злочинністю відіграє Інтерпол (International Criminal Police Organization, ICPO) – міжнародна організація, основним завданням якої є організація широкої співпраці між органами кримінальної поліції держав-учасниць з метою попередження злочинності та боротьби з нею. Як найбільша у світі міжурядова правоохоронна організація, що об’єднує 195 країн, Інтерпол виступає платформою для обміну технологіями, найкращими практиками та координації дій між правоохоронними органами різних держав.

У сфері інновацій Інтерпол активно впроваджує сучасні інформаційно-комунікаційні технології, включаючи штучний інтелект, аналітику великих даних, біометричні системи та кібермоніторинг. Через такі ініціативи, як I-24/7 –

глобальну систему комунікації для обміну кримінальною інформацією в реальному часі, або бази даних з розшуку осіб, викрадених документів і зброї, – Інтерпол забезпечує оперативне реагування на загрози [207].

Інтерпол також бере участь у розробці стандартів етичного використання новітніх технологій, організовує міжнародні тренінги, форуми з кібербезпеки та інновацій, підтримує національні правоохоронні органи в адаптації до цифрової трансформації. Завдяки цьому організація не лише сприяє технологічному прогресу в галузі безпеки, а й зміцнює глобальну правову співпрацю та стійкість до нових форм злочинності.

Україна, як самостійна держава, офіційно подала заявку та вступила до Інтерполу в 1992 році, а от українські правоохоронці почали працювати з Міжнародною організацією кримінальної поліції ще з часів СРСР. Статус Національного центрального бюро Уряд визначив у Постанові від 25.03.93 № 220. Як Укрбюро тоді виступило Міністерство внутрішніх справ (сьогодні – Нацполіція).

На офіційній сторінці Інтерполу сказано, що: «ІНТЕРПОЛ бере участь у кількох проєктах, пов’язаних із законодавством про інформацію, комунікації та технології, починаючи від електронних доказів і Darknet до інструментів розпізнавання голосу. Наша роль полягає в тому, щоб забезпечити врахування потреб правоохоронних органів і їх інтеграцію в рішення, а також те, що правила та норми Інтерполу відображають технологічні зміни в глобальній правоохоронній діяльності» [207].

ІНТЕРПОЛ брав участь у проектах, які отримали фінансування в рамках програми Європейського Союзу «Горизонт 2020», «Правосуддя» та «Сьомої рамкової програми» для досліджень, технологічних розробок та демонстрації:

– «ТИТАН». Цей проект досліджував і розробляв інструменти для дослідження транзакцій віртуальної валюти на підпільних ринках;

– «EVIDENCE2e-CODEX». Дослідницький проект з обміну цифровими доказами в межах Європейського Союзу через e-CODEX у рамках Європейського розслідування та процедур взаємної правової допомоги;

– Інтегрований проект ідентифікації мовця (SIIP) – розробив нову технологію, яка допомагає правоохоронним органам ідентифікувати голоси невідомих осіб, враховуючи поточні закони про конфіденційність і захист даних;

– MAPPING (Управління альтернативами для картографування конфіденційності, власності та управління Інтернетом). Проект слугував форумом для експертних дискусій щодо економічних, соціальних, правових та етичних аспектів поточних подій в Інтернеті з акцентом на управління, права людини (включно з конфіденційністю та захистом даних та інтелектуальну власність;

– Європейська інформаційна система обміну даними для судів і доказів (EVIDENCE) – забезпечила спільну правову основу для систематичного та однакового застосування нових технологій у зборі, використанні та обміні доказами;

– Масштабована міра для технологій автоматизованого розпізнавання (SMART). В епоху експоненційного розвитку інтелектуальних технологій відеоспостереження, які вимагають ефективної законодавчої бази, проект SMART підготував проект модельного закону, який відображає потреби зацікавлених сторін у балансі з правами громадян;

– Правила, очікування та безпека завдяки зручним технологіям із покращеною конфіденційністю (RESPECT). Спираючись на висновки проекту SMART, проект RESPECT розширив сферу правових досліджень на ряд сфер, таких як системи відеоспостереження, моніторинг соціальних мереж і автоматизовані системи відстеження фінансових рухів.

Насьогодні Інтерпол працює над проектом ROXANNE (Аналітика мережі, тексту та мовлення в режимі реального часу для боротьби з організованою злочинністю) – виявлення злочинців шляхом поєднання мовних технологій з аналізом мережі. ROXANNE прагне ефективно ідентифікувати та відслідковувати злочинців за допомогою мови, тексту та відеоданих у поєднанні з аналізом організованих злочинних мереж. Кінцевим продуктом стане передова технічна платформа, яка використовує нові інструменти для розкриття та

відстеження організованих злочинних мереж, підкріплена міцною правовою базою [208].

Для України цей досвід є цінним у контексті модернізації інформаційно-аналітичних систем правоохоронних органів, зокрема у сфері ідентифікації злочинців, обміну доказами та боротьби з організованою злочинністю. Можливість українських правозахисників використовувати ресурси ІНТЕРПОЛУ передбачено в Інструкції «Про порядок використання правоохоронними органами України інформаційної системи Міжнародної організації кримінальної поліції – Інтерпол», затвердженої спільним наказом Міністерства внутрішніх справ України, Офісу Генерального прокурора, Національного антикорупційного бюро України, Служби безпеки України, Державного бюро розслідувань, Міністерства фінансів України, Міністерства юстиції України 17 серпня 2020 року № 613/380/93/228/414/510/2801/5 [209]. Така співпраця сприятиме створенню національної інфраструктури, здатної забезпечити оперативну взаємодію з міжнародними структурами й підвищити ефективність розслідувань.

Окрім міжнародних організацій і інституцій цікавим буде вивчення досвіду правового забезпечення впровадження і використання ІКТ правоохоронними органами окремих країн.

Великий інтерес викликають нормативні розробки в сфері ШІ у Сполучених Штатах Америки. У жовтні 2022 року Управлінням наукової та технологічної політики Білого дому опублікувало проєкт Білля про права у сфері штучного інтелекту (Blueprint for an AI Bill of Rights) [210]**.** Білль спрямований на захист і збереження фундаментальних прав громадян США у світлі прогресу, досягнутого в усьому світі штучного інтелекту. Основна мета Білля про права на штучний інтелект полягає в тому, щоб структура та функції демократії в США залишалися надійними, стійкими та ефективними в майбутньому, керованому ШІ. У цьому відношенні ініціатива окреслює п’ять основних принципів, які включають безпечні та ефективні системи, алгоритмічний захист від дискримінації, конфіденційність даних, право на повідомлення та пояснення, а

також людські альтернативи, розгляд і резервний варіант. Документ є правовою основою діяльності державних органів, поліції і судової системи при захисті прав громадян у сфері ШІ.

30 жовтня 2023 року Президент США підписав Виконавчий наказ про безпечну, захищену та надійну розробку та використання штучного інтелекту. У документі йдеться про захист конфіденційності, встановлення нових стандартів безпеки ШІ, гарантування прав споживачів і працівників, встановлення справедливості та підтримки громадянських прав, сприяння інноваціям і конкуренції: «(f) Конфіденційність і громадянські свободи американців повинні бути захищені, оскільки ШІ продовжує розвиватися. Штучний інтелект полегшує вилучення, повторну ідентифікацію, зв'язування, висновки та дію на основі конфіденційної інформації про особистість людей, місце розташування, звички та бажання. Можливості штучного інтелекту в цих сферах можуть збільшити ризик того, що персональні дані можуть бути використані та розкрити. Для боротьби з цим ризиком федеральний уряд гарантуватиме, що збір, використання та зберігання даних є законним, безпечним і зменшує ризики конфіденційності та конфіденційності. Агенції повинні використовувати доступні політичні та технічні інструменти, у тому числі технології підвищення конфіденційності (PET), де це доцільно, для захисту конфіденційності та боротьби з ширшими правовими та суспільними ризиками, включаючи обмеження прав за Першою поправкою, які є результатом неналежного збору та використання дані людей» [211]. Також в Наказі наголошується, що: «…безвідповідальне використання ШІ може поглибити дискримінацію, упередженість та інші зловживання у сфері правосуддя, охорони здоров'я та житла». Щоб переконатися, що ШІ сприяє справедливості та громадянським правам, наказ передбачає:

– щоб уникнути використання алгоритмів ШІ для посилення дискримінації необхідно розробити і надати федеральним програмам пільг і федеральним підрядникам чітких інструкцій;

– для розв’язання проблеми алгоритмічної дискримінації у результаті машинного навчання, розробити механізми технічної допомоги та координації між відомствами;

– для забезпечення справедливості у всій системі кримінального правосуддя вироблення алгоритмів використання ШІ в процесі досудового звільнення, тримання під вартою, винесення вироків, умовно-дострокового звільнення та умовного засудження, тощо [212].

На нашу думку важливою новацією вказаного документу, яку необхідно взяти до уваги українському законодавцю є доручення держорганам розробити систему стандартів, інструментів та тестів, щоб переконатися, що системи ШІ безпечні та надійні.

11 травня 2017 року Президент США видав указ, спрямований на посилення кібербезпеки федеральних мереж і критичної інфраструктури з метою встановлення «більш узгодженого підходу до того, як федеральний уряд реагує на кіберризики». Наказ вимагає від усіх федеральних відомств використовувати структуру, розроблену Національним інститутом стандартів і технологій для покращення критичної кібербезпеки [213].

Крім того, Сполучені штати Америки мають непоганий досвід застосування технологій ШІ у практичній поліцейській діяльності. Наприклад, застосування ШІ-транскрипції проходить апробацію протягом кількох років. Зокрема, використання систем штучного інтелекту для складання поліцейських звітів дозволило виявити як позитивні, так і проблемні аспекти її функціонування. До позитивних належать підвищення оперативності обробки даних і зменшення навантаження на працівників поліції. Водночас було зафіксовано випадки маніпулювання записами з боді-камер, використання неповних або викривлених даних під час формування звітів, що поставило під сумнів достовірність і легітимність створених документів [214].

Реакцією на зазначені виклики стало прийняття нормативних обмежень, спрямованих на підвищення прозорості та підзвітності у використанні ШІ-документів. Так, у штаті Юта було ухвалено Закон SB 524 [215], підписаний

губернатором Гевіном Ньюсомом, який встановлює вимогу маркування всіх поліцейських звітів, створених за допомогою штучного інтелекту, відповідним позначенням. Крім того, закон зобов'язує правоохоронні органи вести аудиторський журнал, у якому фіксується особа, що використовувала ШІ для підготовки звіту, а також усі аудіо- та відеоматеріали, застосовані в процесі його створення. Законодавець також визначив обов'язок зберігати первинну версію звіту, сформовану за допомогою ШІ, протягом усього періоду зберігання офіційного документа та заборонив вважати таку чернетку офіційною заявою поліцейського.

Ще одна цікава технологія яка випробовується в американських поліцейських департаментах – це «біометрична зброя». Однією з можливих переваг біометричної зброї є підвищення безпеки офіцерів оскільки стріляє, лише якщо його тримають запрограмовані користувачі. Експерти вважають що це може значно зменшити кількість випадків використання вогнепальної зброї офіцерів проти них самих. Біометрична зброя створена для ідентифікації ексклюзивного відбитка пальця або долоні авторизованого користувача та запобігання несанкціонованим користувачам стріляти зі зброї. Це може зменшити небезпеку використання злочинцями вилученої або конфіскованої зброї проти поліції чи населення [216]. Разом з цим, поки що біометрична зброя має деякі технічні та експлуатаційні проблеми, що може вплинути на безпеку правоохоронця. Однією з головних проблем є надійність і точність біометричної технології, яка може не розпізнати авторизованого користувача через бруд, піт, кров, рукавички або інші фактори, які впливають на якість біометричного сканування. Це може поставити під загрозу життя поліцейського, якщо йому знадобиться використати свію зброю у швидкій ситуації.

Ще одна проблема – сумісність біометричної зброї між офіцерами. У деяких ситуаціях їм може знадобитися обміняти або позичити вогнепальну зброю у своїх партнерів чи колег у надзвичайних ситуаціях. Біометрична зброя не пристосована для таких обмінів, якщо для кожної одиниці не буде дозволено

кілька авторизованих користувачів. Однак це може послабити безпеку та підзвітність біометричної системи.

Не дивлячись на те, що ЄС та США є регіональними лідерами в сфері нормативного регулювання ШІ, першою країною у світі, яка створила Національну стратегію ШІ на урядовому рівні була Канада (Панканадська стратегія ШІ оприлюднена у 2017 році). Ця стратегія являє собою п'ятирічний план фінансування досліджень та пошуку талантів для цієї галузі. Окрім того, держава є співзасновником Глобального партнерства з ШІ. У розвиток положень Панканадської стратегії ШІ у 2019 році створено Консультативну раду уряду Канади з питань ШІ. Канада прийняла Закон «Про штучний інтелект і дані» (AIDA) як частину законопроекту С-27 [217], а також Закон «Про впровадження цифрової хартії» у 2022 році. Це дозволило закласти основу для відповідального проектування, розробки та розгортання систем ШІ, гарантувати безпеку і недискримінаційність систем штучного інтелекту.

Подібно до Закону ЄС про штучний інтелект, Канадський Закон С-27 також встановлює класи систем штучного інтелекту, які вважаються системами високого впливу. Зокрема, до них відносяться:

– прийняття рішень судами або адміністративними органами: цей клас включає системи штучного інтелекту, які використовуються судами або адміністративними органами для прийняття рішень щодо осіб у судових або адміністративних процедурах. Мета полягає в тому, щоб запобігти упередженням у цих системах, які можуть мати серйозні наслідки для прав особи та доступу до правосуддя;

– правоохоронна діяльність: цей клас охоплює системи штучного інтелекту, які використовуються офіцерами в правоохоронних цілях. Враховуючи значний вплив поліцейської діяльності на окремих осіб і громади, уряд підкреслює, що існує зацікавленість у тому, щоб ці системи були недискримінаційними, безпечними та ефективними.

Додаючи нові класи систем із високим ступенем впливу, уряд (Рада губернатора) має враховувати тяжкість і ступінь потенційного несприятливого впливу, зокрема на права людини та соціальну шкоду [218].

У розробці та впровадженні корпоративної об'єднаної інформаційної моделі даних для потреб поліції, на нашу думку, на особливу увагу заслуговує досвід Сполученого Королівства Великої Британії. Так, з 2013 року до National Crime Agency (NCA) (Національного кримінального агентства) передано інформаційну систему The National Policing Improvement Agency (NPIA). Доступ до неї мають усі територіальні поліцейські сили Великої Британії, поліція Північної Ірландії (PSNI), Британська транспортна поліція (BTP), поліцейська служба Шотландії, Національна служба ідентифікації (NIS), Національне агентство зі злочинності (NCA), Служба безпеки (MI-5) і Секретна розвідувальна служба (MI-6), Асоціація начальників поліції (ACPO) та інші. Зазначена інформаційна система складається з кількох баз даних:

– «Імена», яка містить великий обсяг інформації щодо осіб, засуджених, попереджених або нещодавно заарештованих. Включає дані відбитків пальців та ДНК; фізичні описи; відомості про попередні арешти та вироки, винесені за кожне правопорушення; усі попередні адреси та інше;

– «Автомобіль», яка містить докладну інформацію про зареєстровані автомашини, зокрема номери шасі, двигуна тощо, дані про статус транспортного засобу (викрадений, страховий стан тощо), їхніх власників тощо;

– «Нерухомість», яка містить відомості про сільськогосподарську та будівельну техніку, зареєстрованих тварин, Відомості містять інформацію про проходження тесту, підтвердження та ліцензії. Ця база даних оновлюється щоранку [219].

