МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ДОНЕЦЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

Кваліфікаційна наукова
праця на правах рукопису

БАТРАК КОСТЯНТИН МИКОЛАЙОВИЧ

УДК 351.74

ДИСЕРТАЦІЯ
ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ В УКРАЇНІ

26 – Цивільна безпека
262 – Правоохоронна діяльність

Подається на здобуття наукового ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело _____ **К.М. Батрак**

Науковий керівник – **Ковальова Ольга Вікторівна**,
доктор юридичних наук, доцент

Кропивницький – 2026

АНОТАЦІЯ

Батрак К.М. Інформаційне забезпечення правоохоронної діяльності в Україні. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня вищої освіти доктора філософії за спеціальністю 262 – «Правоохоронна діяльність». – Донецький державний університет внутрішніх справ, Кропивницький, 2026.

Дисертація є одним із перших монографічних досліджень в якому реалізовано теоретико-правовий підхід щодо інформаційного забезпечення правоохоронної діяльності із визначенням шляхів реалізації низки праксеологічних завдань в умовах воєнного стану.

Здійснена періодизація розвитку інформаційного забезпечення правоохоронної діяльності в Україні шляхом виокремлення протореєстраційного, документально-облікового, криміналістично-ідентифікаційного, централізовано-картотечного, автоматизовано-обчислювального, національно-інформаційного та інтеграційно-цифрового етапів, у межах останнього з яких визначено воєнно-інтеграційний підетап, що дало змогу простежити закономірний перехід від фрагментарного накопичення відомостей до нормативно керованого життєвого циклу даних у правоохоронній сфері.

Надано поняття інформаційного забезпечення правоохоронної діяльності як нормативно врегульованої, організаційно узгодженої й технічно підтримуваної діяльності уповноважених суб’єктів щодо визначення інформаційних потреб, одержання, перевірки, реєстрації, накопичення, систематизації, зберігання, пошуку, зіставлення, аналізу, передавання, використання та захисту відомостей, необхідних для своєчасного, законного й обґрунтованого виконання правоохоронних завдань. Узагальнені наукові підходи щодо змісту інформаційного забезпечення правоохоронної діяльності, за яким правовий режим інформації, взаємодія правоохоронних органів, технічна сумісність інформаційних систем, захист даних, контроль за правомірністю їх

використання та відповідальність уповноважених суб'єктів розглядаються як взаємопов'язані елементи єдиного інформаційно-правоохоронного механізму.

Розроблено структурно-функціональний підхід до використання інформації у правоохоронній діяльності, за яким відомості набувають правоохоронного значення не внаслідок їх наявності в реєстрі, базі даних чи інформаційній системі, а за умови проходження повного циклу: визначення інформаційної потреби, встановлення правової підстави одержання, джерела походження і ступеня перевіреності, розмежування доступу, аналітичного опрацювання, фіксації операцій, захисту даних та персоніфікації відповідальності органу-джерела, органу-користувача, органу-аналітика й органу-координатора за використання інформації у правоохоронному рішенні.

Запропоновані напрями імплементації міжнародно-правових стандартів і зарубіжного досвіду інформаційного забезпечення правоохоронної діяльності в Україні, зокрема щодо ухвалення міжвідомчого нормативно-правового акта про порядок інформаційної взаємодії правоохоронних органів, уніфікації класифікаторів і форматів даних, створення постійного контактного осередку міжнародного інформаційного обміну, закріплення відповідальності органу-джерела за достовірність, повноту й актуальність відомостей, надання доступу до інформації за службовою необхідністю, фіксації кожного запиту, регулярної перевірки якості даних та обов'язкового контролю уповноваженого працівника за результатами автоматизованого аналізу.

Надано поняття електронної готовності впровадження сучасних практик інформаційного забезпечення правоохоронної діяльності в Україні як стану нормативної, організаційної, кадрової, технічної, аналітичної та безпекової спроможності уповноважених суб'єктів використовувати інформаційні ресурси, інформаційно-комунікаційні системи й цифрові інструменти для своєчасного, законного, обґрунтованого та підконтрольного виконання правоохоронних завдань.

Здійснено розподіл інструментів інформаційного забезпечення правоохоронної діяльності на нормативно-правові, організаційні, інформаційно-

ресурсні, інформаційно-аналітичні, техніко-технологічні, безпекові та кадрово-методичні засоби, що розглядаються як взаємопов’язані елементи повного циклу роботи з відомостями.

Окреслений теоретико-правовий підхід до характеристики повноважень правоохоронних органів щодо інформаційного забезпечення правоохоронної діяльності в Україні за такими складовими: створення інформації, що охоплює прийняття заяв, фіксацію подій, реєстрацію кримінальних правопорушень, ведення обліків, формування цифрових документів і внесення даних до реєстрів; доступ і використання інформації, що включає пошук, перевірку, зіставлення, аналіз, отримання відомостей від інших органів та їх застосування під час реагування, оперативно-розшукової діяльності або досудового розслідування; захист і контроль, що передбачає розмежування доступу, реєстрацію дій, перевірку правомірності, актуалізацію даних, виправлення помилок та обмеження подальшого використання відомостей.

Проведено систематизацію інформаційних повноважень правоохоронних органів: повноваження щодо створення і ведення інформаційних систем, реєстрів, баз даних та обліків; повноваження щодо одержання інформації від фізичних, юридичних осіб, органів державної влади, органів місцевого самоврядування та міжнародних партнерів; повноваження щодо доступу до інформаційних ресурсів інших суб’єктів; повноваження щодо перевірки, аналізу, зіставлення та використання відомостей; повноваження щодо передавання інформації в межах міжвідомчої або міжнародної взаємодії; повноваження щодо захисту інформації, розмежування доступу й фіксації операцій; контрольні повноваження щодо законності, актуальності, повноти та цільового використання даних.

Сформульоване теоретичне розуміння форми захисту інформаційних технологій у правоохоронній діяльності як зовнішньо визначеного правом, організаційною процедурою, режимним правилом або технічним стандартом способу забезпечення конфіденційності, цілісності, доступності, достовірності, контрольованості та відновлюваності інформаційних ресурсів, систем, каналів

взаємодії, електронних документів і цифрових доказів, що використовуються під час виконання правоохоронних функцій і завдань. Аргументовано застосування форм захисту інформаційних технологій у сфері правоохоронної діяльності з виокремленням правових, організаційних, режимних, технічних, криптографічних, процедурних, кадрових, контрольних, аналітико-перевірочних, відновлювальних, міжнародно-кооперaційних та етичних форм, що розглядаються як взаємопов'язані способи охорони інформації, інформаційних систем, користувачів, електронних документів, цифрових доказів і каналів електронної взаємодії.

Визначено механізми захисту інформаційних технологій у сфері правоохоронної діяльності із систематизацією за їх функціональним призначенням на превентивні, поточні, моніторингові, реагувальні, відновлювальні, контрольні, механізми службової відповідальності, процесуально-доказові, міжвідомчі та міжнародні, що забезпечує технічну працездатність інформаційних систем, правомірність доступу, захищеність відомостей, перевірюваність інформаційних операцій і належний рух даних від джерела походження до правоохоронного рішення.

Визначені пріоритети оптимізації механізмів захисту інформаційних технологій у правоохоронній діяльності через поєднання ідентифікації інформаційного активу, оцінки ризиків, визначення правового режиму інформації, допуску й авторизації користувача, електронної ідентифікації, розмежування доступу, журналювання, створення та підтримання КСЗІ, криптографічного захисту, реагування на інциденти, резервного відновлення, контролю автоматизованого аналізу та відповідальності за порушення встановленого режиму.

Науково доведено доцільність посиленого захисту інформаційних технологій у сфері правоохоронної діяльності в умовах воєнного стану для забезпечення безперервності роботи інформаційних ресурсів, збереження цифрових доказів, захисту персональних і біометричних даних, протидії кіберінцидентам та недопущення використання спотворених, застарілих або

неперевірених відомостей шляхом правомірного збереження конфіденційності, цілісності, доступності даних та інформаційного шляху їх використання, що охоплює джерело походження, правову підставу доступу, службову мету, режим інформації, дії користувача, журналювання операцій, контрольованість передавання, можливість виправлення помилки та перевірку впливу відомостей на правоохоронне рішення.

Надані рекомендації щодо інформаційної взаємодії правоохоронних органів шляхом ухвалення міжвідомчого нормативно-правового акта про порядок такої взаємодії, закріплення відповідальності органу-джерела за достовірність, повноту й актуальність даних, доступу до інформації за службовою необхідністю, уніфікації класифікаторів і форматів даних, автоматизованої реєстрації дій користувачів, регулярного перегляду актуальності записів та обов’язкового контролю уповноваженого працівника за результатами автоматизованого аналізу з урахуванням умов воєнного стану.

Запропоновані напрями уніфікації електронної взаємодії правоохоронних органів, що передбачають ухвалення міжвідомчого нормативно-правового акта про порядок електронної інформаційної взаємодії, запровадження правових метаданих, уніфікацію класифікаторів і форматів, закріплення відповідальності органу-джерела й органу-користувача, доступ за службовою необхідністю, журналювання кожного запиту, виправлення помилок, захист цифрових доказів і контроль результатів автоматизованого аналізу.

Загалом, обґрунтовано концептуальний підхід до інформаційного забезпечення правоохоронної діяльності в умовах воєнного стану та європейської інтеграції як самостійної організаційно-правової основи належного виконання правоохоронних завдань, зміст якого полягає у правомірному формуванні достовірної, актуальної, захищеної та простежуваної інформаційної основи запобігання, виявлення, припинення, документування й розслідування правопорушень, координації міжвідомчої взаємодії, міжнародного обміну правоохоронною інформацією та прийняття обґрунтованих правоохоронних

рішень, а також у недопущенні використання неперевірених, несумісних, неактуальних або неконтрольовано отриманих даних.

Ключові слова: інформація, інформаційне забезпечення, правоохоронні органи, правоохоронна діяльність, електронна готовність, інформаційні ресурси, інформаційні технології, електронна взаємодія, захист інформації, інформаційна безпека.

ABSTRACT

Batrak K.M. Information Support of Law Enforcement Activities in Ukraine. – Qualifying scientific work submitted as a manuscript.

Dissertation for the degree of Doctor of Philosophy in the specialty 262 – «Law Enforcement Activities». – Donetsk State University of Internal Affairs, Kropyvnytskyi, 2026.

The dissertation is one of the first monographic studies to implement a theoretical and legal approach to information support of law enforcement activities and to identify ways of addressing a range of praxeological tasks under martial law.

The study provides a periodization of the development of information support for law enforcement activities in Ukraine by distinguishing the proto-registration, documentary-record-keeping, forensic-identification, centralised-filing, automated-computing, national-information, and integration-digital stages. Within the latter, a military-integration sub-step is identified, which made it possible to trace the logical transition from fragmented accumulation of information to a normatively regulated data life cycle in the law enforcement sphere.

The concept of information support for law enforcement activities is defined as a normatively regulated, organisationally coordinated, and technically supported activity of authorised entities aimed at identifying information needs; obtaining, verifying, registering, accumulating, systematising, storing, searching, comparing, analysing, transmitting, using, and protecting information necessary for the timely, lawful, and well-founded performance of law enforcement tasks. Scientific approaches to the content of information support for law enforcement activities are generalised, according to which the legal regime of information, interaction among law enforcement bodies, technical compatibility of information systems, data protection, oversight of the lawfulness of their use, and the liability of authorised entities are regarded as interrelated elements of a unified information and law enforcement mechanism.

A structural and functional approach to the use of information in law enforcement activities has been developed, according to which information acquires law enforcement significance not merely by virtue of its presence in a register,

database, or information system, but subject to completion of the full cycle: identification of the information need; establishment of the legal basis for obtaining the information, its source, and degree of verification; access delineation; analytical processing; logging of operations; data protection; and attribution of responsibility to the source body, user body, analytical body, and coordinating body for the use of information in a law enforcement decision.

Directions for implementing international legal standards and foreign experience in information support for law enforcement activities in Ukraine are proposed, including the adoption of an interagency regulatory legal act governing information exchange among law enforcement bodies; unification of data classifiers and formats; establishment of a permanent contact unit for international information exchange; assignment of responsibility to the source body for the accuracy, completeness, and currency of information; provision of access to information on a need-to-know basis; recording of every request; regular data quality checks; and mandatory oversight by an authorised employee of the results of automated analysis.

The concept of electronic readiness for implementing modern practices of information support for law enforcement activities in Ukraine is defined as the state of regulatory, organisational, personnel, technical, analytical, and security capacity of authorised entities to use information resources, information and communication systems, and digital tools for the timely, lawful, well-founded, and controlled performance of law enforcement tasks.

The instruments of information support for law enforcement activities are classified into regulatory and legal, organisational, information-resource, information-analytical, technical and technological, security, and personnel and methodological means, which are regarded as interrelated elements of the complete information-handling cycle.

A theoretical and legal approach to characterising the powers of law enforcement bodies concerning information support for law enforcement activities in Ukraine is outlined according to the following components: information creation, encompassing the acceptance of applications, recording of events, registration of criminal offences,

maintenance of records, creation of digital documents, and entry of data into registers; access to and use of information, including searching, verification, comparison, analysis, obtaining information from other bodies, and its application in response activities, operational-search activities, or pre-trial investigation; and protection and control, involving access delineation, recording of actions, verification of lawfulness, updating of data, correction of errors, and restriction of further use of information.

The information-related powers of law enforcement bodies are systematised as follows: powers to create and maintain information systems, registers, databases, and records; powers to obtain information from individuals, legal entities, state authorities, local self-government bodies, and international partners; powers to access information resources of other entities; powers to verify, analyse, compare, and use information; powers to transmit information within interagency or international cooperation; powers to protect information, delineate access, and record operations; and supervisory powers concerning the lawfulness, currency, completeness, and intended use of data.