Національна база даних ДНК кримінальної розвідки Великої Британії National Criminal Intelligence DNA Database (NDNAD) створена 1995 року. Вона перебуває у віданні Міністерства внутрішніх справ Великої Британії. Дані, що містяться в NDNAD, належать поліцейському органу, який надав зразок для аналізу. Зразки зберігаються постійно компаніями, які аналізують їх за щорічну

плату. NDNAD Великої Британії у своєму роді є головною і найбільшою у світі базою даних судових ДНК і містить дані щодо приблизно 10% населення. Дані, що містяться в Національній базі даних ДНК, складаються з даних приватних осіб, відібраних на підставі Закону про поліцію і докази у кримінальних справах, і вилучених за нерозкритими злочинами у вигляді плям (наприклад, від крові, сперми, слини, волосся тощо, що залишилися на місці злочину). Щоразу, коли надходить новий профіль, відбувається автоматичний пошук на збіг серед записів NDNAD між даними фізичних осіб і даними нерозкритих злочинів [197].

Також варто згадати досвід Великої Британії з використання ШІ в роботі органів поліції. Наприклад, ця технологія використовує поліцейський архів, вивчаючи рішення, прийняті працівниками поліції протягом конкретного періоду за аналогічними справами в рамках адміністративних проваджень. А потім оцінює ризики, враховуючи різні фактори, та пов’язує їх з подібними правопорушеннями. Це сприяє оцінці поліцейськими або органами суду доказів і прийнятті процесуального рішення по справі. При цьому поліція регулярно проводить аудит функціонування ШІ і надійність його висновків.

28 вересня 2023 року Ради керівників Національної поліції Великої Британії схвалила Угоду про використання штучного інтелекту (ШІ) в поліцейській діяльності [220]. Цей документ є цікавим для вивчення бо містить визначення і характеристику ШІ, принципи його застосування, розподіл відповідальності і контролю між поліцейськими органами.

Цікавим є досвід англійських правоохоронців щодо використання носимих технологій з елементами ШІ. Так, Ліверпульський центр передових досліджень поліцейської діяльності Ліверпульського університету Джона Мурса протягом трьох років брав участь у інноваційних дослідженнях щодо використання такої технології разом із поліцією Мерсісайду. В липні 2024 року було проведено подовжнє дослідження, у якому взяли участь понад 100 офіцерів і персоналу, які носили браслет Biostrap. Повні результати цього дослідження ще не доступні, але перші ознаки свідчать про те, що 93% учасників вважають, що технологія допомогла підвищити рівень їхньої обізнаності про здоров’я, 82% вважали, що

вона допомогла їм визначити зміну поведінки, а 72% погодилися, що вона призвела до реальних змін для покращення здоров’я та благополуччя [221].

Підхід Великої Британії відрізняється від регулювання, заснованого на ризиках ЄС. Запропонований ЄС Закон про штучний інтелект забороняє певне використання штучного інтелекту, наприклад технологію розпізнавання обличчя в реальному часі, коли люди, показані на каналі камери, порівнюються зі «списками спостереження» поліції в громадських місцях.

Підхід ЄС створює суворі стандарти для так званих систем ШІ високого ризику. До них належать системи, що використовуються для оцінки заявок на роботу, прийому студентів, права на отримання позик і державних послуг.

Підхід Великобританії до регулювання штучного інтелекту складається з трьох ключових компонентів. По-перше, він спирається на існуючі правові рамки, такі як закони про конфіденційність, захист даних і відповідальність за продукт, а не на впровадження нового законодавства, орієнтованого на ШІ. По-друге, документ містить п’ять загальних принципів, кожен із яких складається з кількох компонентів і застосовуватиметься регулятором разом із існуючими законами. Ці принципи: 1) безпека та надійність; 2) відповідна прозорість і можливість пояснення; 3) справедливість; 4) підзвітність і управління; 5) оскарженість і відшкодування. Під час початкового впровадження регулюючі органи не будуть зобов’язані за законом забезпечувати виконання принципів. Закон, що накладає ці зобов'язання, буде прийнято пізніше, якщо це буде визнано за необхідне. Тому очікується, що у першу чергу організації добровільно дотримуватимуться цих принципів [222].

Хоча штучний інтелект приносить численні переваги поліцейській діяльності у Великобританії, він також створює етичні та правові проблеми. Розгортання технологій ШІ викликає занепокоєння щодо конфіденційності, громадянських свобод і упередженості алгоритмів. Критики стверджують, що інтелектуальна поліція та системи розпізнавання облич можуть призвести до дискримінації, особливо відносно меншин. Помилкова ідентифікація за допомогою систем розпізнавання облич викликала дебати щодо точності та

справедливості цих інструментів, деякі вимагають суворіших правил або навіть заборони на їх використання.

У березні 2023 року Управління інформаційного комісара (ICO) оновило свої Посібники щодо штучного інтелекту та захисту даних після запитів підприємців Великобританії щодо роз'яснення вимог до справедливості в штучному інтелекті.

У вересні 2020 року Апеляційний суд постановив, що використання поліцією Південного Уельсу технології розпізнавання облич було незаконним і порушує Європейську конвенцію з прав людини. Це рішення викликало триваючі дискусії про баланс між безпекою та конфіденційністю в епоху цифрових технологій. Тим не менш, поліція Північного Уельсу нещодавно розширила використання технології розпізнавання облич, заявивши, що основне використання цієї технології – «забезпечити безпеку населення» [223].

Протягом останніх п'яти років Управління поліції та боротьби зі злочинністю Вест-Мідлендса (WMOPCC) і Поліція Вест-Мідлендсу (WMP) підтримували інноваційний Комітет з етики даних. Цей міждисциплінарний орган, до складу якого входять незалежні експерти з права, інформатики, етики, соціального впливу та прав жертв, консультує щодо проектування, розробки та розгортання передових інструментів штучного інтелекту та аналітики даних у поліцейській діяльності. Комітет, до складу якого входять незалежні експерти з права, інформатики, етики, соціального впливу та прав жертв, консультує щодо проектування, розробки та розгортання передових інструментів штучного інтелекту та аналітики даних у поліцейській діяльності. Дослідження показало, що робота Комітету не перешкоджає оперативній поліцейській діяльності, а радше підтримує її, що призвело до більш відповідального та етичного використання ШІ. Було зроблено висновок, що такий незалежний контроль може слугувати моделлю для відповідального використання ШІ по всій країні [224].

В свою чергу, у 2018 році Німеччина проявила стратегічне бачення та ініціативу, ставши однією з перших країн, які розробили національну стратегію розвитку штучного інтелекту. Відтоді федеральний уряд цілеспрямовано сприяє

розвитку ШІ з метою посилення як національної, так і європейської конкурентоспроможності, при цьому акцент робиться на людиноцентричному підході – на користь працівників і суспільства загалом. У політиці ШІ особливе місце займають принципи інклюзивного розвитку, прозорості та підзвітності у впровадженні ШІ. Ця стратегія підтримує демократичні цінності та прагне до впровадження надійного й відповідального штучного інтелекту у сфері державного управління. Визнається важливість дотримання високих стандартів щодо недискримінації, прозорості, відстежуваності, справедливості, можливості перевірки, участі та захисту персональних даних – як ключових умов для збереження довіри громадян до використання ШІ у публічному секторі.

Разом із тим уряд розуміє необхідність створення чіткої політики та правового регулювання, які б забезпечували безпечне, етичне та орієнтоване на суспільне благо застосування ШІ, з урахуванням можливих ризиків. При цьому використання ШІ в діяльності правоохоронних органів у Німеччині викликає певні суперечки через потенційні юридичні, етичні та соціально-політичні виклики.

Як і більшість країн, які розробили національну стратегію ШІ, Німеччина включила ШІ в державний сектор як сильний компонент своєї національної стратегії. Федеральний уряд підтверджує свою зацікавленість у використанні ШІ для реагування на надзвичайні ситуації та підтримки внутрішньої та зовнішньої безпеки. Одним із важливих компонентів цього є безпека інформаційних технологій, сфера, у якій федеральний уряд зобов’язується сприяти дослідженням у державному секторі та забезпечувати розвиток належного досвіду для відповідних органів.

Оновлення зазначеної стратегії у 2020 року можна охарактеризувати як рух до загальної розбудови потенціалу в державному секторі. Він також посилив елементи безпеки початкової стратегії, обговорюючи потенціал штучного інтелекту для захисту від кібератак, боротьби з надзвичайними ситуаціями та стихійними лихами, а також спостереження за Землею. Що стосується внутрішньої та зовнішньої безпеки, стратегія 2018 року включала деякі досить

конкретні дії, такі як криміналістика соціальних мереж і кроки для захисту дітей від сексуального насильства в Інтернеті. Оновлення 2020 року запровадило більш конкретні дії, зокрема розширення пов’язаних зі штучним інтелектом можливостей Центрального управління інформаційних технологій у сфері безпеки (ZITiS),

Приклади застосування ШІ в державному секторі Німеччини:

– *датчики освітленості* – відстежують дорожню ситуацію на перехресті. Отримані дані використовуються для керування світлофорами на різних перехрестях. Заявлені результати включають скорочення часу транспортування (на 25%), зменшення забруднення навколишнього середовища та зниження рівня шуму;

– *автоматизоване розпізнавання зображень*. Використовується, щоб відрізнити дитячу порнографію від подібних, але легальних зображень (наприклад, із сімейних свят). Вибрані зображення, позначені як образливі/порнографічні, пересилаються відповідним службам:

– *соціальний моніторинг* (загальнодоступні дані, як-от: новини, звіти неурядових організацій, соціально-економічні показники та кліматичні дані). Данні збираються та проводиться багатофакторний аналіз для оцінки ймовірності виникнення політичних криз (так званий PREVIEW: візуалізація прогнозів і раннє попередження) для прогнозування конфліктів та очікуваних смертельних випадків. Результати передаються до персоналу, який проводить якісне оцінювання.

– *LLM*. Програмне забезпечення, що допомагає державним службовцям аналізувати тексти, оптимізуючи роботу над законопроектами шляхом покращення сумісності. Допомагає у фоновому дослідженні та генерує текст за допомогою людського введення [225].

Правоохоронні органи Федеративної Республіки Німеччина активно використовують телекомунікаційні засоби та запроваджують інноваційні комп'ютерні технології для ефективного та якісного інформаційного забезпечення своєї службової діяльності. Так, наприклад, інформаційно-

пошукова система Федеральної кримінальної поліції – Informationssystem der Polizei (INPOL) включає базу даних усіх осіб, оголошених у розшук, відомості про викрадені автомобілі, документи тощо. Дані щодо осіб, яких розшукує німецька поліція або судові органи, вже за кілька секунд після внесення до бази стають доступними для всіх користувачів зазначеної системи, а це всі відділення поліції та митні органів ФРН.

Франція. У березні 2011 року французький парламент ухвалив закон, спрямований на забезпечення внутрішньої безпеки «Loppsi II», що став основою для модернізації нормативно-правових актів, які стосуються інформаційно-телекомунікаційного забезпечення. Так, під час розслідування злочинів, пов'язаних із дитячою порнографією, поліції надано право підключення до Інтернету та телефонних ліній, а також відслідковувати звернення до провайдерів для фільтрації Інтернет-з'єднання тощо. Також ухваленим законодавчим актом дозволено створення інформаційної платформи, що з'єднує численні державні бази даних, таких як: – «Le fichier judiciaire automatisé des auteurs d'infractions sexuelles ou violentes» (FIJAIS) – автоматизована база даних сексуальних злочинців; база даних іноземців у Франції – L'application de gestion des dossiers des ressortissants étrangers en France (AGEDREF); автоматична інформаційно-пошукова система «Кассіопея» містить інформацію про скарги, зареєстровані суддею під час судового розгляду, про обвинувачених, свідків, потерпілих і цивільних позивачів тощо; автоматизована система ідентифікації відбитків пальців осіб, які вчинили злочини або правопорушення – Système d'identification automatique par empreintes digitales (AFIS).

Також в державі створено Державний автоматизований банк даних судимостей що перебуває у віданні міністра юстиції (Департамент у кримінальних справах і помилувань).

В Австралії було запроваджено низку ініціатив, спрямованих на покращення обміну інформацією та розвідданими між юрисдикціями. Ці ініціативи включають: Австралійську мережу звітності про кіберзлочинність (ACORN); Національну систему кримінальної розвідки (NCIS); проекти, розроблені за

допомогою Data to Decisions Cooperative Research Center (D2D CRC). Прийнято Закони про перехоплення телекомунікацій, які є життєво важливими інструментами для правоохоронних агентств в їх розслідуваннях правопорушень, як онлайн, так і офлайн. Так, Закон про телекомунікації (перехоплення та доступ) 1979 року (Закон TIA) та Закон про пристрої спостереження 2004 року (Закон SD про електронне спостереження) визнають, що правоохоронні та розвідувальні органи повинні мати доступ до комунікацій, якщо виконуються певні попередні умови. У 2015 році Комітет Сенату з юридичних і конституційних справ почув заклики правоохоронних органів реформувати Закон TIA, щоб він адаптувався до технологічного прогресу [226]. У травні 2013 року Об'єднаний парламентський комітет з питань розвідки та безпеки рекомендував «здійснювати перехоплення на основі конкретних атрибутів комунікацій» на основі «існуючих ордерів на перехоплення іменованих осіб».

Показові результати має застосування системи штучного інтелекту «Prometea» у роботі судів та правоохоронних органів (поліції) Аргентини під час здійснення провадження у справах про адміністративні правопорушення та прийняття по ній рішення. Зокрема, система ШІ «Prometea» здатна за 10 секунд винести і оформити судове рішення з ряду категорій адміністративних справ. А отже, можна впевнено казати про ефективність і економічність прийняття процесуальних рішень за допомогою застосування ШІ [227].

Таким чином, законодавче регулювання використання штучного інтелекту у правоохоронній сфері посідає пріоритетне місце в політико-правових стратегіях більшості розвинених держав, що свідчить про усвідомлення потенційних ризиків, пов'язаних із технологічною автономністю таких систем, і необхідність забезпечення ефективного захисту прав людини та громадської безпеки. Незважаючи на відмінності у правових традиціях, держави послідовно прагнуть гармонізувати підходи до правового врегулювання ШІ, орієнтуючись на досягнення балансу між ефективністю правоохоронної діяльності та дотриманням фундаментальних прав і свобод людини. Основоположні принципи

функціонування систем ШІ (недискримінація, прозорість, справедливість, відстежуваність, участь людини та захист персональних даних) набули статусу універсальних і закріплені у нормативних актах більшості країн.