A theoretical understanding of a form of information technology protection in law enforcement activities is formulated as a means, externally defined by law, an organisational procedure, a regulatory regime, or a technical standard, of ensuring the confidentiality, integrity, availability, authenticity, controllability, and recoverability of information resources, systems, communication channels, electronic documents, and digital evidence used in the performance of law enforcement functions and tasks. The application of forms of information technology protection in the law enforcement sphere is substantiated, with the identification of legal, organisational, regulatory, technical, cryptographic, procedural, personnel, supervisory, analytical and verification, recovery, international cooperation, and ethical forms, regarded as interrelated means of protecting information, information systems, users, electronic documents, digital evidence, and electronic communication channels.

Mechanisms for protecting information technologies in the law enforcement sphere are identified and systematised according to their functional purpose into preventive, ongoing, monitoring, response, recovery, supervisory, official accountability, procedural and evidentiary, interagency, and international mechanisms.

This classification ensures the technical operability of information systems, lawfulness of access, security of information, verifiability of information operations, and proper movement of data from the source of the information to a law enforcement decision.

The priorities for optimising mechanisms for protecting information technologies in law enforcement activities are identified through the combination of information asset identification, risk assessment, determination of the legal regime of information, user admission and authorisation, electronic identification, access delineation, logging, establishment and maintenance of a Comprehensive Information Protection System (CIPS), cryptographic protection, incident response, backup and recovery, oversight of automated analysis, and liability for violations of the established information regime.

The expediency of enhanced protection of information technologies in the law enforcement sphere under martial law is scientifically substantiated in order to ensure the uninterrupted operation of information resources, preserve digital evidence, protect personal and biometric data, counter cyber incidents, and prevent the use of distorted, outdated, or unverified information through the lawful preservation of data confidentiality, integrity, and availability and control over the information pathway through which such data are used. This pathway encompasses the source of the information, legal basis for access, official purpose, information regime, user actions, logging of operations, control over data transmission, the possibility of correcting errors, and verification of the impact of information on a law enforcement decision.

Recommendations are provided for information interaction among law enforcement bodies through the adoption of an interagency regulatory legal act governing such interaction; assignment of responsibility to the source body for the accuracy, completeness, and currency of data; access to information on a need-to-know basis; unification of data classifiers and formats; automated recording of user actions; regular review of the currency of records; and mandatory oversight by an authorised employee of the results of automated analysis, taking into account the conditions of martial law.

Directions for unifying electronic interaction among law enforcement bodies are proposed, including the adoption of an interagency regulatory legal act governing electronic information exchange; introduction of legal metadata; unification of classifiers and formats; assignment of responsibility to the source body and user body; access on a need-to-know basis; logging of every request; correction of errors; protection of digital evidence; and oversight of the results of automated analysis.

In general, a conceptual approach to information support for law enforcement activities under martial law and in the context of European integration is substantiated as an independent organisational and legal basis for the proper performance of law enforcement tasks. Its substance consists in the lawful formation of a reliable, current, protected, and traceable information foundation for the prevention, detection, suppression, documentation, and investigation of offences; coordination of interagency cooperation; international exchange of law enforcement information; and adoption of well-founded law enforcement decisions, as well as in preventing the use of unverified, incompatible, outdated, or uncontrollably obtained data.

Keywords: information, information support, law enforcement agencies, law enforcement activity, e-readiness, information resources, information technologies, electronic interaction, information protection, information security.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

в яких опубліковані основні наукові результати дисертації:

1. Батрак К. М. Інформаційне забезпечення правоохоронної діяльності в умовах воєнного стану. *Юридичний науковий електронний журнал.* 2024. № 9. С. 200–203.

DOI: https://doi.org/10.32782/2524-0374/2024-9/44

2. Ковальова О. В., Батрак К. М. Міжнародно-правові засади інформаційного забезпечення правоохоронної діяльності в Україні. *Українська поліцеїстика: теорія, законодавство, практика*. 2026. № 1 (17). С. 132–137. (Особистий внесок здобувача: досліджено європейський досвід правового регулювання інформаційних відносин та механізми адаптації стандартів ЄС (GDPR, директиви щодо персональних даних і транс'європейських мереж) до інформаційного забезпечення правоохоронної діяльності в Україні).

DOI: https://doi.org/10.32782/2709-9261-2026-1-17-22

3. Батрак К. М. Інструменти інформаційного забезпечення правоохоронної діяльності в Україні. *Вісник кримінологічної асоціації України*. 2025. № 3(36). С. 668–679.

DOI: https://doi.org/10.32631/vca.2025.3.58

які засвідчують апробацію матеріалів дисертації:

4. Батрак К. М., Юрах В. М. Термінологічні аспекти поняття «інформаційне забезпечення» та класифікація інформації в прокурорській діяльності. *Future of science: innovations and perspectives:* Proceedings of the 3rd International scientific and practical conference. SSPG Publish. Stockholm, Sweden. 2025. Pp. 348–352.

DOI: https://sci-conf.com.ua/wp-content/uploads/2025/01/FUTURE-OF-SCIENCE-INNOVATIONS-AND-PERSPECTIVES-26-28.01.25.pdf

5. Ковальова О. В., Батрак К. М. Організація правоохоронної діяльності в європейських державах: кращі практики. *European congress of scientific discovery:*

Proceedings of the 2nd International scientific and practical conference. Barca Academy Publishing. Madrid, Spain. 2025. Pp. 344–349.

DOI: https://sci-conf.com.ua/wp-content/uploads/2025/02/EUROPEAN-CONGRESS-OF-SCIENTIFIC-DISCOVERY-3-5.02.25.pdf

6. Батрак К. М. Європейські стандарти інформаційного забезпечення правоохоронної діяльності. *Актуальні проблеми юридичної науки та практики у воєнний період*: міжнар. наук.-практ. конф. (Львів, 10 жовт. 2025 р.). Львів. Торунь : Liha-Pres, 2025. С. 177–181.

DOI: https://doi.org/10.36059/978-966-397-550-4-52

які додатково відображають наукові результати дисертації:

7. Батрак К. М. Проблеми та перспективи розвитку інформаційного забезпечення діяльності правоохоронних органів України. *Інтернаука*. 2025. Вип. №6. С. 131–136.

DOI: https://doi.org/10.25313/2520-2057-2025-6-11101

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ 17

ВСТУП 18

РОЗДІЛ 1. СТАНОВЛЕННЯ ТА РОЗВИТОК ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ: НАЦІОНАЛЬНИЙ І МІЖНАРОДНИЙ ВИМІРИ 32

1.1. Генеза інформаційного забезпечення правоохоронної діяльності в Україні 32

1.2. Міжнародно-правові стандарти та зарубіжний досвід інформаційного забезпечення правоохоронної діяльності 55

Висновки до розділу 1 84

РОЗДІЛ 2. ТЕОРЕТИЧНІ ЗАСАДИ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ В УКРАЇНІ 88

2.1. Характеристика електронної готовності впровадження сучасних практик інформаційного забезпечення правоохоронної діяльності в Україні 90

2.2. Інструменти інформаційного забезпечення правоохоронної діяльності в Україні 110

2.3. Характеристика та повноваження правоохоронних органів щодо інформаційного забезпечення правоохоронної діяльності в Україні 127

Висновки до розділу 2 145

РОЗДІЛ 3. ФОРМИ ТА МЕХАНІЗМИ ЗАХИСТУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У СФЕРІ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ 148

3.1. Поняття та види форм захисту інформаційних технологій у сфері правоохоронної діяльності 152

3.2. Механізм захисту інформаційних технологій у сфері правоохоронної діяльності 168

3.3. Шляхи запровадження та уніфікації електронної взаємодії правоохоронних органів у питаннях інформаційного забезпечення та використання інформаційних технологій..... 185

Висновки до розділу 3 200

ВИСНОВКИ..... 203

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ..... 208

ДОДАТКИ..... 227

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

API – прикладний програмний інтерфейс

ISO/IEC – Міжнародна організація зі стандартизації / Міжнародна електротехнічна комісія

АІС ОП – автоматизована інформаційна система оперативного призначення

БЕБ – Бюро економічної безпеки України

ДБР – Державне бюро розслідувань

ДІПКП – Департамент інформаційної підтримки та координації поліції

ДНК – дезоксирибонуклеїнова кислота

ДПСУ – Державна прикордонна служба України

ДТП – дорожньо-транспортна пригода

ЕОМ – електронно-обчислювальна машина

ЄІС МВС – єдина інформаційна система Міністерства внутрішніх справ України

ЄРДР – Єдиний реєстр досудових розслідувань

ЄС – Європейський Союз

ІПНП – інформаційний портал Національної поліції України

ІТ – інформаційні технології

ІТС – інформаційно-телекомунікаційна система

КК України – Кримінальний кодекс України

КПК України – Кримінальний процесуальний кодекс України

КСЗІ – комплексна система захисту інформації

МВС – Міністерство внутрішніх справ України

НАБУ – Національне антикорупційне бюро України

ООН – Організація Об’єднаних Націй

ОРД – оперативно-розшукова діяльність

САП – Спеціалізована антикорупційна прокуратура

СБУ – Служба безпеки України

ТЗІ – технічний захист інформації

ФБР – Федеральне бюро розслідувань США

ШІ – штучний інтелект

ВСТУП

Обґрунтування вибору теми дослідження. Інформаційне забезпечення правоохоронної діяльності в Україні в сучасних умовах набуває значення одного з ключових чинників належного виконання правоохоронних завдань. Від своєчасності, повноти, достовірності, захищеності та правомірності використання інформації залежить здатність правоохоронних органів запобігати правопорушенням, виявляти і припиняти їх, здійснювати розшук осіб, документувати кримінальні правопорушення, забезпечувати публічну безпеку і порядок, протидіяти організованій злочинності, корупції, кіберзагрозам, незаконному обігу зброї, диверсійній діяльності та іншим загрозам національній безпеці. Інформація у правоохоронній сфері дедалі більше виступає перевірюваною основою правоохоронного рішення, що має відповідати вимогам законності, обґрунтованості, цільового призначення, підконтрольності та відповідальності.

В умовах воєнного стану зазначена проблема набула особливого практичного значення, оскільки правоохоронні органи одночасно виконують завдання щодо протидії загальнокримінальній злочинності, документування воєнних злочинів, встановлення осіб, причетних до колабораційної діяльності, розшуку безвісти зниклих, ідентифікації загиблих, перевірки переміщення зброї, захисту критичної інфраструктури, протидії кіберінцидентам та взаємодії з міжнародними партнерами. За таких обставин помилка в інформаційному ресурсі, несвоєчасне оновлення відомостей, неправомірний доступ, дублювання записів, втрата журналів або неконтрольоване передавання даних можуть спричинити не лише організаційні, а й процесуальні, правозахисні та безпекові наслідки.

Розвиток цифрової держави створює додаткові передумови для переосмислення інформаційного забезпечення правоохоронної діяльності. За даними United Nations E-Government Survey 2024, Україна посіла 30 місце за індексом розвитку електронного урядування, 1 місце за індексом електронної

участі та 5 місце за індексом онлайн-послуг [180], що засвідчують істотний прогрес держави у сфері цифрових сервісів, однак у правоохоронній діяльності цифровізація потребує не лише технологічного впровадження, а й належного правового режиму даних, сумісності інформаційних систем, визначення повноважень користувачів, фіксації інформаційних операцій, захисту персональних даних, збереження цифрових доказів та контролю за результатами автоматизованого аналізу.

Кібернетичний вимір проблеми набув особливої гостроти, зокрема у 2024 році CERT-UA опрацювала 4315 кіберінцидентів, що на 69,8 % більше, ніж у 2023 році [130]. Наведені дані засвідчують, що правоохоронні інформаційні ресурси функціонують в умовах постійного ризику кібератак, фішингу, шкідливого програмного забезпечення, атак на доступність, компрометації облікових записів, спотворення або втрати даних, а тому інформаційне забезпечення правоохоронної діяльності потребує дослідження у зв'язку з електронною готовністю органів правопорядку, кіберстійкістю, захистом інформаційних технологій, резервним відновленням, криптографічним захистом, журналюванням доступу та персоніфікацією відповідальності за використання відомостей. На підтвердження, 64,7 % опитаних визнали інформаційне забезпечення визначальною умовою своєчасного й обґрунтованого правоохоронного рішення, 60,3 % оцінили електронну готовність правоохоронних органів як часткову й нерівномірну, 73,7 % підтримали необхідність ухвалення міжвідомчого нормативно-правового акта про порядок інформаційної взаємодії правоохоронних органів, а 80,6 % зазначили, що автоматизований збіг, ризиковий профіль або інший результат машинного аналізу має використовуватися лише як орієнтир для подальшої перевірки уповноваженим працівником. Одержані результати підтверджують запит практики на впорядкування правових, організаційних, технічних і контрольних засад роботи з інформацією у правоохоронній сфері.

Теоретичною основою дослідження стали наукові праці вітчизняних учених, зокрема В. Б. Авер'янова, І. В. Арістової, С. В. Банаха, К. І. Бєлякова,

А. І. Берлача, А. М. Благодарного, Р. І. Благути, В. В. Вітвіцького, А. В. Гарбінської-Руденко, В. П. Горбуліна, Ю. О. Горбаня, С. М. Гусарова, М. В. Гуцалюка, Т. І. Демчук, О. П. Дзьобаня, Д. В. Дубова, К. Ю. Ісмайлова, І. Є. Іванова, І. П. Катеринчука, С. В. Ківалова, О. В. Ковальової, О. Є. Користіна, В. А. Кудінова, В. А. Ліпкана, О. В. Литвиненка, В. П. Маковія, О. А. Марущака, А. В. Мовчана, Н. С. Моргун, В. В. Остроухова, В. Ф. Пашковського, В. М. Петрика, С. В. Петряєва, Б. В. Потятиника, Г. Г. Почепцова, М. М. Присяжнюка, С. В. Сеника, Т. В. Сивак, Г. П. Ситника, Я. В. Свічкарьової, О. В. Таран, В. П. Терехова, Т. В. Ткачука, Г. О. Усатої, Д. В. Федотова, М. Я. Швеця, Х. П. Ярмакі, К. В. Ярового та ін.