Зарубіжний досвід засвідчує, що результативне використання інтелектуальних технологій у сфері правопорядку можливе лише за умови створення чіткої системи контролю, що включає: етичне регулювання, незалежний аудит алгоритмів, функціонування спеціалізованих органів моніторингу та правового нагляду. У цьому контексті доцільним для України є формування незалежного Комітету з питань штучного інтелекту у правоохоронній сфері, який здійснюватиме експертно-наглядові функції щодо відповідності застосування ШІ міжнародним стандартам прав людини, а також розроблення національних стандартів аудиту алгоритмів і систем ШІ, аналогічних до американської моделі сертифікації безпеки, точності та захисту даних. Такі кроки сприятимуть забезпеченню законності, прозорості та довіри суспільства до процесів цифрової трансформації правоохоронної діяльності в Україні.

Висновки до розділу 3

1. Проведено аналіз законодавства Європейського Союзу в сфері правового регулювання ІКТ і його застосування правоохоронними органами. Виявлено, що інформаційні системи країн Європейського Союзу, як правило, утворені на загальнонаціональному рівні та забезпечують стратегічний аналіз даних, щодо функціонування злочинних угруповань. На центральному рівні ведуться обліки осіб, які вчинили правопорушення, самі злочини, готуються законодавчі пропозиції нормативного урегулювання роботи кримінальної поліції, підтримуються контакти з Інтерполом. Такий розподіл повноважень дозволяє краще спрямовувати та координувати зусилля, враховуючи розширення міжрегіональних та міжнародних контактів, а також міграцію організованих злочинців, що забезпечує більший рівень конспірації при значному вплив

криміналітету на політичні, економічні, а нерідко і правоохоронні структури на місцях, особливо у невеликих містах.

2. Проаналізовано Закон ЄС про штучний інтелект як найповніше у світі законодавство щодо ШІ, орієнтоване на ризики і спрямоване на розвиток інновацій. З'ясовано, що документ класифікує системи штучного інтелекту на основі ризик-орієнтованого підходу та передбачає чотири категорії ризику: неприйнятний, високий, обмежений і мінімальний. Системи ШІ з неприйнятним рівнем ризику заборонені для використання, окрім визначених в законі виключень. Закон забороняє використання систем біометричної ідентифікації в реальному часі правоохоронцями. Системи штучного інтелекту, призначені для правоохоронної діяльності чи здійснення правосуддя, класифікуються як високоризикові згідно з Додатком ІІІ Закону, що передбачає обов'язкове дотримання вимог щодо управління ризиками, тестування, точності, надійності, прозорості, людського нагляду, кібербезпеки та оцінки відповідності. Врахування цього європейського досвіду є доцільним при формуванні нормативної бази застосування ШІ в діяльності правоохоронних органів України.

3. Встановлено, що хоча в ЄС немає спеціального закону, який регулює загальні засади використання ШІ в правоохоронних органах, однак існує кілька законодавчих актів, які регулюють використання окремих технологій ШІ в правоохоронній діяльності. Подальший аналіз еволюції правового регулювання відеоспостереження та біометричної ідентифікації в правоохоронних цілях дає підстави зробити висновок, що сфера і межи застосування цих технологій суттєво відрізнятимуться як між державами-членами Європейського Союзу, так і в межах цих юрисдикцій.

4. Проаналізовано діяльність міжнародної організації ІНТЕРПОЛ в сфері розробки і використання ІКТ для боротьби із злочинністю. Зроблено висновок, що для України цей досвід є цінним у контексті модернізації інформаційно-аналітичних систем правоохоронних органів, зокрема у сфері ідентифікації злочинців, обміну доказами та боротьби з організованою злочинністю. Адаптація таких рішень сприятиме створенню національної інфраструктури, здатної

забезпечити оперативну взаємодію з міжнародними структурами й підвищити ефективність розслідувань.

5. Проаналізовано законодавство щодо застосування ШІ у правоохоронній сфері таких країн, як: США, Канади, Сполученого Королівства Великої Британії, Німеччини, Франції, Австралії та Аргентини.

Зазначено, що новацією законодавства США щодо ШІ, яку необхідно взяти до уваги українському законодавцю є доручення держорганам розробити систему стандартів, інструментів та тестів, щоб переконатися, що системи ШІ безпечні та надійні. Велика Британія при розробці і впровадження нормативних актів щодо використання ШІ поліцейськими спирається на існуючи акти, які забезпечують громадянські права і свободи, отже нові документи повинні узгоджуватись з існуючими стандартами. В свою чергу Канада та країни Європейського Союзу – навпаки, створюють нові стандарти використання ШІ основані на ризиках, тобто класифікації технологій з ШІ в залежності від ступеню його впливу на права і свободи людини.

На основі аналізу міжнародного досвіду використання ШІ у правоохоронній сфері запропоновано створити в Україні незалежний Комітет з питань штучного інтелекту, який здійснюватиме експертно-наглядові функції щодо відповідності застосування ШІ міжнародним стандартам прав людини та розроблятиме національні стандарти аудиту алгоритмів і систем ШІ, подібні до американської моделі сертифікації безпеки, точності та захисту даних.

ВИСНОВКИ

У дисертаційному дослідженні здійснено комплексний теоретико-правовий аналіз, порівняльно-правове узагальнення та обґрунтовано нове вирішення наукового завдання, що полягає у визначенні теоретико-правових засад впровадження та використання інформаційно-комунікаційних технологій у діяльності правоохоронних органів України.

Під час дослідження враховано положення чинного національного законодавства, міжнародні правові стандарти та практику їх застосування, що стосуються цифровізації діяльності правоохоронних органів. Проведено всебічний аналіз теоретичних підходів, нормативно-правових актів і практичних аспектів функціонування інформаційно-комунікаційних систем у правоохоронній сфері. Це дозволило обґрунтувати й вирішити комплекс завдань, які мають важливе наукове та прикладне значення для розвитку правового регулювання використання ІКТ у діяльності правоохоронних органів.

У результаті виконання дисертаційного дослідження сформульовано низку висновків, пропозицій та рекомендацій, що полягають у такому:

1. Визначено, що методологія дослідження теоретико-правових засад упровадження та використання інформаційно-комунікаційних технологій у діяльності правоохоронних органів становить цілісну систему принципів, підходів і методів наукового пізнання, спрямовану на виявлення закономірностей формування, розвитку та реалізації правових механізмів цифровізації діяльності правоохоронних органів.

З’ясовано, що вона інтегрує філософський, загальнонауковий, спеціально-юридичний і міждисциплінарний рівні пізнання, забезпечуючи комплексне осмислення правових явищ, пов’язаних із застосуванням ІКТ у правоохоронній сфері. Такий підхід уможливлює перехід від абстрактного теоретичного розуміння ролі цифрових технологій у праві до розроблення конкретних концептуальних положень щодо їх упровадження, правового регулювання та контролю в діяльності правоохоронних органів України.

2. З’ясовано, що інформаційно-комунікаційні технології і цифрові технології співвідносяться як загальне й окреме: ІКТ охоплюють ширший спектр процесів, що включає не лише цифрові технології, а й інші інструменти, спрямовані на забезпечення інформаційних операцій – збирання, обробку, зберігання та передавання даних.

Запропоновано авторське визначення терміну «інформаційно-комунікаційні технології у діяльності правоохоронних органів та поглиблено його сутнісне розуміння, яке полягає у цілеспрямованому використанні сучасних цифрових засобів для підвищення ефективності, оперативності, прозорості та результативності функціонування правоохоронних органів.

3. Встановлено, що застосування ІКТ у правоохоронній сфері ґрунтується на поєднанні базових (загальноправових), галузевих (інформаційно-правових та адміністративно-правових) та інституційних принципів, що відображають специфіку функціонування правоохоронних органів. Аргументовано доцільність класифікації галузевих принципів використання ІКТ залежно від рівня та сфери їх дії (ступеня універсальності та спеціалізації) на універсальні та спеціальні.

Надано авторське визначення поняття «принципи використання інформаційно-комунікаційних технологій у діяльності правоохоронних органів» як системи керівних ідей і нормативно-доктринальних засад, що визначають зміст, спрямованість і межі правового регулювання процесів упровадження, застосування та контролю за використанням ІКТ у діяльності правоохоронних органів.

4. Досліджено наукові підходи до класифікації законодавства у сфері правоохоронної діяльності. На основі аналізу чинної нормативно-правової бази визначено її структурні особливості та запропоновано розширений підхід до класифікації актів, що регулюють застосування ІКТ у діяльності правоохоронних органів. Зокрема, обґрунтовано доцільність їх поділу за такими критеріями: предмет правового регулювання; функціональне призначення; ступінь спеціалізації; напрям впливу (сфера дії норм).

Сформульовано авторське визначення поняття «правова основа застосування інформаційно-комунікаційних технологій у діяльності правоохоронних органів» як системи нормативно-правових актів та доктринальних положень, що визначають порядок, умови, межі та механізми впровадження, використання й контролю ІКТ у діяльності правоохоронних органів. Доведено, що формування правової основи впровадження та використання ІКТ у правоохоронній діяльності має бути спрямоване на створення комплексних передумов для ефективного, безпечного та правомірного функціонування цифрових технологій у цій сфері. Реалізація цього завдання вимагає вдосконалення правового регулювання на кількох рівнях, кожен із яких має власну сферу дії, механізми впливу та інструменти, що забезпечують узгоджене функціонування цифрових технологій у межах правової системи.

5. Зазначено, що широке впровадження технологій штучного інтелекту в діяльність правоохоронних органів зумовлює виникнення нових юридичних викликів, пов’язаних із забезпеченням законності, прозорості, обґрунтованості та підзвітності алгоритмічних рішень. У результаті дослідження правового регулювання впровадження та використання технологій ШІ у процесах збору, накопичення, обробки та аналізу інформації правоохоронними органами обґрунтовано необхідність формування концептуальних засад використання ШІ, які мають визначати принципи та правові механізми інтеграції цих технологій у правоохоронну практику з дотриманням вимог законності, безпеки й захисту прав людини.

Проаналізовано наукові підходи до розуміння феномену штучного інтелекту: когнітивно-символічний, нейронний, філософсько-теоретичний, правовий і соціально-гуманітарний. З’ясовано, що в науковій доктрині відсутня єдність щодо визначення правової природи ШІ. Виокремлено дві основні концепції його правового статусу: як інструмента (об’єкта) діяльності людини та як потенційного суб’єкта права. Для правоохоронної практики обґрунтовано перевагу інструментального підходу з одночасним встановленням чіткої системи відповідальності за дії та рішення, прийняті з використанням ШІ

(адміністративна, дисциплінарна, кримінально-правова та цивільно-правова відповідальність людини/органу). Наукова дискусія про суб'єктність ШІ має переважно теоретичний характер, а нормативні рішення повинні враховувати прогнозовані ризики й забезпечувати механізми контролю.

Розкрито особливості реалізації принципів використання ШІ у правоохоронній діяльності як складової частини ІКТ, зокрема принципів конфіденційності, оспорюваності та відшкодування, законної мети й верховенства інтересів людини, які мають забезпечувати баланс між ефективністю технологій і гарантіями прав людини.

Досліджено правові та технологічні аспекти використання систем відеоаналітики, розпізнавання обличь та допустимості документів, створених або згенерованих штучним інтелектом.

Визначено, що документи, створені або згенеровані із застосуванням систем штучного інтелекту, за своєю юридичною природою можуть бути еквівалентними традиційним офіційним документам, якщо вони відповідають вимогам автентичності, достовірності, цілісності та перевірюваності джерел даних. Проведено класифікацію документів, створених із використанням технологій штучного інтелекту, за критерієм ступеня автономності системи у процесі їх формування. Обґрунтовано, що документи, згенеровані автономними алгоритмічними системами, не мають автора у класичному правовому розумінні, оскільки рішення приймаються без безпосереднього людського втручання. Тому виникає необхідність визначення суб'єкта юридичної відповідальності за створення, перевірку і використання таких документів. Ним має бути оператор, адміністратор або орган, який експлуатує систему, адже саме він приймає кінцеве рішення про застосування згенерованих результатів у подальшій роботі правоохоронного органу. Сформульовані вимоги для документів, згенерованих штучним інтелектом.

6. Зазначено, що застосування мережі Інтернет як інструменту аналітичної, пошукової та розвідувальної діяльності правоохоронних органів супроводжується істотними нормативно-правовими прогалинами. Відсутність

спеціального законодавства, яке б регламентувало використання поліцією соціальних мереж і відкритих онлайн-ресурсів, призводить до правової невизначеності щодо меж допустимих дій, прав та обов'язків правоохоронців у цій сфері. Зроблено висновок, що ефективний моніторинг соціальних мереж правоохоронними органами потребує визначення кола уповноважених суб'єктів та закріплення їхніх прав, обов'язків і меж компетенції; збір інформації має здійснюватися лише за наявності обґрунтованих підстав, з дотриманням принципів доцільності та необхідності, документуватися та оцінюватися на предмет достовірності; застосування таємних облікових записів повинно обмежуватися рамками санкціонованого розслідування і бути підконтрольним, без втручання в персональні дані поза визначеними цілями.

7. Запропоновано удосконалення підготовки кадрів правоохоронних органів через включення до навчальних програм модулів з цифрової етики, правових основ використання ШІ та управління ризиками у сфері ІКТ. Зроблено висновок, що успішне застосування ШІ потребує системного підходу, який включає тестування алгоритмів, регламентовану обробку інформації та активне залучення всіх зацікавлених сторін, що забезпечує підвищення ефективності роботи та безпеки працівників за умови дотримання етичних стандартів, конфіденційності даних та надійності алгоритмів.

8. Проаналізовано міжнародний досвід впровадження інформаційно-комунікаційних технологій у правоохоронну діяльність, який ґрунтується на поєднанні централізованого управління даними, ризик-орієнтованого регулювання та системи незалежного контролю. Зазначено, що європейський підхід, заснований на принципах прозорості, підзвітності та захисту прав людини, формує правову основу для безпечного й етичного використання ШІ. Модель ЄС, яка передбачає класифікацію систем за рівнями ризику, може бути адаптована в Україні з урахуванням національних особливостей правозастосування. Досвід INTERPOL і провідних країн (США, Великої Британії, Канади, Німеччини, Франції, Австралії, Аргентини) підтверджує доцільність створення в Україні єдиної інформаційно-аналітичної

інфраструктури та незалежного органу для нагляду за використанням ШІ у правоохоронній сфері (Комітету з питань ШІ та ІКТ у правоохоронній діяльності) для здійснення аудиту алгоритмів, сертифікації інформаційних систем і моніторингу відповідності міжнародним стандартам прав людини.

9. Проведене дослідження засвідчило необхідність системного оновлення правового регулювання впровадження та контролю за використанням інформаційно-комунікаційних технологій у діяльності правоохоронних органів України. З урахуванням міжнародних стандартів (зокрема ризик-орієнтованої моделі ЄС щодо штучного інтелекту та принципів пропорційності, прозорості й підзвітності) доцільним є внесення доповнень до законів України «Про Національну поліцію», «Про оперативно-розшукову діяльність», «Про Службу безпеки України», «Про захист персональних даних» щодо: визначення права відповідних правоохоронних органів застосовувати у своїй діяльності інформаційно-комунікаційні технології та системи штучного інтелекту; закріплення особливостей збирання, обробки та зберігання цифрових доказів; запровадження механізмів моніторингу і контролю за законністю використання ІКТ; а також встановлення гарантій захисту прав людини під час використання ІКТ і ШІ (Додаток Б).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Деякі питання цифрової трансформації : розпорядження Кабінету Міністрів України від 02.08.2024 № 735-р. // Офіційний портал Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/735-2024-%D1%80#n14 (дата звернення: 05.12.2025).

2. Копча В. Методологія дослідження правового явища: поняття, структура, інструментарій // Часопис Київського університету права. 2020. № 1. С. 54–58. DOI: 10.36695/2219-5521.1.2020.08.

3. Балинська О. М., Ященко В. А. Методологія сучасного правознавства : посібник / за заг. ред. О. М. Балинської. Львів : Львів. держ. ун-т внутрішніх справ, 2018. 372 с.

4. Рабінович П. М. Основи загальної теорії права та держави : навч. посібник. 5-те вид. Київ : Атіка, 2001. 176 с.

5. Козюбра М. І. Методологія правознавства і методологія права: співвідношення понять та їх особливості // Право України. 2014. № 1. С. 22–32.

6. Харитонов Є. О. До визначення поняття та системи цивілістики (науки цивільного права) // Актуальні проблеми держави і права : зб. наук. пр. / Нац. ун-т «Одес. юрид. акад.». Одеса, 2009. Вип. 51. С. 7–13.

7. Данильян О. Г., Дзьобань О. П. Організація та методологія наукових досліджень : навч. посіб. Харків : Право, 2017. 448 с.

8. Пономарьов С. В. Методологія та методи дослідження адміністративно-правових засад сектору безпеки і оборони України // Науковий вісник Ужгородського національного університету. Серія: Право. 2017. Вип. 43, т. 4. С. 263–268.

9. Бірта Г. О., Бургу Ю. Г. Методологія і організація наукових досліджень : навч. посіб. Київ : ЦУЛ, 2014. 142 с.

10. Шевчук Р. Ще раз про діалектичний метод у правознавстві // Підприємництво, господарство і право. 2016. № 11. С. 216–219.

11. Костицький М. В. Про діалектику як методологію юридичної науки // Філософські та методологічні проблеми права. 2012. № 1. С. 3–17.

12. Оржинська Е. Використання загальнонаукових методів у слідчій практиці // Підприємництво, господарство і право. 2021. № 2. С. 272–276.

13. Скакун О. Ф. Теорія держави і права (енциклопедичний курс). Харків : Консум, 2011. 520 с.

14. Філатов В. Загальнонаукові та спеціально-правові методи дослідження моделі перехідного правосуддя // Юридичний вісник. 2022. № 2. С. 23–29. DOI: 10.32837/yuv.v0i2.2317.

15. Dubber M. D. Legal History as Legal Scholarship: Doctrinalism, Interdisciplinarity, and Critical Analysis of Law // Oxford Handbook of Historical Legal Research. [London], 2016. P. 1–15. URL: https://ssrn.com/abstract=3002587 (дата звернення: 05.12.2025).

16. Лук'янова Г. Ю. Методологічні основи дослідження права у сучасній юридичній науці // Науковий вісник Львівського державного університету внутрішніх справ. Серія: Юридична : зб. наук. пр. Львів, 2011. Вип. 4. С. 33–43.

17. Saxby S. A. Jurisprudence for Information Technology Law // International Journal of Law and Information Technology. 1994. Vol. 2, № 1. P. 1–31. DOI: 10.1093/ijlit/2.1.1.

18. Barlow J. P. Declaration of Independence of Cyber space : Davos, Switzerland, 8.02.1996 // Electronic Frontier Foundation : website. URL: https://www.eff.org/cyberspaceindependence (дата звернення: 02.12.2025).

19. Lessig L. Code and Other Laws of Cyberspace. Version 2.0. New York : Basic Books, 2006. 410 p.

20. McCartan K. F., McAlister R. Mobile phone technology and sexual abuse // Information Communications and Technology Law. 2012. Vol. 21, № 3. P. 257–268. DOI: 10.1080/13600834.2012.744223.

21. Jewkes Y. Public Policing & Internet Crime // Handbook of Internet Crime / Y. Jewkes, M. Yar (eds.). London : Willan Publishing, 2010. P. 525–545.

22. Banks J. Internet Gambling, Crime and the Regulation of Virtual Environments // Gambling, Crime and Society / J. Banks. London : Palgrave Macmillan, 2017. P. 183–223. DOI: 10.1057/978-1-137-57994-2.

23. Волуйко О., Дручек О. Поняття правоохоронної діяльності та правоохоронних органів у світлі концепції національної безпеки України // Підприємництво, господарство і право. 2020. № 10. С. 95–100. DOI: 10.32849/2663-5313/2020.10.16.

24. Ковальська В. В. Міліція в системі правоохоронних органів держави (адміністративно-правові аспекти) : дис. … д-ра юрид. наук : 12.00.07. Київ, 2010. 422 с.

25. Юридична енциклопедія : в 6 т. Київ : Укр. енцикл., 2003. Т. 5: П–С. 736 с.

26. Субота С. І. Аксіологічні засади правоохоронної діяльності в умовах розвитку громадянського суспільства // Юридичний науковий електронний журнал. 2020. № 1. С. 35–38. DOI: 10.32782/2524-0374/2020-1/7.

27. Про державний захист працівників суду і правоохоронних органів : Закон України : із змінами, внесеними законами України від 16.01.2014 № 721-VII та від 28.01.2014 № 732-VII // Офіційний портал Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/3781-12#Text (дата звернення: 15.12.2025).

28. Про контррозвідувальну діяльність : Закон України // Відомості Верховної Ради України. 2003. № 12. Ст. 89.

29. Порядок проведення інспектування Державною аудиторською службою, її міжрегіональними територіальними органами : постанова Кабінету Міністрів України від 20.04.2006 № 550 // Офіційний портал Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/550-2006-%D0%BF#Text (дата звернення: 19.12.2025).

30. Хлистік М. А. Визначення поняття правоохоронного органу в законодавстві України // Вчені записки ТНУ ім. В. І. Вернадського. Серія:

Юридичні науки. 2021. Т. 32 (71), № 4. С. 49–53. DOI: 10.32838/TNU-2707-0581/2021.4/09.

31. Мельник М. І., Хавронюк М. І. Правоохоронні органи та правоохоронна діяльність : навч. посіб. Київ : Атіка, 2002. 576 с.

32. Тацій В. Я. Доповідь Комісії з питань правоохоронної діяльності щодо визначення поняття та системи правоохоронних органів : 6 грудня 2012 р. // Конституанта : вебсайт. URL: http://constituanta.blogspot.com/2013/02/blog-post_2280.html (дата звернення: 23.12.2025).

33. Наукова концепція законодавчого забезпечення діяльності органів правопорядку України // Дослідницька служба Верховної Ради України : вебсайт. Київ, 2024. 128 с. URL: https://research.rada.gov.ua/uploads/documents/33251.pdf (дата звернення: 26.12.2025).

34. Кучук А. М. Теоретико-правові засади правоохоронної діяльності в Україні : автореф. дис. … канд. юрид. наук : 12.00.01. Київ, 2007. 22 с.

35. Юдкова К. В. Інформаційні технології у правовій сфері України: основні підходи до визначення // Science and Education a New Dimension. Humanities and Social Sciences. Budapest, 2017. Vol. 23, № 139. P. 40–43. URL: https://seanewdim.com/wp-content/uploads/2021/03/Information-technologies-in-the-legal-sphere-of-Ukraine-basic-approaches-to-the-definition-K.-V.-Yudkova.pdf (дата звернення: 25.12.2025).

36. Інформаційні технології : конспект лекцій / уклад.: Д. В. Риндюк, В. А. Пешко. Київ : КПІ ім. Ігоря Сікорського, 2022. 180 с.

37. Poppel H. L., Goldstein B. Information Technology: The Trillion-Dollar Opportunity. New York : McGraw-Hill, 1987. 207 p.

38. Триняк В. Ю. Інформаційна безпека як соціокультурний феномен (соціально-філософський аналіз) : дис. ... канд. філос. наук : 09.00.03. Донецьк, 2009. 189 с.

39. Баженов В. А., Венгерський П. С., Горлач В. М. Інформатика. Комп’ютерна техніка. Комп’ютерні технології. Київ : Каравела, 2004. 464 с.

40. Берназюк О. О. Проблема наукового визначення поняття цифрових технологій у праві // Науковий вісник Ужгородського національного університету. Серія: Право. 2017. Вип. 47, т. 2. С. 83–86.

41. Ерфан Є. А., Кушнірчук А. А. Дослідження ролі інформаційних технологій у сучасному міжнародному бізнесі // Науковий вісник Ужгородського національного університету. Серія: Міжнародні економічні відносини та світове господарство. 2020. Вип. 33, ч. 1. С. 49–54.

42. Синєокий О. В. Високотехнологічне інформаційне право України : [навч. посіб. для студентів юрид. та неюрид. спеціальностей]. Харків : Право, 2010. 360 с.

43. The Proposed ICT Sector Definition: Comments by the Task Force on Information Society Statistics: 18–19 June 1998 / OECD, DSTI/ICCP/AH/M(98) 1/REV1. Paris, 1998. 7 p. URL: https://one.oecd.org/document/DSTI/ICCP/ AH/RD(98)1/en/pdf (дата звернення: 11.12.2025).

44. Guide to measuring information and communication technologies (ICT) in education / UNESCO Institute for Statistics. Montreal, 2009. 138 p. // UNESCO Digital Library : website. URL: https://learningportal.iiep.unesco.org/en/glossary/information-and-communication-technologies-ict (дата звернення: 22.12.2025).

45. Закон України «Про Національну програму інформатизації» № 2807-IX від 01.12.2022 // Офіційний портал Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2807-20#Text (дата звернення: 20.12.2025).

46. Калюжний Д. Захист інформаційних прав особи в умовах цифровізації правоохоронної діяльності: теоретико-правовий аспект // Науковий вісник Ужгородського національного університету. Серія: Право. 2025. Вип. 90, ч. 3. С. 214–219. DOI: 10.24144/2307-3322.2025.90.3.30.

47. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР // Відомості Верховної Ради України. 1996. № 30. Ст. 141.

48. Правова доктрина України : у 5 т. / Ю. П. Битяк, О. В. Петришин, В. І. Борисов, В. Я. Тацій, Ю. С. Шемшученко, Н. С. Кузнєцова. Харків : Право, 2013. Т. 2. 863 с.

49. Юдкова К. В. Особливості визначення поняття «інформаційні технології» // Інформація і право. 2015. № 1 (13). С. 63–67.

50. Козюбра М. І. Принципи права: методологічні підходи до розуміння природи та класифікації в умовах сучасних глобалізаційних трансформацій // Право України. 2017. № 11. С. 142–164

51. Щупаківський Р. В. Загальні принципи права та їх значення для адміністративно-телекомунікаційного права // Держава та регіони. Серія: Право. 2019. № 4 (66). С. 123–128. DOI: 10.32840/1813-338X-2019-4-21.

52. Колодій А. М. Принципи права: генеза, поняття, класифікація та реалізація // Альманах права. 2012. № 3. С. 42–46.

53. Шатіло В. А. Загальнонаукові підходи до визначення принципів права та їх вплив на розвиток конституційного механізму державної влади // Публічне право. 2019. № 2 (34). С. 9–14. DOI: 10.37374/2019-34-01.

54. Шатрава С. О., Денищук Д. Є., Погорілець О. В. Нормативне закріплення правових принципів: сутність та значення на прикладі законодавства з охорони державної таємниці // Європейські перспективи. 2025. № 2. С. 375–381. DOI: 10.71404/EP.2025.2.55.

55. Уварова О. О. Принципи права у правозастосуванні: загальнотеоретична характеристика : монографія. Харків : Друкарня Мадрид, 2012. 196 с.

56. Макеєва О. М. Принципи правової комунікації: теоретико-правові аспекти // Юридичний вісник. Повітряне і космічне право. 2018. № 1. С. 48–53.

57. Калюжний Д. Принципи використання інформаційних технологій правоохоронними органами // Протидія дезінформації в умовах російської агресії проти України: виклики і перспективи : тези доп. міжнар наук.-практ. конф., Харків, 12–13 груд. 2023 р. / НДІ публ. політики і соц. наук та ін. Харків, 2023. С. 221–224. URL: https://library.pp-

ss.pro/index.php/ndippsn_20231212/article/view/kaliuzhnyi/pdf (дата звернення: 30.01.2026).

58. Бабенко А. М., Борисова О. О., Шаповалова І. О. Принципи права: поняття та класифікація // Прикарпатський юридичний вісник : зб. наук. пр. / Нац. ун-т «Одес. юрид. акад.». Івано-Франківськ, 2022. № 3 (44). С. 3–7. DOI: 10.32782/pyuv.v3.2022.1.

59. Братасюк М., Росоляк О. Співвідношення принципу верховенства права та принципу законності // Актуальні проблеми правознавства : зб наук. пр. / Західноукр. нац. ун-т. Тернопіль, 2018. Вип. 1 (13). С. 11–17.

60. Рішення Конституційного Суду України: п. п. 4.1 п. 4 мотивувальної частини у справі за конституційним поданням Верховного Суду України щодо відповідності Конституції України (конституційності) положень статті 69 Кримінального кодексу України, справа про призначення судом більш м'якого покарання від 2 листопада 2004 р. № 15-рп/2004 // Офіційний портал Верховної Ради України. URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=v015p710-04 (дата звернення: 22.12.2025).

61. Максименко Н. В. Принцип законності в адміністративному судочинстві як один із складових елементів принципу верховенства права // Наукові записки. Серія: Право : зб. наук. пр. / Центральноукр. держ. ун-т ім. Володимира Винниченка. Кропивницький, 2024. Вип. 16. С. 111–115. DOI: 10.36550/2522-9230-2024-16-111-115.

62. Постанова Верховного Суду від 26.10.2023, справа № 380/4680/21, адміністративне провадження № К/990/21589/23 // Liga 360 : онлайн-платформа. URL: https://cutt.ly/eeeOdIDD (дата звернення: 15.12.2025).