Доробок зазначених авторів, безперечно, має важливе наукове та практичне значення. Водночас, окремого наукового осмислення потребує співвідношення інформаційного забезпечення з інформаційно-аналітичною діяльністю, інформаційною безпекою, електронною готовністю правоохоронних органів, формами та механізмами захисту інформаційних технологій. Важливим є також визначення шляхів уніфікації електронної взаємодії правоохоронних органів, запровадження правових метаданих, закріплення відповідальності органу-джерела й органу-користувача, доступу за службовою необхідністю, журналювання кожного запиту, регулярної перевірки актуальності даних, контролю автоматизованого аналізу та поновлення прав особи у разі помилки або неправомірного використання відомостей.

Таким чином, обрана тема дисертації має належне наукове і практичне значення й зумовлена потребою у цілісному осмисленні інформаційного забезпечення правоохоронної діяльності в Україні, визначенні його генези, міжнародно-правових стандартів, теоретичних засад, інструментів, суб’єктних повноважень, форм і механізмів захисту інформаційних технологій, а також шляхів уніфікації електронної взаємодії правоохоронних органів в умовах воєнного стану та європейської інтеграції.

Зв’язок роботи з науковими програмами, планами, темами. Обрана тема дисертаційного дослідження ґрунтується на положеннях Цілей сталого

розвитку України на період до 2030 року, затверджених Указом Президента України від 30 вересня 2019 р. № 722/2019; Комплексного стратегічного плану реформування органів правопорядку як частини сектору безпеки і оборони України на 2023–2027 роки, схваленого Указом Президента України від 11 травня 2023 р. № 273/2023; Стратегії цифрового розвитку інноваційної діяльності України на період до 2030 року, схваленої розпорядженням Кабінету Міністрів України від 31 грудня 2024 р. № 1351-р.; Переліку пріоритетних тематичних напрямів наукових досліджень і науково-технічних розробок на період до 31 грудня року, наступного після припинення або скасування воєнного стану в Україні, затвердженого постановою Кабінету Міністрів України від 30 квітня 2024 р. № 476; Основних наукових напрямів та найважливіших проблем фундаментальних досліджень у галузі природничих, технічних, суспільних і гуманітарних наук Національної академії наук України на 2024–2028 роки, затверджених постановою Президії НАН України від 10 січня 2024 р. № 8.

Тему дисертації затверджено рішенням Вченої ради Донецького державного університету внутрішніх справ 28 листопада 2023 року (протокол № 6).

Мета і завдання дослідження. *Метою* роботи є наукове обґрунтування теоретико-правових та організаційних засад інформаційного забезпечення правоохоронної діяльності в Україні, а також розроблення практичних рекомендацій з урахуванням умов воєнного стану та європейської інтеграції.

Для досягнення зазначеної мети поставлено такі завдання:

– з’ясувати генезу інформаційного забезпечення правоохоронної діяльності в Україні та визначити основні етапи його становлення і розвитку;

– розкрити зміст інформаційного забезпечення правоохоронної діяльності, його співвідношення з інформаційно-аналітичним забезпеченням, інформаційною безпекою та використанням інформаційних технологій;

– узагальнити міжнародно-правові стандарти та зарубіжний досвід інформаційного забезпечення правоохоронної діяльності;

– визначити електронну готовність правоохоронних органів України до впровадження сучасних практик інформаційного забезпечення;

– систематизувати інструменти інформаційного забезпечення правоохоронної діяльності в Україні;

– охарактеризувати повноваження правоохоронних органів щодо створення, одержання, перевірки, аналізу, передавання, використання і захисту відомостей;

– визначити поняття та види форм захисту інформаційних технологій у сфері правоохоронної діяльності;

– розкрити механізми захисту інформаційних технологій у сфері правоохоронної діяльності;

– обґрунтувати шляхи запровадження та уніфікації електронної взаємодії правоохоронних органів у питаннях інформаційного забезпечення та використання інформаційних технологій;

– сформулювати науково обґрунтовані пропозиції щодо вдосконалення правового, організаційного, інформаційно-аналітичного, техніко-технологічного та безпекового забезпечення правоохоронної діяльності в Україні.

Об'єкт дослідження – суспільні відносини, що виникають у процесі інформаційного забезпечення правоохоронної діяльності в Україні.

Предмет дослідження – інформаційне забезпечення правоохоронної діяльності в Україні.

Методи дослідження. Для досягнення мети та виконання завдань використано комплекс загальнонаукових і спеціальних методів дослідження. *Історико-правовий* метод дозволив з'ясувати генезу інформаційного забезпечення правоохоронної діяльності, визначити основні етапи його становлення та простежити перехід від первинної фіксації відомостей до сучасних цифрових форм роботи з даними (підрозділ 1.1). *Логіко-семантичний* метод використано для уточнення понятійного апарату дослідження, зокрема понять «інформаційне забезпечення правоохоронної діяльності», «електронна готовність правоохоронних органів», «інструменти інформаційного

забезпечення», «форми захисту інформаційних технологій», «механізми захисту інформаційних технологій», «правові метадані», «службова необхідність доступу» (підрозділи 1.1, 2.1, 2.2, 3.1, 3.2). *Формально-юридичний* метод використано для аналізу нормативно-правових актів, міжнародних договорів, актів Ради Європи та права Європейського Союзу, що визначають правові підстави створення, одержання, перевірки, використання, передавання та захисту інформації у правоохоронній сфері (підрозділи 1.2, 2.2, 2.3, 3.1–3.3). За допомогою *порівняльного* методу узагальнено міжнародно-правові стандарти та зарубіжний досвід інформаційного забезпечення правоохоронної діяльності (підрозділ 1.2). *Системно-структурний* метод застосовано для характеристики інформаційного забезпечення як цілісної системи, що охоплює правові, організаційні, суб'єктні, інформаційно-ресурсні, аналітичні, техніко-технологічні, безпекові та кадрово-методичні складові (підрозділи 2.1, 2.2). *Структурно-функціональний* метод дав змогу систематизувати інформаційні повноваження правоохоронних органів і визначити роль органу-джерела, органу-користувача, адміністратора інформаційного ресурсу, аналітичного підрозділу та суб'єкта контролю у повному циклі роботи з відомостями (підрозділ 2.3). *Праксеологічний* метод використано для оцінювання інформаційного забезпечення з погляду його придатності для виконання конкретних правоохоронних завдань (підрозділи 2.1–2.3, 3.3). *Класифікаційний* метод дав змогу виокремити форми захисту інформаційних технологій та систематизувати механізми їх реалізації за функціональним призначенням (підрозділи 3.1, 3.2). Метод *моделювання* використано під час розроблення структурно-функціонального підходу до використання інформації у правоохоронній діяльності та обґрунтування моделі міжвідомчого нормативно-правового акта про порядок електронної інформаційної взаємодії правоохоронних органів (підрозділи 2.3, 3.3). *Прогностичний* метод застосовано для визначення напрямів розвитку інформаційного забезпечення правоохоронної діяльності в умовах воєнного стану, цифрової трансформації, європейської інтеграції (підрозділи 1.2, 3.2, 3.3). *Соціологічний* метод використано під час

анкетування респондентів. *Статистичний* метод забезпечив узагальнення одержаних емпіричних даних і визначення кількісних показників підтримки окремих положень дослідження (розділи 2–3).