63. Comprehensive revision of the Telecommunications (Interception and Access) Act 1979. Report / Legal and Constitutional Affairs References Committee, The Senate, Commonwealth of Australia // Parliament of Australia : website. URL: https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs/Comprehensive_revision_of_TIA_Act/Report (дата звернення: 05.12.2025).

64. Андрусів У. Б., Федик С. Є. Елементи принципу юридичної визначеності // Часопис Київського університету права. 2019. № 1. С. 19–25.

65. Про ратифікацію Конвенції про захист прав людини і основоположних свобод 1950 р., Першого протоколу та протоколів № 2, 4, 7 та 11 до Конвенції (1997 р.) : Закон України від 17.07.1997 № 475/97-ВР // Відомості Верховної Ради України. 1997. № 40. Ст. 263.

66. Закон України «Про засади запобігання та протидії дискримінації в Україні» № 5207-VI від 06.09.2012 // Офіційний портал Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/5207-17#Text (дата звернення: 20.12.2025).

67. Про Національну поліцію : Закон України від 2.07.2015 № 580-VIII // Відомості Верховної Ради України. 2015. № 40–41. Ст. 379.

68. Загальна декларація прав людини : прийнята і проголошена резолюцією 217 А (III) Генеральної Асамблеї ООН від 10 грудня 1948 року // Офіційний вісник України. 2008. № 93. Ст. 3103.

69. Міжнародний пакт про громадянські і політичні права : прийнятий резолюцією 2200 А (XXI) Генеральної Асамблеї ООН від 16 грудня 1966 року, ратифікований Україною 19 жовтня 1973 року // Відомості Верховної Ради УРСР. – 1973. № 48. Ст. 438.

70. Про Службу безпеки України : Закон України від 25.03.1992 № 2229-XII // Відомості Верховної Ради України. 1992. № 27. Ст. 382.

71. Про оперативно-розшукову діяльність : Закон України від 18.02.1992 № 2135-XII // Відомості Верховної Ради України. 1992. № 22. Ст. 303.

72. Про прокуратуру : Закон України від 14.10.2014 № 1697-VII // Відомості Верховної Ради України. 2015. № 2/3. Ст. 12.

73. Тихонова Д. С. Поняття «правоохоронна діяльність» і функції правоохоронної діяльності // Проблеми сучасної поліцеїстики : тези доп. наук.-практ. конф., Харків, 20 квіт. 2022 р. / Харків. нац. ун-т внутр. справ. Харків, 2022. С. 224–225.

74. Holodnyk Y. Principles of activity of law enforcement bodies // Visegrad Journal on Human Rights. 2023. № 2. P. 55–61. URL: https://journals.uran.ua/journal-vjhr/article/view/295351 (дата звернення: 22.12.2025).

75. Сокуренко В. В. Принципи правоохоронної діяльності Національної поліції України // Вісник Харківського національного університету внутрішніх справ : зб. наук. пр. Харків, 2016. Вип. 4. С. 118–124.

76. Григоренко І. А. Принципи правоохоронної (поліцейської) діяльності в Україні та Німеччині // Наше право. 2013. № 7. С. 24–30.

77. Любарський В. С. Принцип відкритості та прозорості в діяльності правоохоронних органів // Часопис Київського університету права. 2023. № 3. С. 95–100. DOI: 10.36695/2219-5521.3.2023.18.

78. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI // Відомості Верховної Ради України. 2010. № 34. Ст. 481.

79. Положення про інформаційно-комунікаційну систему «Інформаційний портал Національної поліції України» : затверджене Наказом МВС України від 03.08.2017 № 676 // Офіційний портал Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/z1067-1 (дата звернення: 19.12.2025).

80. Case of S. and Marper v. the United Kingdom. Strasbourg. 4 Dec. 2008. Case of Roman Zakharov v. Russia. Strasbourg. 4 Dec. 2015 // The European Court of Human Rights : website. URL: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-159324%22]} (дата звернення: 11.12.2025).

81. Конвенція про кіберзлочинність : ратифікована Верховною Радою України 07.09.2005 № 2824-IV // Офіційний портал Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 27.12.2025).

82. Рекомендація CM/Rec (2020)1 Комітету Міністрів державам-членам щодо впливу алгоритмічних систем на права людини (ухвалено Комітетом Міністрів 8 квітня 2020 р. на 1373 засіданні Заступників Міністрів). URL: https://www.ppl.org.ua/wp-

content/uploads/2020/05/%D0%94%D0%BE%D0%B4%D0%B0%D1%82%D0%BE%D0%BA-Rec-20201.pdf (дата звернення: 22.12.2025).

83. The OECD AI Principles: adopted 2019; updated May 2024 // OECD Legal Instruments : website. URL: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 (дата звернення: 11.12.2025).

84. Регламент Європейського парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) // Офіційний портал Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 22.12.2025).

85. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII // Офіційний портал Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 20.12.2025).

86. Концепція розвитку цифрової економіки та суспільства України на 2018–2020 роки : розпорядження Кабінету Міністрів України від 17.01.2018. № 67-р // Офіційний портал Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text (дата звернення: 27.12.2025).

87. Стратегії розвитку системи Міністерства внутрішніх справ України до 2030 року : Наказ МВС № 547 від 22.06.2023 // Міністерство внутрішніх справ України : офіц. вебсайт. URL: https://mvs.gov.ua/ (дата звернення: 22.12.2025).

88. Мовчан А. В. Інформаційно-аналітична робота в оперативно-розшуковій діяльності Національної поліції : навч. посіб. Львів : ЛьвДУВС, 2017. 244 с.

89. Державне будівництво і місцеве самоврядування в Україні : підручник / І. І. Бодрова, С. В. Болдирєв, В. О. Величко та ін. ; за ред. С. Г. Серьогіної. 2-ге вид., перероб. та допов. Харків : Право, 2011. 360 с.

90. Поляк С. П. Правові основи діяльності оперативних підрозділів кримінальної поліції Національної поліції України з протидії втягненню неповнолітніх у злочинну діяльність // Форум права. 2017. № 2. С. 87–94. URL: http://nbuv.gov.ua/j-pdf/FP_index.htm_2017_2_16.pdf (дата звернення: 19.12.2025).

91. Загальна теорія держави і права : навч. посіб. / А. М. Колодій, В. В. Копєйчиков, С. Л. Лисенков та ін. ; за ред. В. В. Копєйчикова. Київ : Юрінком Інтер, 1999. 320 с.

92. Мельниченко Б. Б. Правова основа організації та діяльності органів публічного управління в Україні // Підприємництво, господарство і право. 2017. № 12. С. 174–177.

93. Голубов А. Є. Правова основа провадження в справах про злочини неповнолітніх: зміст та структура // Право і безпека. 2010. № 2. С. 137–142.

94. Лапкін А. В. Основи прокурорської діяльності в Україні : навч. посіб. у схемах. 3-тє вид., змін. та допов. Харків : Право, 2015. 148 с.

95. Бугайчук К. Л. Правові основи діяльності національної поліції України // Прикарпатський юридичний вісник : зб. наук. пр. / Нац. ун-т «Одес. юрид. акад.». Івано-Франківськ, 2018. Вип. 2 (23), т. 3. С. 125–130.

96. Павленко С. О. Генезис правового регулювання оперативно-розшукової тактики // Правова держава. 2021. № 43. С. 151–167.

97. Пеньков С. В., Шендрик В. В. Інформаційно-аналітичне забезпечення діяльності оперативних підрозділів Міністерства внутрішніх справ України: нормативно-правове регулювання // Jurnalul juridic naţional: teorie şi practică. 2015. № 3, т. 2. С. 78–80. URL: http://jurnaluljuridic.in.ua/archive/2015/3/part_2/16.pdf (дата звернення: 19.12.2025).

98. Василенко В. М. Цифрова трансформація правоохоронних органів: ризики в умовах гібридних загроз та шляхи їх подолання // Вісник Кримінологічної асоціації України : зб. наук. пр. / Харків. нац. ун-т внутр. справ, Кримінолог. асоц. України. Харків, 2024. Вип. 2 (32). С. 945–958. DOI: 10.32631/vca.2024.2.74.

99. Зінченко Д. А., Макарова О. П. Аналіз ризиків і стратегій захисту від кібератак у сучасному цифровому світі // Протидія кіберзлочинності та торгівлі людьми : зб. матеріалів Міжнар. наук.-практ. конф., Вінниця, 31 трав. 2023 р. / Харків. нац. ун-т внутріш. справ та ін. Вінниця, 2023. С. 118–121.

100. Каліман М. Р. Запобігання і нейтралізація загроз національним інтересам у галузі інформаційної безпеки. Міжнародна та національна безпека: теоретичні і прикладні аспекти : матеріали V Міжнар. наук.-практ. конф., Дніпро, 12 берез. 2021 р. / Дніпр. держ. ун-т внутрішніх справ. Дніпро, 2021. С. 196–197.

101. Онищук І. І. Правова цифровізація як інтегральний метод формалізації права // Наукові записки Інституту законодавства Верховної Ради України. 2020. № 6. С. 41–50. DOI: 10.32886/instzak.2020.06.05.

102. A European Strategy for Data / European Commission: DG Communications Networks Content and Technology // European Sources Online : website. 19 Febr. 2020. URL: https://www.europeansources.info/record/communication-on-a-european-strategy-for-data/?utm_source=chatgpt.com (дата звернення: 10.11.2025).

103. Okinawa Charter on Global Information Society : 22 July 2000 // Kyushu-Okinawa Summit 2000 (Official Documents) / Ministry of Foreign Affairs of Japan : website. URL: https://www.mofa.go.jp/policy/economy/summit/2000/documents/charter.html?utm_source=chatgpt.com (дата звернення: 22.12.2025).

104. Creation of global culture of cyber-safety and protection of critical infrastructure information : UN GA Resolution, adopted 21 January 2003. Daccess-DDS UN Document: N02/555/24. [New York], 2004. 3 p. URL: https://digitallibrary.un.org/record/509571?ln=ru&v=pdf (дата звернення: 05.12.2025).

105. Закон України «Про захист інформації в інформаційно-комунікаційних системах» № 80/94-ВР від 05.07.1994 // Офіційний портал Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр (дата звернення: 20.12.2025).

106. Масюк Л. Я. Правове регулювання правил етичної поведінки поліцейських та місце адміністративного законодавства в ньому // Вісник

Кримінологічної асоціації України : зб. наук. пр. / Харків. нац. ун-т внутр. справ, Кримінолог. асоц. України. Харків, 2024. Т. 32, № 2. С. 544–555. DOI: 10.32631/vca.2024.2.39.

107. Горбонос В. В. Класифікація нормативно-правових актів, які регулюють діяльність Експертної служби МВС України // Знання європейського права. 2020. № 3. С. 73–78. DOI: 10.32837/chern.v0i3.102.

108. Біла В. Р. Нормативні акти державного управління: питання класифікації // Вісник Харківського національного університету внутрішніх справ : зб. наук. пр. Харків, 2019. Вип. 87, № 4. С. 71–80. DOI: 10.32631/v.2019.4.07.

109. Концепція розвитку штучного інтелекту в Україні : схвалена розпорядженням Кабінету Міністрів України від 02.12.2020 № 1556-р // Офіційний портал Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#n8 (дата звернення: 27.12.2025).

110. Храпенко О. О., Меденцев А. М., Сперанський В. О. Цифровізація правоохоронної діяльності: використання штучного інтелекту для боротьби з кіберзлочинністю // Юридичний науковий електронний журнал. 2024. № 11. С. 505–508. DOI: 10.32782/2524-0374/2024-11/117.

111. McCarthy J. What is Artificial Intelligence? / Stanford University. Stanford, 2007. 15 p. URL: https://www-formal.stanford.edu/jmc/whatisai.pdf?utm_source=chatgpt.com (дата звернення: 22.12.2025).

112. Augusto L. M. From Symbols to Knowledge Systems: A. Newell and H. A. Simon’s Contribution to Symbolic AI // Journal of Knowledge Structures & Systems. 2021. Vol. 2, № 1. P. 29–62. URL: https://philarchive.org/archive/AUGFST-2 (дата звернення: 02.12.2025).

113. Субботін С. О., Олійник А. О., Олійник О. О. Неітеративні, еволюційні та мультиагентні методи синтезу нечіткологічних і нейромережних моделей : монографія / під заг. ред. С. О. Субботіна. Запоріжжя : ЗНТУ, 2009. 375 с.

114. Варипаєв О. М. Філософія науки та штучний інтелект: деконструкція суб’єкта і нова онтологія пізнання // Вісник гуманітарних наук. 2025. № 7. С. 1–21. DOI: 10.5281/zenodo.15525177.

115. Melnyk Y., Todorova S., Shevchenko H. Philosophical understanding of artificial intelligence as a technology // Philosophy and Governance. 2025. Vol. 3, № 7. P. 1–7. DOI: 10.70651/3041-248X/2025.3.01.

116. Popovych T. Artificial intelligence and human rights: philosophical and ethical foundations of legal regulation // Visegrad Journal on Human Rights. 2025. № 2. P. 127–132. DOI: 10.61345/1339-7915.2025.2.18.

117. Філіпенко Н., Лукашевич С., Андреєва О., Салаєва К. Соціально-правові та морально-етичні проблеми застосування штучного інтелекту та інформаційно-комунікаційних технологій // Вісник Пенітенціарної асоціації України. 2024. № 4. P. 95–103. DOI: 10.34015/2523-4552.2023.4.10.

118. Баранов О. Особливості визначення правового статусу робота із штучним інтелектом // Інформація і право. 2023. № 4 (47). С. 40–54. DOI: 10.37750/2616-6798.2023.4(47).291581.

119. Стратегія розвитку штучного інтелекту в Україні : монографія / за заг. ред. А. І. Шевченка. Київ : Наука і освіта, 2023. 305 с.

120. Федоренко О. А., Стрільців О. М., Тарасенко О. С. Використання технологій штучного інтелекту у правоохоронній діяльності : аналіт. огляд. Київ : Нац. акад. внутр. справ, 2022. 105 с.

121. Андрощук Г. Тенденції розвитку технологій штучного інтелекту: економіко-правовий аспект // Теорія і практика інтелектуальної власності. 2019. № 3. С. 84–101. DOI: 10.33731/32019.173817.

122. Hachkevych A. O. Revisiting the issue of legal determination of the concept of artificial intelligence // Journal of the National Academy of Legal Sciences of Ukraine. 2025. Vol. 32, № 1. P. 27–46. DOI: 10.31359/1993-0909-2025-32-1-27.

123. Баранов О. А. Визначення терміну «штучний інтелект» // Інформація і право. 2023. № 1 (44). С. 32–49. DOI: 10.37750/2616-6798.2023.1(44).287537.

124. ISO/IEC TR 24028:2020. Information technology – Artificial intelligence – Overview of trustworthiness in artificial intelligence. URL: https://www.iso.org/obp/ui/#iso:std:isoiec:tr:24028:ed-1:v1:en (дата звернення: 22.12.2025).

125. Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law : Vilnius, 5 IX 2024 // Council of Europe : website. URL : https://www.coe.int/en/web/artificial-intelligence/work-in-progress#02EN (дата звернення: 05.12.2025).

126. Калюжний Д. Проблеми та перспективи штучного інтелекту в діяльності правоохоронних органів // Науковий вісник Дніпровського державного університету внутрішніх справ. 2025. № 1 (132). С. 281–287. DOI: 10.32782/2078-3566-2025-1-36.

127. Павликівський В. Розвиток інформаційних технологій та штучного інтелекту в концепції прав людини // Пропілеї права та безпеки. 2025. № 8. С. 134–136. DOI: 0.32620/pls.2025.8.29.

128. The Bletchley Declaration by Countries Attending the AI Safety Summit, 1–2 Nov. 2023 // GOV.UK: public sector information : website. URL: https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023 (дата звернення: 11.12.2025).

129. Recommendation on the Ethics of Artificial Intelligence : adopted by the General Conference of the United Nations Educational, Scientific and Cultural Organization on 23 November 2021 // UNESCO : website. URL: https://www.unesco.org/en/legal-affairs/recommendation-ethics-artificial-intelligence (дата звернення: 26.12.2025).

130. Про наукову і науково-технічну діяльність : Закон України від 26.11.2015 № 848-VIII // Відомості Верховної Ради. 2016. № 3. Ст. 25.

131. Про технічні регламенти та оцінку відповідності : Закон України від 15.01.2015 № 124-VIII // Офіційний портал Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/124-19 (дата звернення: 22.12.2025).

132. Про звернення громадян : Закон України від 02.10.1996 № 393/96-ВР Офіційний портал Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/393/96-вр (дата звернення: 15.12.2025).

133. Про інформацію : Закон України від 02.10.1992 № 2657-XII // Офіційний портал Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення: 15.12.2025).

134. Положення про Міністерство внутрішніх справ України : затверджене Постановою КМУ від 28.10.2015 № 878 // Офіційний портал Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/878-2015-%D0%BF#Text (дата звернення: 19.12.2025).

135. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI // Офіційний портал Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 15.12.2025).

136. Порядок проведення повної перевірки декларації особи, уповноваженої на виконання функцій держави або місцевого самоврядування : Наказ Національного агентства з питань запобігання корупції від 29.01.2021 № 26/21 // Офіційний портал Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/z0158-21#Text (дата звернення: 19.12.2025).

137. НАЗК сформувало рейтинг ризикованості декларацій за 2024 рік та завершило автоперевірки декларацій // Східне міжрегіональне управління Державної служби України з питань праці : вебсайт. 8 серп. 2025 р. URL: https://smu.dsp.gov.ua/nazk-sformuvalo-reitynh-ryzykovanosti-deklaratsii-za-2024-rik-ta-zavershylo-avtoperevirky-deklaratsii/?utm_source=chatgpt.com (дата звернення: 19.12.2025).

138. Digital Technologies in the Judiciary Under Martial Law in Ukraine – article by judge of the Criminal Cassation Court of the Supreme Court Oleksandra Yanovska // Ukrainian Judiciary. Press-center : website.

URL:https://court.gov.ua/eng/supreme/pres-centr/news/1894732/?utm_source=chatgpt.com (дата звернення: 19.12.2025).

139. Звіт Національної поліції України про результати роботи у 2024 році // Національна поліція України : офіц. вебпортал. URL: https://npu.gov.ua/diyalnist/zvitnist/richni-zviti?utm_source=chatgpt.com (дата звернення: 19.12.2025).

140. Калюжний Д. Проблеми правового регулювання використання систем відеоспостереження правоохоронними органами // Пропілеї права та безпеки. 2025. № 6/7: Захист та стійкість критичної інфраструктури : матеріали наук.-практ. конф., Харків, 14 трав. 2025 р. С. 65–67. DOI: 10.32620/pls.2025.67.16.

141. The CEO of the American company Clearview AI whose product identified the occupiers and traitors will continue cooperation with the Ministry of Internal Affairs of Ukraine // Clearview AI : website. 13 Apr. 2023. URL: https://www.clearview.ai/press-room/the-ceo-of-the-american-company-clearview-ai-whose-product-identified-the-occupiers-and-traitors-will-continue-cooperation-with-the-ministry-of-internal-affairs-of-ukraine (дата звернення: 27.12.2025).

142. Bergengruen V. Ukraine's 'Secret Weapon' Against Russia Is a Controversial U.S. Tech Company // Time. 14.11.2023. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_fpu/cgiirbis_64.exe?C21COM=2&I21DBN=UPRES&P21DBN=UPRES&Z21ID=&Image_file_name=PDF/574828769868%2Epdf&IMAGE_FILE_DOWNLOAD=0 (дата звернення: 27.12.2025).

143. Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement] // European Data Protection Board : website. URL: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_hu (дата звернення: 20.12.2025).

144. EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data] / European Data Protection Board. [S. l.], 2019. 15 p.

URL: https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf (дата звернення: 20.12.2025).

145. Raposo V. L. The Use of Facial Recognition Technology by Law Enforcement in Europe: a Non-Orwellian Draft Proposal // European Journal of Criminal Policy and Research. 2023. Vol. 29. P. 515–533. DOI: 10.1007/s10610-022-09512-y.

146. Директива (ЄС) 2016/680 Європейського Парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб у зв'язку з обробкою персональних даних компетентними органами з метою запобігання, розслідування, виявлення або кримінального переслідування правопорушень, а також щодо вільного переміщення таких даних і скасування Рамкового рішення Ради 2008/977/ЈНА // EUR-Lex Access to European Union law : website. URL: https://eur-lex.europa.eu/eli/dir/2016/680/oj/eng (дата звернення: 11.12.2025).

147. Facial recognition technology: fundamental rights considerations in the context of law enforcement / European Union Agency for Fundamental Rights. Vienna, 2020. 36 p. URL: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf (дата звернення: 05.12.2025).

148. Harwell D. A face-scanning algorithm increasingly decides whether you deserve the job // The Washington Post. 6 Nov. 2019. URL: https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/ (дата звернення: 22.12.2025).

149. Taylor N. State Surveillance and the Right to Privacy // Surveillance & Society. 2002. Vol. 1, № 1. P. 66–85. DOI: 10.24908/ss.v1i1.3394.

150. Lukens P. It's Not A Police Report, It's A Transcription: A Better Term for AI-Generated Police Documents // Policing Insight – Global progressive policing : website. 23 Jul. 2024. URL: https://policinginsight.com/feature/innovation/its-not-a-police-report-its-a-transcription-a-better-term-for-ai-generated-police-documents/ (дата звернення: 22.12.2025).

151. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 № 851-IV // Офіційний портал Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення: 15.12.2025).

152. European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their Environment (Strasbourg, 3–4 December 2018) // Council of Europe. European Commission for the Efficiency of Justice (CEPEJ) : website. URL: https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment (дата звернення: 05.12.2025).

153. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 on Artificial Intelligence (Artificial Intelligence Act) // Official Journal of the European Union. L1689. 12 July 2024. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689 (дата звернення: 26.12.2025).

154. Кримінальний процесуальний кодекс України від 13.04.2012 № 4651-VI // Відомості Верховної Ради України. 2012. № 40/41. Ст. 378.

155. Recommendation on Artificial Intelligence (OECD/LEGAL/0449) / Organization for Economic Co-operation and Development. Paris : OECD Publishing, 2019. URL: https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449 (дата звернення: 22.12.2025).

156. Lynam M., Keatley D., Maker G., Coumbaros J. Vulnerability of individuals on mental health medications to drug facilitated sexual assaults // Forensic Science International: Synergy. 2024. Vol. 9. DOI: 10.1016/j.fsisyn.2024.100550.

157. Концепція Єдиної судової інформаційно-телекомунікаційної системи (ЄІТС) : Наказ Державної судової адміністрації України № 178 від 30.04.2025. 62 с. URL: https://court.gov.ua/storage/portal/dsa/normatyvno-pravova%20baza/N_178_2025_dodatok.pdf (дата звернення: 27.12.2025).

158. Bhati N. AI Transcription: Benefits, Applications, and Use Cases // Appquipo : Artificial Intelligence Development Company : website. URL: https://appquipo.com/blog/ai-transcription/ (дата звернення: 02.12.2025).

159. Gibbs J. How Law Enforcement Transcription Helps Justice Move Faster // Pev.com : website. URL: https://www.rev.com/blog/law-enforcement-transcription (дата звернення: 22.12.2025).

160. Зернецька О. В. Рух смислів у глобальному Інтернет-середовищі // Смислова морфологія соціуму : кол. монографія / Л. Аза, О. Зернецька, Н. Костенко та ін. / за ред. Н. Костенко. Київ : Ін-т соціології НАН України. 2012. С. 373–391.

161. Статистичні відомості про роботу із запитами на інформацію, які надійшли до Служби безпеки України // Служба безпеки України : вебсайт. URL: https://ssu.gov.ua/statystychni-vidomosti-pro-robotu-iz-zapytamy (дата звернення: 15.01.2026).

162. Річний звіт про діяльність Державного бюро розслідувань за 2024 рік // Державне бюро розслідувань : вебсайт. URL: https://dbr.gov.ua/reports (дата звернення: 15.01.2026).

163. Звіт про роботу органів Прокуратури за 2025 рік // Офіс Генерального прокурора : вебсайт. URL: https://gp.gov.ua/ua/posts/pro-robotu-organiv-prokuraturi-2 (дата звернення: 20.12.2025).

164. Звіт про діяльність Департаменту кіберполіції Національної поліції України у 2024 році // Департамент кіберполіції : вебсайт. 31 січ. 2025 р. URL: https://cyberpolice.gov.ua/news/zvitpro-diyalnist-departamentu-kiberpolicziyi-naczionalnoyi-policziyi-ukrayiny-u--roczi-7074 (дата звернення: 20.12.2025).

165. Результати СБУ за час повномасштабного вторгнення рф (станом на березень 2024 року) // Служба безпеки України : вебсайт. URL: https://ssu.gov.ua/rezultaty-sbu-za-chas-povnomasshtabnoho-vtorhnennia-stanom-na-berezen-2024-roku (дата звернення: 20.12.2025).

166. Segerstedt-Wiberg and Others v. Sweden: Application № 62332/00 // European Court of Human Rights : website. 6 June 2006. URL: https://hudoc.echr.coe.int (дата звернення: 26.12.2025).

167. Поліція Києва. Повідомлення про випадок із незаконним використанням ознак належності до поліції // Facebook : соціальна мережа. 2025.

URL: https://www.facebook.com/UA.KyivPolice/posts/pfbid0JuvsGB9MzW4qB9gjM7HC7xxikXgGh7kUvnkkjX5m4fyHRFCb7HsMhy4PDaPqhhJW (дата звернення: 19.12.2025).

168. Denef S., Kaptein N., Bayerl S., Ramirez L. Best practice in police social media adaptation // COMPOSITE – Comparative Police Studies in the EU. 2012. 19 p. URL: http://hdl.handle.net/1765/40562 (дата звернення: 05.12.2025).

169. СБУ знешкодила потужну ботоферму: 6 тисяч акаунтів працювали на розхитування протестних настроїв // Служба безпеки України : вебсайт. 1 груд. 2021 р. URL: https://ssu.gov.ua/novyny/sbu-zneshkodyla-potuzhnu-botofermu-6-tysiach-akauntiv-pratsiuvaly-na-rozkhytuvannia-protestnykh-nastroiv (дата звернення: 27.12.2025).

170. Синеколодезський Р., Кисельов А. Соціальні мережі та осінт-аналіз в розшуковій діяльності та діагностиці особистості // Universum. 2024. № 12. С. 40–48. URL: https://archive.liga.science/index.php/universum/article/view/1204 (дата звернення: 22.12.2025).

171. Гавловський В. Д. Правоохоронний моніторинг соціальних мереж // Правова інформатика. 2014. № 3 (43). С. 19–25.

172. Fortin F., Kentzinger C., Donne J. D., Chopin J. From the virtual frontlines: law enforcement’s experience with social media in policing activities // CrimRxiv : website. 2023. URL: https://www.crimrxiv.com/pub/et0nxukq (дата звернення: 22.12.2025).

173. Про затвердження Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні : Наказ16.11.2012 № 114/1042/516/1199/936/1687/5 / Ген. прокуратура України, М-во внутрішніх справ України, Служба безпеки України, Адмін. Держ. прикордонної служби України, М-во фінансів України, М-во юстиції України // Офіційний портал Верховної Ради України. URL: https://zakon.rada.gov.ua/go/v0114900-12 (дата звернення: 15.12.2025).

174. Levinson-Waldman R. Principles for Social Media Use by Law Enforcement // Brennan Center for Justice : website. 7 Febr. 2024.

URL: https://www.brennancenter.org/our-work/research-reports/principles-social-media-use-law-enforcement (дата звернення: 24.11.2025).

175. Internet of Things Global Standards Initiative // International Telecommunication Union (ITU) : website. URL: http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx (дата звернення: 22.12.2025).

176. Баранов О. А. Інтернет речей (IoT) і блокчейн // Інформація і право. 2018. № 1 (24). С. 59–71. DOI: 10.37750/2616-6798.2018.1(24).270747.

177. Костенко О. В. Напрями розвитку права у сфері інтернет речей (IoT) та штучного інтелекту // Актуальні проблеми вітчизняної юриспруденції. 2021. № 3. С. 130–136. DOI:10.15421/392161.

178. Самойленко М. Ю. Принципи застосування технології Інтернет речей у сучасному світі техніки // Вчені записки ТНУ ім. В. І. Вернадського. Серія: Технічні науки. 2020. Т. 31 (70), ч. 1, № 6. С. 142–148. DOI: 10.32838/TNU-2663-5941/2020.6-1/24 (дата звернення: 22.12.2025).

179. Бугера О. Інтернет речей та запобігання злочинності // Підприємництво, господарство і право. 2018. № 6. С. 295–298.

180. Future of Education and Skills 2030: Conceptual learning framework / Organization for Economic Co-operation and Development. Paris : OECD Publishing, 2018. 29 p. URL: https://www.oecd.org/education/2030-project/teaching-andlearning/learningskills/Skills_for_2030.pdf (дата звернення: 22.12.2025).

181. Ocak M. Global Skills Trends, Training Needs and Lifelong Learning Strategies for the Future of Work : Report Prepared for the G20 Employment Working Group // EPALE – Electronic Platform for Adult learning in Europe. 20 Nov. 2019. URL: https://epale.ec.europa.eu/en/resource-centre/content/global-skills-trends-training-needs-and-lifelong-learning-strategies-future (дата звернення: 22.12.2025).

182. Гуцу С. Вплив штучного інтелекту на професійні навички працівників // Пропілеї права та безпеки. 2024. № 4. С. 61–64. DOI: 10.32620/pls.2024.4.08.