Нормативну основу дослідження становлять Конституція України, міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, акти Ради Європи та Європейського Союзу, а також національні нормативно-правові акти законодавчого й підзаконного рівнів. Особливе значення для дослідження мають КПК України, закони України «Про інформацію», «Про захист персональних даних», «Про захист інформації в інформаційно-комунікаційних системах», «Про основні засади забезпечення кібербезпеки України», «Про публічні електронні реєстри», «Про електронні документи та електронний документообіг», «Про електронну ідентифікацію та електронні довірчі послуги», «Про Національну поліцію», «Про оперативно-розшукову діяльність», «Про державну таємницю», «Про доступ до публічної інформації», «Про критичну інфраструктуру», «Про хмарні послуги», а також нормативно-правові акти, що регламентують діяльність СБУ, ДБР, БЕБ, НАБУ, ДПСУ та інших суб'єктів правоохоронної діяльності.

Науково-теоретичне підґрунтя роботи сформували праці вітчизняних і зарубіжних учених у галузі правоохоронної діяльності, адміністративного та інформаційного права, кримінального процесу, кримінального аналізу, інформаційної безпеки, кібербезпеки. Використання відповідного наукового доробку дозволило розкрити генезу, зміст, структуру, принципи, інструменти, суб'єктні повноваження, форми і механізми інформаційного забезпечення правоохоронної діяльності, а також обґрунтувати напрями уніфікації електронної взаємодії правоохоронних органів в умовах воєнного стану та європейської інтеграції України.

Інформаційну основу дослідження становлять офіційні статистичні, аналітичні й довідкові матеріали органів державної влади України, міжнародних організацій, Ради Європи, Європейського Союзу, Європолу, Інтерполу, CERT-UA, Державної служби спеціального зв'язку та захисту інформації України, а

також матеріали, що характеризують практику використання інформаційних ресурсів, електронних реєстрів, інформаційно-аналітичних систем, відкритих джерел, цифрових доказів і захищених каналів обміну у правоохоронній сфері.

Емпіричну базу роботи становлять результати анкетування 155 працівників Національної поліції України та 210 працівників закладів вищої освіти системи МВС України, а також узагальнення практики інформаційного забезпечення правоохоронної діяльності, міжвідомчої взаємодії, захисту інформаційних технологій і використання автоматизованого аналізу в діяльності органів правопорядку.

Наукова новизна одержаних результатів полягає в тому, що дисертація є одним із перших монографічних досліджень, у якому науково обґрунтовано теоретико-правові та організаційні засади інформаційного забезпечення правоохоронної діяльності в Україні, а також визначено напрями удосконалення правового регулювання, електронної взаємодії, використання й захисту інформаційних ресурсів для своєчасного, законного й обґрунтованого виконання правоохоронних завдань в умовах воєнного стану та європейської інтеграції. До найбільш значущих наукових положень, що визначають новизну дисертації, належать такі:

вперше:

– обґрунтовано концептуальний підхід до інформаційного забезпечення правоохоронної діяльності в умовах воєнного стану та європейської інтеграції як самостійної організаційно-правової основи належного виконання правоохоронних завдань, зміст якого полягає у правомірному формуванні достовірної, актуальної, захищеної та простежуваної інформаційної основи запобігання, виявлення, припинення, документування й розслідування правопорушень, координації міжвідомчої взаємодії, міжнародного обміну правоохоронною інформацією та прийняття обґрунтованих правоохоронних

рішень, а також у недопущенні використання неперевірених, несумісних, неактуальних або неконтрольовано отриманих даних;

– розроблено структурно-функціональний підхід до використання інформації у правоохоронній діяльності, за яким відомості набувають правоохоронного значення не внаслідок їх наявності в реєстрі, базі даних чи інформаційній системі, а за умови проходження повного циклу: визначення інформаційної потреби, встановлення правової підстави одержання, джерела походження і ступеня перевіреності, розмежування доступу, аналітичного опрацювання, фіксації операцій, захисту даних та персоніфікації відповідальності органу-джерела, органу-користувача, органу-аналітика й органу-координатора за використання інформації у правоохоронному рішенні;

– аргументовано застосування форм захисту інформаційних технологій у сфері правоохоронної діяльності з виокремленням правових, організаційних, режимних, технічних, криптографічних, процедурних, кадрових, контрольних, аналітико-перевірочних, відновлювальних, міжнародно-кооперaційних та етичних форм, що розглядаються як взаємопов’язані способи охорони інформації, інформаційних систем, користувачів, електронних документів, цифрових доказів і каналів електронної взаємодії;

– визначено механізми захисту інформаційних технологій у сфері правоохоронної діяльності із систематизацією за їх функціональним призначенням на превентивні, поточні, моніторингові, реагувальні, відновлювальні, контрольні, механізми службової відповідальності, процесуально-доказові, міжвідомчі та міжнародні, що забезпечує технічну працездатність інформаційних систем, правомірність доступу, захищеність відомостей, перевірюваність інформаційних операцій і належний рух даних від джерела походження до правоохоронного рішення;

– науково доведено доцільність посиленого захисту інформаційних технологій у сфері правоохоронної діяльності в умовах воєнного стану для забезпечення безперервності роботи інформаційних ресурсів, збереження цифрових доказів, захисту персональних і біометричних даних, протидії

кіберінцидентам та недопущення використання спотворених, застарілих або неперевірених відомостей шляхом правомірного збереження конфіденційності, цілісності, доступності даних та інформаційного шляху їх використання, що охоплює джерело походження, правову підставу доступу, службову мету, режим інформації, дії користувача, журналювання операцій, контрольованість передавання, можливість виправлення помилки та перевірку впливу відомостей на правоохоронне рішення;

удосконалено:

– поняття інформаційного забезпечення правоохоронної діяльності як нормативно врегульованої, організаційно узгодженої й технічно підтримуваної діяльності уповноважених суб'єктів щодо визначення інформаційних потреб, одержання, перевірки, реєстрації, накопичення, систематизації, зберігання, пошуку, зіставлення, аналізу, передавання, використання та захисту відомостей, необхідних для своєчасного, законного й обґрунтованого виконання правоохоронних завдань;

– науковий підхід до змісту інформаційного забезпечення правоохоронної діяльності, за яким правовий режим інформації, взаємодія правоохоронних органів, технічна сумісність інформаційних систем, захист даних, контроль за правомірністю їх використання та відповідальність уповноважених суб'єктів розглядаються як взаємопов'язані елементи єдиного інформаційно-правоохоронного механізму;