183. Каталог тренінгових програм для прокурорів // Тренінговий центр прокурорів України : вебсайт. URL: https://ptcu.gp.gov.ua/uk/prokuroram/ (дата звернення: 22.12.2025).

184. Публічний звіт Служби безпеки України за 2024 рік // Служба безпеки України : вебсайт. URL: https://ssu.gov.ua/publichnyi-zvit-sluzhby-bezpeky-ukrainy-za-2024-rik.

185. Денищук Д. Особливості здійснення контролю знань з охорони державної таємниці в ДКВС України // Вісник кримінологічної асоціації України. 2023. № 2 (29). С. 361–372.

186. Wearable Technology Market Size & Share Analysis – Growth Trends and Forecast (2026–2031) // Mordor Intelligence : website. URL: https://www.mordorintelligence.com/industry-reports/wearable-technology-market?utm_source=chatgpt.com (дата звернення: 11.12.2025).

187. Lukens P. AI and driver fatigue: Enhancing officer wellness and safety // Policing Insight – Global progressive policing : website. 12 June 2024. URL: https://policinginsight.com/feature/innovation/ai-and-driver-fatigue-enhancing-officer-wellness-and-safety (дата звернення: 22.12.2025).

188. Revolutionizing employee wellness: how AI and machine learning are making a difference // Corporate Wellness Magazine : website. 4 Nov. 2023. URL: https://www.corporatewellnessmagazine.com/article/revolutionizing-employee-wellness-how-ai-and-machine-learning-are-making-a-difference (дата звернення: 05.12.2025).

189. Катеринчук І. Міжнародний та зарубіжний досвід застосування інформаційних технологій у діяльності правоохоронних органів // National law journal: teory and practice. Chisinau, 2015. № 7. С. 22–26.

190. Угода між Україною та Європейським поліцейським офісом про стратегічне співробітництво : Закон України від 05.10.2010 № 2576-VI // Офіційний вісник України. 2010. № 96/84. Ст. 2934/3432.

191. Угода між Україною та Європейським поліцейським офісом про оперативне та стратегічне співробітництво, ратифікована Законом від 12.07.2017 № 2129-VIII // Офіційний вісник України. 2017. № 62/71. ст. 2192. URL: https://zakon.rada.gov.ua/laws/show/984_001-16#Text (дата звернення: 27.12.2025).

192. ENISA: 15 years of building cybersecurity bridges together : press release, 20 March 2019 // European Union Agency for Network and Information Security (ENISA) : website. URL: https://www.enisa.europa.eu/news/enisa-news/enisa-15-years-of-building-cybersecurity-bridges-together (дата звернення: 05.12.2025).

193. Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence – Compliance of the legal bases of Articles 114 and 16 TFEU with respect to provisions applicable to law enforcement and judicial authorities (Council document 12302/22). Brussels, 2022. 20 p. URL: https://www.statewatch.org/media/3510/eu-council-ai-act-law-enforcement-legal-basis-cls-12302-22.pdf (дата звернення: 26.12.2025).

194. Реутов І. Правове регулювання штучного інтелекту: міжнародний досвід та українські перспективи // Право: видавництво «Юридична практика» : вебсайт. 10 листоп. 2023 р. URL: https://pravo.ua/pravove-rehuliuvannia-shtuchnoho-intelektu-mizhnarodnyi-dosvid-ta-ukrainski-perspektyvy/ (дата звернення: 22.12.2025).

195. Montagne T. Overview of the AI Act, the first ever legal framework on AI // Crypto and digitization : website. 26 March 2024. URL: https://paytechlaw.com/en/overview-of-the-ai-act-the-first-ever-legal-framework-on-ai/ (дата звернення: 22.12.2025).

196. Кознова О. Європарламент ухвалив Закон про штучний інтелект // Liga Zakon : інформ.-правовий сервіс : вебсайт. 13 берез. 2024 р. URL: https://biz.ligazakon.net/news/226272_vroparlament-ukhvaliv-zakon-pro-shtuchniy-ntelekt (дата звернення: 20.12.2025).

197. Kalyuzhnyi D. Legal grounds for artificial intelligence use in law enforcement: international and foreign experience // Архів кримінології та судових наук. 2024. № 1 (9). С. 117–127. DOI:10.32353/acfs.9.2024.08.

198. European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal proceedings, 2020/2021(INI) // EUR-Lex : Access to European Union law : website.

URL: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html (дата звернення: 05.12.2025).

199. Kafteranis D., Sachoulidou A., Turksen U. Artificial Intelligence in Law Enforcement Settings: AI Solutions for Disrupting Illicit Money Flows // EUCRIM. 2023. Vol. 18 (1). P. 60–66. DOI: 10.30709/eucrim-2023-006.

200. Assessing technologies in law enforcement : a method for ethical decision-making. Luxembourg : Publications Office of the European Union, 2025. 29 p. DOI: 10.2813/1291864.

201. Article 29 Data Protection Working Party. Opinion on some key issues of the Law Enforcement Directive (EU 2016/680) – WP258 (2017) // European Commission : website. URL: https://ec.europa.eu/newsroom/article29/items/610178 (дата звернення: 02.12.2025).

202. Guidelines 3/2019 on processing of personal data through video devices. Version 2.0. Adopted on 29 January 2020 / European Data Protection Board. [S. l.], 2020. 33 p. URL: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf (дата звернення: 02.12.2025).

203. Ban biometric mass surveillance! // EDRI : website. URL: https://edri.org/our-work/blog-ban-biometric-mass-surveillance/ (дата звернення: 05.12.2025).

204. Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. Convention 108. Guidelines on Facial Recognition / Directorate General of Human Rights and Rule of Law. 28 Jan. 2021. 16 p. URL: https://rm.coe.int/guidelines-on-facial-recogni=tion/1680a134f3 (дата звернення: 05.12.2025).

205. Lynch N. Facial Recognition Technology in Policing and Security: Case Studies in Regulation // Laws. 2024. Vol. 13, № 3, art. 35. P. 1–14. DOI: 10.3390/laws13030035.

206. Kwilinski A., Reznik O. Governance of artificial intelligence technologies and systems in the eu and ukraine: legal foundations and institutional mechanisms //

Forum Scientiae Oeconomia. 2025. Vol. 13 (3), P. 8–52. DOI: 10.23762/FSO_VOL13_NO3_1.

207. INTERPOL: Five actions for a safer world // INTERPOL : website. URL: //www.interpol.int/Who-we-are/What-is-INTERPOL/INTERPOL-Five-actions-for-a-safer-world доступу (дата звернення: 22.12.2025).

208. ROXANNE Project : website. URL: https://www.interpol.int/Who-we-are/Legal-framework/Information-communications-and-technology-ICT-law-projects/ROXANNE-Project (дата звернення: 26.12.2025).

209. Інструкції «Про порядок використання правоохоронними органами України інформаційної системи Міжнародної організації кримінальної поліції – Інтерпол», затверджені спільним наказом Міністерства внутрішніх справ України, Офісу Генерального прокурора, Національного антикорупційного бюро України, Служби безпеки України, Державного бюро розслідувань, Міністерства фінансів України, Міністерства юстиції України № 613/380/93/228/414/510/2801/5 від 17.08.2020 // Офіційний портал Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/z0849-20#Text (дата звернення: 20.12.2025).

210. Blueprint for an AI Bill of Rights // The White House : official website. URL: https://www.whitehouse.gov/ostp/ai-bill-of-rights (дата звернення: 02.12.2025).

211. Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence : 30 Oct. 2023 // The White House : official website. URL: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/?utm_source=link (дата звернення: 05.12.2025).

212. Красніков Д. Новий указ Президента Байдена про штучний інтелект: більше обмежень чи стимулювання розвитку // Укрінформ : вебсайт. 15 листоп. 2023. URL: https://www.ukrinform.ua/rubric-technology/3787099-novij-ukaz-prezidenta-bajdena-pro-stucnij-intelekt-bilse-obmezen-ci-stimuluvanna-rozvitku.html (дата звернення: 27.12.2025).

213. Cyber crime // Australian Federal Police : website. URL: https://www.afp.gov.au/what-we-do/crime-types/cyber-crime (дата звернення: 05.12.2025).

214. Ferguson A. G. Concerns about AI-written police reports spur states to regulate the emerging practice // The Conversation : website. 15 Oct. 2025. URL: https://theconversation.com/concerns-about-ai-written-police-reports-spur-states-to-regulate-the-emerging-practice-267410 (дата звернення: 22.12.2025).

215. Senate Bill No. 524, Chapter 587. An act to add Section 13663 to the Penal Code, relating to law enforcement agencies // California legislature Information : website. URL: https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202520260SB524 (дата звернення: 11.12.2025).

216. Treacy S. Biometrics could improve gun safety one fingerprint at a time // Electronics 360: Electronics Industry News and Analysis : website. 17 July 2017. URL: https://electronics360.globalspec.com/article/9301/biometrics-couldimprove-gun-safety-one-fingerprint-at-a-time (дата звернення: 11.12.2025).

217. The Artificial Intelligence and Data Act (AIDA) : Companion Document // Government of Canada : website. URL: https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document#s10 (дата звернення: 11.12.2025).

218. Ferguson C., Whiteside H. Bill C-27: Federal Government Releases Amendments to Canada's Proposed AI Law // Privacy & Cybersecurity Bulletin. 7 Dec. 2023. URL: https://www.fasken.com/en/knowledge/2023/12/bill-c27-federal-government-releases-amendments-to-canadas-proposed-ai-law#authors (дата звернення: 02.11.2025).

219. National Crime Agency : official website. URL: http://www.nationalcrimeagency.gov.uk (дата звернення: 22.12.2025).

220. Covenant for Using Artificial Intelligence (AI) in Policing / National Police Chiefs' Council. 7 p. URL: https://science.police.uk/site/assets/files/4682/ai_principles_1_1_1.pdf (дата звернення: 05.12.2025).

221. Police turn to wearable tech to improve sleep and fitness // Liverpool John Moores University : website. URL: https://www.ljmu.ac.uk/about-us/news/articles/2025/3/18/police-turn-to-wearable-tech?utm_source=chatgpt.com. (дата звернення: 22.12.2025).

222. Gikay A. How the UK is getting AI regulation right // Policing Insight. 26 June 2023. URL: https://policinginsight.com/feature/opinion/how-the-uk-is-getting-ai-regulation-right// (дата звернення: 22.12.2025).

223. Devonshire J. How artificial intelligence use in policing is transforming law enforcement // Emergency Services Times. 27 Sept. 2024. URL: https://emergencyservicestimes.com/2024/09/27/how-artificial-intelligence-use-in-policing-is-transforming-law-enforcement (дата звернення: 22.12.2025).

224. Police use of AI more responsible with an independent data ethics advisory committee // Northumbria University : website. URL: https://www.northumbria.ac.uk/about-us/news-events/news/police-use-of-ai-more-responsible-with-an-independent-data-ethics-advisory-committee/ (дата звернення: 26.12.2025).

225. Artificial Intelligence Review of Germany / Organization for Economic Co-operation and Development. Paris : OECD Publishing, 2024. 173 p. DOI: 10.1787/609808d6-en.

226. Report of the Inquiry into Potential Reforms of Australia's National Security Legislation / Parliament of Australia, Parliamentary Joint Committee on Intelligence and Security. Canberra, 2013. 321 p. URL: https://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=pjcis/nsl2012/report.htm (дата звернення: 26.12.2025).

227. Казанчук І. Д. Правові засади використання штучного інтелекту в діяльності правоохоронних органів (поліції) та органів суду під час здійснення адміністративного провадження (аналіз зарубіжного та українського досвіду) // Право.ua. 2023. № 4. С. 63–69. DOI: 10.32782/LAW.UA.2023.4.10.

Додаток А

Список публікацій здобувача за темою дисертації

Наукові праці, в яких опубліковані основні наукові результати дисертації:

1. Kalyuzhnyi D. Legal grounds for artificial intelligence use in law enforcement: international and foreign experience // Архів кримінології та судових наук. 2024. № 1 (9). С. 117–127. DOI: 10.32353/acfs.9.2024.08.

2. Калюжний Д. До питання правового статусу документів, згенерованих штучним інтелектом, в правоохоронній сфері // Науковий вісник Ужгородського національного університету. Серія: Право. 2025. Вип. 88, ч. 2. С. 399–404. DOI: 10.24144/2307-3322.2025.88.2.55.

3. Калюжний Д. Проблеми та перспективи штучного інтелекту в діяльності правоохоронних органів // Науковий вісник Дніпровського державного університету внутрішніх справ. 2025. № 1 (134). С. 281–287. DOI: 10.32782/2078-3566-2025-1-36.

4. Калюжний Д. Захист інформаційних прав особи в умовах цифровізації правоохоронної діяльності: теоретико-правовий аспект // Науковий вісник Ужгородського національного університету. Серія: Право. 2025. Вип. 90, ч. 3. С. 214–219. DOI: 10.24144/2307-3322.2025.90.3.30.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

1. Калюжний Д. Сучасні інформаційні технології в діяльності правоохоронних органів: проблеми і перспективи правового регулювання // Безпека та сталий розвиток критичної інфраструктури в умовах воєнного стану : тези доп. наук.-практ. конф., Харків, 8 листоп. 2023 р. / Нац. аерокосм. ун-т ім. М. Є. Жуковського «Харків. авіац. ін-т». Харків, 2023. С. 65–69. URL: http://library.khai.edu/library/fulltexts/doc/Bezpeka_Ta_Stalyy_Rozvytok.pdf (дата звернення: 30.01.2026).

2. Калюжний Д. Принципи використання інформаційних технологій правоохоронними органами // Протидія дезінформації в умовах російської агресії проти України: виклики і перспективи : тези доп. міжнар наук.-практ. конф.,

Харків, 12–13 груд. 2023 р. / НДІ публ. політики і соц. наук та ін. Харків, 2023. С. 221–224. URL: https://library.pp-ss.pro/index.php/ndippsn_20231212/article/view/kaliuzhnyi/pdf (дата звернення: 30.01.2026).

3. Калюжний Д. Щодо питання правового визначення і особливостей ІКТ у правоохоронній діяльності // Сучасні проблеми розвитку авіаційно-космічної галузі України: інженерія, бізнес, право : тези доп. міждисциплінар. наук.-практ. конф., Харків, 5 листопда 2024 р. / Нац. аерокосм. ун-т ім. М. Є. Жуковського «Харків. авіац. ін-т». Харків, 2024. С. 132–137. URL: http://library.khai.edu/library/fulltexts/Conf/Konf_SPR_2024.pdf (дата звернення: 30.01.2026).

4. Калюжний Д. Правові засади використання ІКТ в правоохоронній діяльності: європейський досвід // Міждисциплінарний дискурс: стійкість критичної інфраструктури : тези доп. наук.-практ. конф., Харків, 14 трав. 2024 р. / Нац. аерокосм. ун-т ім. М. Є. Жуковського «Харків. авіац. ін-т». Харків, 2024. С. 64–69. URL: https://library.khai.edu/library/fulltexts/Conf/Mizhdystsyplinarnyy_Dyskurs.pdf(дата звернення: 30.01.2026).

5. Калюжний Д. Проблеми правового регулювання використання систем відеоспостереження правоохоронними органами // Пропілеї права та безпеки. 2025. № 6/7: Захист та стійкість критичної інфраструктури : матеріали наук.-практ. конф., Харків, 14 трав. 2025 р. С. 65–67. DOI: 10.32620/pls.2025.67.16.

Додаток Б

Пропоновані зміни до законодавства щодо впровадження інформаційно-комунікаційних технологій у правоохоронну діяльність

Норма, що підлягає зміні/доповненню	Поточна редакція	Пропонована зміна/доповнення
Закон України «Про оперативно-розшукову діяльність»		
Стаття 8	Не згадує ІКТ	***частину першу статті 8 доповнити пунктом 22 наступного змісту***: «Застосовувати інформаційно-комунікаційні технології в тому числі програмно-апаратні засоби, бази даних, системи штучного інтелекту, аналітичні платформи, технологій розпізнавання облич, аналізу поведінкових шаблонів, геолокаційного спостереження тощо, в оперативно-розшуковій діяльності здійснюється виключно з дотриманням принципів законності, пропорційності, необхідності та забезпечення захисту прав і свобод людини і громадянина. Види інформаційно-комунікаційних технологій, порядок їх застосування, зберігання і обробки отриманої інформації, а також механізми контролю за їх використанням визначаються цим Законом та іншими нормативно-правовими актами, прийнятими відповідно до нього.»
стаття 9 ч.11	«Підрозділи, що використовують автоматизовані інформаційні системи в оперативно-розшуковій діяльності, повинні забезпечити можливість	**Доповнити ч.11 ст.9 новим абзацом такого змісту:** «Кожне використання таких систем повинно бути зафіксовано в електронному журналі, що підлягає внутрішньому та зовнішньому контролю. Доступ до цифрових матеріалів здійснюється за індивідуальним цифровим ідентифікатором з обов'язковим протоколюванням усіх дій. Оперативні підрозділи мають право застосовувати програмно-апаратні засоби, бази даних, системи штучного інтелекту, аналітичні платформи тощо – виключно на підставі та в порядку, визначених законом.»

	видавати дані про особу на запит органів досудового розслідування, прокуратури, суду. В місцях зберігання інформації повинна бути гарантована її достовірність та надійність охорони».	
Закон України «Про Національну поліцію»		
Стаття 23	Не має прямої згадки про використання інформаційно-комунікаційних технологій	**Статтю 23 доповнити новим п.26-1:** «Застосовує інформаційно-комунікаційні технології, у тому числі технології розпізнавання облич, аналізу поведінкових шаблонів, геолокаційного спостереження тощо, для виявлення та фіксації правопорушень, моніторингу публічного порядку, з'ясування причин та умов правопорушень, а також аналітичної обробки інформації. Застосування інформаційно-комунікаційних технологій здійснюється відповідно до спеціального порядку, затвердженого Кабінетом Міністрів України.»
Закон України «Про захист персональних даних»		
Пункт 7 частини другої статті 7	7) стосується вироків суду, виконання завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом та здійснюється державним органом в межах його повноважень, визначених законом	**Доповнити Пункт 7 частини другої статті 7 новим абзацом такого змісту:** *«*Обробка персональних даних органами, що здійснюють оперативно-розшукову, слідчу або іншу правоохоронну діяльність із застосуванням інформаційно-комунікаційних технологій, допускається виключно за умови технічного аудиту системи, ведення журналу доступів, і не повинна порушувати права суб'єктів персональних даних, за винятком випадків, прямо передбачених законом. Усі операції з даними (збирання, доступ, передача, аналіз) фіксуються в автоматизованому режимі. Органи, що використовують інформаційно-комунікаційні технології у роботі з персональними даними, зобов'язані пройти щорічну незалежну перевірку систем захисту інформації..*»*

Закон України «Про Службу безпеки України»		
Стаття 25	Не згадує інформаційно-комунікаційні технології	**Доповнити частину першу статті 25 новим пунктом 12-1 такого змісту:** «Застосувати сучасні інформаційно-комунікаційні технології, в тому числі розвідувальне програмне забезпечення, системи автоматизованого аналізу (включаючи ШІ) тощо, виключно в рамках спеціальних процедур, визначених законом та внутрішніми регламентами СБУ»
Нова стаття 26-1	відсутня	**Стаття 26-1. Порядок використання інформаційно-комунікаційних технологій у діяльності Служби безпеки України.** Служба безпеки України у своїй діяльності має право використовувати інформаційно-комунікаційні технології з метою забезпечення національної безпеки, захисту державного суверенітету, територіальної цілісності, конституційного ладу України, а також для запобігання, виявлення, припинення та розслідування злочинів, віднесених до її компетенції. Застосування інформаційно-комунікаційних технологій у діяльності Служби безпеки України не може бути спрямоване на неправомірне втручання в приватне життя особи, обмеження її прав чи свобод, крім випадків, прямо передбачених законом і санкціонованих у встановленому порядку. Кожне втручання в інформаційний простір, що пов'язане з персональними даними або електронною ідентичністю особи, підлягає обов'язковому журналюванню та контролю з боку визначених уповноважених підрозділів Служби безпеки України. Відомості про такі дії зберігаються у захищених журналах обліку в порядку, визначеному відомчими нормативно-правовими актами. Служба безпеки України впроваджує щорічний аудит кібербезпеки та функціонування інформаційних систем, що використовуються в оперативно-службовій діяльності. Контроль за дотриманням законності під час використання інформаційно-комунікаційних технологій у діяльності Служби безпеки України здійснюється Верховною Радою України, Уповноваженим Верховної Ради України з прав людини, а також у межах компетенції — іншими державними органами.

ЗАТВЕРДЖУЮ

Директор Науково-дослідного
інституту публічної політики і
соціальних наук
доктор юридичних наук, професор

М. В. Завальний

«12» _____ 2026 р.

АКТ
про впровадження результатів дисертаційного дослідження Калюжного Дмитра Олександровича «Теоретико-правові засади впровадження і використання інформаційно-комунікаційних технологій у діяльності правоохоронних органів», поданого на здобуття наукового ступеня доктора філософії зі спеціальності 081 «Право» у правотворчу діяльність Науково-дослідного інституту публічної політики і соціальних наук

Повідомляємо спеціалізованій вченій раді, що результати дисертації Калюжного Дмитра Олександровича «Теоретико-правові засади впровадження і використання інформаційно-комунікаційних технологій у діяльності правоохоронних органів», поданого на здобуття наукового ступеня доктора філософії зі спеціальності 081 «Право», спрямовані на комплексне теоретико-правове осмислення процесів цифровізації правоохоронної діяльності в умовах розвитку інформаційного суспільства, впровадження штучного інтелекту та трансформації публічного управління.

У дисертації здійснено системний аналіз нормативно-правових засад використання інформаційно-комунікаційних технологій у діяльності правоохоронних органів, розкрито їх вплив на організацію оперативно-службової діяльності, управлінські процеси, прийняття рішень, забезпечення особистої безпеки працівників та захист прав і свобод людини. Особливу увагу приділено дослідженню правових аспектів застосування технологій штучного інтелекту, автоматизованих аналітичних систем, цифрових платформ, засобів моніторингу та обробки даних у правоохоронній сфері.

У роботі виявлено основні правові ризики та виклики, пов'язані з цифровізацією правоохоронної діяльності, зокрема у частині захисту персональних і біометричних даних, дотримання принципів законності, пропорційності, підзвітності та етичності використання алгоритмічних систем. Узагальнено міжнародний і зарубіжний досвід правового регулювання впровадження ІКТ і технологій штучного інтелекту у діяльність правоохоронних органів, а також визначено можливості його адаптації до національної правової системи України.

За результатами дослідження сформульовано науково обґрунтовані пропозиції щодо вдосконалення нормативно-правового регулювання цифрової трансформації правоохоронних органів, розвитку цифрових і професійних компетентностей персоналу, підвищення ефективності управлінських та аналітичних процесів, а також забезпечення балансу між технологічною ефективністю та гарантіями прав людини.

Розроблені наукові положення використовуються Науково-дослідним інститутом публічної політики і соціальних наук та іншими науково-експертними установами під час підготовки аналітичних матеріалів, експертних висновків і пропозицій щодо формування та реалізації державної політики у сфері цифровізації правоохоронної діяльності, інформаційної безпеки та впровадження штучного інтелекту у публічне управління.

Отримані результати дисертаційного дослідження можуть бути використані у законопроєктній діяльності у сфері адміністративного, інформаційного та кримінального процесуального права, у практичній діяльності правоохоронних органів з метою підвищення ефективності застосування ІКТ, а також у навчальному процесі під час підготовки та підвищення кваліфікації фахівців у галузі права, публічного управління та правоохоронної діяльності.

Результати дисертаційного дослідження Калюжного Дмитра Олександровича мають належний теоретичний рівень, наукову новизну та практичну значущість і сприятимуть подальшому вдосконаленню правового регулювання використання інформаційно-комунікаційних технологій і технологій штучного інтелекту у діяльності правоохоронних органів України відповідно до європейських стандартів та принципів верховенства права.

Члени комісії:

А. Є. Голубов

О. Є. Кухарєв

Проректору з наукової роботи
Національного аерокосмічного університету
«Харківський авіаційний інститут»
д-ру наук з держ. управління, професору
Світлані ДОМБРОВСЬКІЙ
м. Харків, вул. Вадима Манька, 17
61000, khai@khai.edu

ДОВІДКА
про впровадження результатів дисертаційного дослідження Калюжного Дмитра Олександровича «Теоретико-правові засади впровадження і використання інформаційно-комунікаційних технологій у діяльності правоохоронних органів»

Повідомляємо, що результати дисертаційного дослідження Калюжного Дмитра Олександровича на тему «Теоретико-правові засади впровадження і використання інформаційно-комунікаційних технологій у діяльності правоохоронних органів», поданого на здобуття наукового ступеня доктора філософії зі спеціальності 081 «Право», впроваджено у практичну діяльність підрозділів ***(Департаменту кіберполіції Національної поліції України.)***

Зокрема, висновки та рекомендації дисертаційного дослідження використовуються у діяльності кіберполіції під час правового та організаційного забезпечення протидії кримінальним правопорушенням, що вчиняються з використанням інформаційно-комунікаційних технологій, автоматизованих систем та цифрових платформ;

Окремі положення дисертаційного дослідження враховуються при організації службової підготовки працівників кіберполіції, зокрема в частині підвищення рівня правової обізнаності щодо використання сучасних інформаційних технологій, цифрових інструментів розслідування та елементів штучного інтелекту.

Начальник УПК в Харківській області
Департаменту кіберполіції НПУ
полковник поліції **Валерій БЕРЕЗА**

ЗАТВЕРДЖУЮ

В.о. декана гуманітарно-правового факультету доктор філософії з права, доцент
Ірина ТУР
«20» 10 2026 р.

А К Т

впровадження результатів дисертаційного дослідження здобувача вищої освіти ступеня доктора філософії Калюжного Дмитра Олександровича «Теоретико-правові засади впровадження і використання інформаційно-комунікаційних технологій у діяльності правоохоронних органів» зі спеціальності 081 Право в освітній процес Національного аерокосмічного університету «Харківського авіаційний інститут»

Комісія у складі:
1) завідувача кафедри, д.ю.н., проф. Павліківського Віталія Івановича;
2) доцента кафедри, д. ю. н., доцент Мельника Валентина Володимировича;
3) професора кафедри, к.ю.н., проф. Фіалки Михайла Ігоревича.

цим актом засвідчує, що результати дисертаційного дослідження здобувача Калюжного Дмитра Олександровича на тему «Теоретико-правові засади впровадження і використання інформаційно-комунікаційних технологій у діяльності правоохоронних органів» використовуються співробітниками кафедри права гуманітарно-правового факультету Національного аерокосмічного університету «Харківського авіаційний інститут» під час підготовки та проведення лекційних, семінарських і практичних занять з навчальних дисциплін «Інформаційне право», «Інформаційне право та інформаційна безпека критичної інфраструктури», «Адміністративне право та процес», «Кримінальне право», а також похідних від них спеціальних курсів, зокрема «Захист персональних даних», «Правове регулювання інформаційної безпеки в Україні», «Міжнародне співробітництво правоохоронних органів».

Дисертація Калюжного Дмитра Олександровича є одним із перших в Україні комплексних самостійних кваліфікаційних наукових досліджень, присвячених теоретико-правовому осмисленню процесів впровадження та використання інформаційно-комунікаційних технологій і технологій штучного інтелекту у діяльності правоохоронних органів, у результаті якого сформульовано низку нових наукових положень, висновків і пропозицій, розроблених автором особисто.

Зокрема, здобувачем під критичним кутом зору досліджено поняття, зміст і

правову природу інформаційно-комунікаційних технологій у правоохоронній діяльності, запропоновано авторське розуміння їх ролі як інструменту підвищення ефективності управлінських, оперативно-службових та аналітичних процесів за умови дотримання принципів законності, пропорційності, підзвітності та захисту прав людини. Надано комплексну характеристику основних напрямів використання ІКТ і штучного інтелекту в діяльності правоохоронних органів, зокрема в частині автоматизації рутинних процесів, підтримки прийняття рішень, забезпечення особистої безпеки працівників та розвитку їх цифрових і професійних компетентностей.

На підставі аналізу чинного законодавства України, міжнародних стандартів і зарубіжного досвіду обґрунтовано необхідність удосконалення нормативно-правового регулювання цифрової трансформації правоохоронних органів, з урахуванням ризиків, пов'язаних з обробкою персональних і біометричних даних, використанням алгоритмічних систем та впровадженням технологій штучного інтелекту. Автором визначено ключові напрями формування системи правових гарантій при застосуванні ІКТ у правоохоронній діяльності, а також запропоновано підходи до інтеграції цифрової та алгоритмічної грамотності у систему професійної підготовки та підвищення кваліфікації правоохоронців.

Таким чином, отримані під час проведення дисертаційного дослідження результати вирішують конкретне наукове завдання, що має істотне значення для подальшого розвитку теорії інформаційного та адміністративного права, а також для вдосконалення освітнього процесу у сфері підготовки фахівців для правоохоронних органів в умовах цифровізації та впровадження штучного інтелекту.

Комісія констатує, що сформульовані в дисертаційному дослідженні Калюжного Дмитра Олександровича наукові висновки, а також запропоновані теоретичні положення і практичні рекомендації можуть бути використані при підготовці навчальної, науково-методичної та науково-практичної літератури з інформаційного, адміністративного права, а також у межах спеціальних курсів, присвячених цифровій трансформації правоохоронної діяльності.

Члени комісії:

_____ Віталій ПАВЛИКІВСЬКИЙ

_____ Валентин МЕЛЬНИК

_____ Михайло ФІАЛКА

«20» січня 2026 р.