– поняття електронної готовності впровадження сучасних практик інформаційного забезпечення правоохоронної діяльності в Україні як стану нормативної, організаційної, кадрової, технічної, аналітичної та безпекової спроможності уповноважених суб'єктів використовувати інформаційні ресурси, інформаційно-комунікаційні системи й цифрові інструменти для своєчасного, законного, обґрунтованого та підконтрольного виконання правоохоронних завдань;

– розподіл інструментів інформаційного забезпечення правоохоронної діяльності на нормативно-правові, організаційні, інформаційно-ресурсні,

інформаційно-аналітичні, техніко-технологічні, безпекові та кадрово-методичні засоби, що розглядаються як взаємопов’язані елементи повного циклу роботи з відомостями;

– систематизацію інформаційних повноважень правоохоронних органів: повноваження щодо створення і ведення інформаційних систем, реєстрів, баз даних та обліків; повноваження щодо одержання інформації від фізичних, юридичних осіб, органів державної влади, органів місцевого самоврядування та міжнародних партнерів; повноваження щодо доступу до інформаційних ресурсів інших суб’єктів; повноваження щодо перевірки, аналізу, зіставлення та використання відомостей; повноваження щодо передавання інформації в межах міжвідомчої або міжнародної взаємодії; повноваження щодо захисту інформації, розмежування доступу й фіксації операцій; контрольні повноваження щодо законності, актуальності, повноти та цільового використання даних;

– теоретичне розуміння форми захисту інформаційних технологій у правоохоронній діяльності як зовнішньо визначеного правом, організаційною процедурою, режимним правилом або технічним стандартом способу забезпечення конфіденційності, цілісності, доступності, достовірності, контрольованості та відновлюваності інформаційних ресурсів, систем, каналів взаємодії, електронних документів і цифрових доказів, що використовуються під час виконання правоохоронних функцій і завдань;

дістало подальший розвиток:

– періодизація розвитку інформаційного забезпечення правоохоронної діяльності в Україні шляхом виокремлення протореєстраційного, документально-облікового, криміналістично-ідентифікаційного, централізовано-картотечного, автоматизовано-обчислювального, національно-інформаційного та інтеграційно-цифрового етапів, у межах останнього з яких визначено воєнно-інтеграційний підетап, що дало змогу простежити

закономірний перехід від фрагментарного накопичення відомостей до нормативно керованого життєвого циклу даних у правоохоронній сфері;

– напрями імплементації міжнародно-правових стандартів і зарубіжного досвіду інформаційного забезпечення правоохоронної діяльності в Україні, зокрема щодо ухвалення міжвідомчого нормативно-правового акта про порядок інформаційної взаємодії правоохоронних органів, уніфікації класифікаторів і форматів даних, створення постійного контактного осередку міжнародного інформаційного обміну, закріплення відповідальності органу-джерела за достовірність, повноту й актуальність відомостей, надання доступу до інформації за службовою необхідністю, фіксації кожного запиту, регулярної перевірки якості даних та обов'язкового контролю уповноваженого працівника за результатами автоматизованого аналізу;

– теоретико-правовий підхід до характеристики повноважень правоохоронних органів щодо інформаційного забезпечення правоохоронної діяльності в Україні за такими складовими: створення інформації, що охоплює прийняття заяв, фіксацію подій, реєстрацію кримінальних правопорушень, ведення обліків, формування цифрових документів і внесення даних до реєстрів; доступ і використання інформації, що включає пошук, перевірку, зіставлення, аналіз, отримання відомостей від інших органів та їх застосування під час реагування, оперативно-розшукової діяльності або досудового розслідування; захист і контроль, що передбачає розмежування доступу, реєстрацію дій, перевірку правомірності, актуалізацію даних, виправлення помилок та обмеження подальшого використання відомостей;

– рекомендації щодо інформаційної взаємодії правоохоронних органів шляхом ухвалення міжвідомчого нормативно-правового акта про порядок такої взаємодії, закріплення відповідальності органу-джерела за достовірність, повноту й актуальність даних, доступу до інформації за службовою необхідністю, уніфікації класифікаторів і форматів даних, автоматизованої реєстрації дій користувачів, регулярного перегляду актуальності записів та

обов’язкового контролю уповноваженого працівника за результатами автоматизованого аналізу з урахуванням умов воєнного стану;

– пріоритети оптимізації механізмів захисту інформаційних технологій у правоохоронній діяльності через поєднання ідентифікації інформаційного активу, оцінки ризиків, визначення правового режиму інформації, допуску й авторизації користувача, електронної ідентифікації, розмежування доступу, журналювання, створення та підтримання КСЗІ, криптографічного захисту, реагування на інциденти, резервного відновлення, контролю автоматизованого аналізу та відповідальності за порушення встановленого режиму;

– напрями уніфікації електронної взаємодії правоохоронних органів, що передбачають ухвалення міжвідомчого нормативно-правового акта про порядок електронної інформаційної взаємодії, запровадження правових метаданих, уніфікацію класифікаторів і форматів, закріплення відповідальності органу-джерела й органу-користувача, доступ за службовою необхідністю, журналювання кожного запиту, виправлення помилок, захист цифрових доказів і контроль результатів автоматизованого аналізу.

Практичне значення одержаних результатів полягає в тому, що сформульовані в дисертації положення, висновки і пропозиції становлять науково-теоретичний та прикладний інтерес і можуть бути використані у:

– *науково-дослідній сфері* – як основа для подальшого розроблення теоретико-правових, організаційних і прикладних засад інформаційного забезпечення правоохоронної діяльності, електронної готовності правоохоронних органів, міжвідомчої інформаційної взаємодії, використання інформаційних технологій та захисту інформаційних ресурсів у правоохоронній сфері (акт Донецького державного університету внутрішніх справ від 05.10.2026 р.);

– *практичній діяльності правоохоронних органів* – для удосконалення організаційних процедур одержання, перевірки, реєстрації, накопичення, систематизації, аналізу, передавання, використання та захисту відомостей, підвищення ефективності міжвідомчої й міжнародної інформаційної взаємодії,

запровадження правових метаданих, контролю автоматизованого аналізу та персоніфікації відповідальності за використання інформації у правоохоронних рішеннях;

– *освітньому процесі* – під час підготовки підручників, навчальних посібників, курсів лекцій, методичних рекомендацій, практикумів, тестових завдань та інших дидактичних матеріалів з навчальних дисциплін «Правоохоронна діяльність», «Інформаційне забезпечення правоохоронної діяльності», «Кримінальний аналіз», «Інформаційна безпека», «Кібербезпека», «Використання інформаційних технологій у правоохоронній діяльності» (акт Донецького державного університету внутрішніх справ від 07.10.2026 р.).

Апробація матеріалів дисертації. Основні положення та результати дослідження оприлюднено на науково-практичних конференціях: «Future of science: innovations and perspectives» (м. Стокгольм, 26-28 січ. 2025 р.); «European congress of scientific discovery» (м. Мадрід, 3-5 лют. 2025 р.); «Актуальні проблеми юридичної науки та практики у воєнний період (м. Львів, 10 жовт. 2025 р.).

Публікації. Основні наукові результати дисертації відображено у семи публікаціях, із яких три статті опубліковано у наукових фахових виданнях України, три праці – у збірниках матеріалів науково-практичних конференцій, та одна стаття – у міжнародному науковому журналі.

Структура та обсяг дисертації. Робота складається з анотації, переліку умовних позначень, вступу, трьох розділів, що містять вісім підрозділів, висновків, списку використаних джерел (182 найменування на 19 сторінках) та трьох додатків на 16 сторінках. Повний обсяг дисертації становить 242 сторінки, із них основний текст дисертації – 177 сторінок.

РОЗДІЛ 1. СТАНОВЛЕННЯ ТА РОЗВИТОК ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ: НАЦІОНАЛЬНИЙ І МІЖНАРОДНИЙ ВИМІРИ

1.1. Генеза інформаційного забезпечення правоохоронної діяльності в Україні

У сучасних умовах інформація є однією з визначальних передумов належної організації правоохоронної діяльності, оскільки саме від своєчасності, повноти, достовірності та захищеності відомостей залежить здатність уповноважених органів виявляти, попереджати, припиняти й розслідувати кримінальні та інші протиправні прояви. Зростання транснаціональної організованої злочинності, поширення кіберзагроз, терористичних ризиків, незаконного обігу зброї, корупційних практик, а в умовах воєнного стану також необхідність документування воєнних злочинів і забезпечення міжнародної взаємодії у сфері безпеки, істотно підвищують значення правових механізмів обміну, обробки, перевірки та захисту інформації. За таких умов інформаційне забезпечення правоохоронної діяльності набуває не лише внутрішньоорганізаційного, а й міжнародно-правового значення, оскільки ефективність реагування на сучасні загрози значною мірою залежить від узгодженості дій національних правоохоронних органів з компетентними органами іноземних держав та міжнародними організаціями.

Міжнародне співробітництво у сфері інформаційного забезпечення правоохоронної діяльності ґрунтується на поєднанні потреби в оперативному обміні відомостями з обов’язком держав забезпечувати дотримання прав людини, захист персональних даних, повагу до державного суверенітету, належний рівень інформаційної безпеки та недопущення свавільного використання інформаційних ресурсів. Саме тому інформаційний обмін у правоохоронній сфері не може розглядатися як суто технічна передача даних. За

своїм змістом він є правовою формою міжнародної взаємодії, у межах якої мають бути чітко визначені суб'єкти обміну, підстави доступу до інформації, мета її використання, строки зберігання, порядок перевірки достовірності, режим захисту та відповідальність за неправомірне поширення чи використання відомостей.

Україна як суб'єкт міжнародного правоохоронного співробітництва поступово адаптує національну систему інформаційного забезпечення до міжнародних і європейських стандартів. Вказаний процес охоплює імплементацію міжнародно-правових норм, розвиток співпраці з Інтерполом, Європолом, Організацією Об'єднаних Націй, Радою Європи, інституціями Європейського Союзу, а також удосконалення двосторонніх і багатосторонніх механізмів обміну правоохоронною інформацією. Практичне значення такої взаємодії виявляється у протидії організованій злочинності, кіберзлочинності, тероризму, корупції, незаконній міграції, торгівлі людьми, легалізації доходів, одержаних злочинним шляхом, а також у збиранні, перевірці та передаванні інформації, необхідної для документування кримінальних правопорушень, пов'язаних зі збройною агресією проти України.

Нормативну основу міжнародного інформаційного обміну у правоохоронній сфері становлять, зокрема, Конвенція Організації Об'єднаних Націй проти транснаціональної організованої злочинності 2000 року, Конвенція Ради Європи про кіберзлочинність 2001 року, Глобальна контртерористична стратегія ООН, документи Ради Європи щодо захисту персональних даних, а також акти Європейського Союзу, спрямовані на врегулювання обробки інформації, захисту даних і поліцейського співробітництва. Значення цих актів полягає в тому, що вони формують не лише загальні напрями співпраці, а й правові межі використання інформації у правоохоронній діяльності. Йдеться, зокрема, про вимоги законності, цільового призначення, пропорційності, достовірності, актуальності, захищеності та контрольованості обробки даних.

Поряд із міжнародними зобов'язаннями важливе значення має національне правове регулювання інформаційного забезпечення правоохоронної діяльності.

Воно охоплює законодавство про інформацію, доступ до публічної інформації, захист інформації в інформаційно-комунікаційних системах, захист персональних даних, оперативно-розшукову діяльність, кримінальне провадження, кібербезпеку, а також спеціальні нормативно-правові акти, що визначають правовий статус, завдання і повноваження Національної поліції України, Служби безпеки України, Державного бюро розслідувань, Бюро економічної безпеки України, органів прокуратури, Державної прикордонної служби України та інших суб'єктів правоохоронної діяльності. У цьому контексті національне регулювання має забезпечувати не лише доступ уповноважених органів до необхідних інформаційних ресурсів, а й належний баланс між інтересами безпеки, потребами кримінального провадження, захистом прав людини та вимогами інформаційної безпеки.

Отже, міжнародно-правові засади інформаційного забезпечення правоохоронної діяльності в Україні доцільно розглядати як систему правових принципів, стандартів і механізмів, що визначають порядок отримання, обробки, обміну, використання та захисту інформації у взаємодії національних правоохоронних органів з іноземними державами й міжнародними організаціями. Їх дослідження дає змогу встановити ступінь узгодженості національного законодавства з міжнародними стандартами, виявити проблеми міжвідомчої та міжнародної інформаційної взаємодії, а також визначити напрями подальшого розвитку інформаційного забезпечення правоохоронної діяльності в умовах воєнного стану, цифровізації та європейської інтеграції України.

Водночас з'ясування витоків інформаційного забезпечення правоохоронної діяльності в Україні потребує звернення до історико-правового розвитку української державності, оскільки способи одержання, фіксації, накопичення, передавання та використання відомостей завжди залежали від стану публічної влади, рівня правового регулювання, характеру загроз правопорядку та організаційної побудови органів, наділених охоронними й правоохоронними повноваженнями. У зв'язку з цим генезу інформаційного

забезпечення доцільно розглядати не як історію появи окремих обліків, реєстрів чи технічних засобів, а як поступове формування правових, організаційних і процедурних умов, за яких інформація починає виконувати самостійну забезпечувальну функцію у правоохоронній діяльності.

Наукове осмислення генези інформаційного забезпечення правоохоронної діяльності потребує попереднього уточнення змісту базових понять. У юридичній літературі інформаційне забезпечення нерідко ототожнюють з інформаційно-аналітичною діяльністю, інформаційною підтримкою, інформатизацією або використанням інформаційних технологій. Такий підхід звужує досліджуване явище, оскільки зводить його або до сукупності технічних засобів, або до аналітичної обробки вже одержаних відомостей. Як слушно зазначає І. П. Катеринчук, правова природа інформаційного забезпечення правоохоронних органів розкривається через поєднання правового регулювання, організаційних процедур, інформаційних ресурсів і діяльності уповноважених суб’єктів [35, с. 10]. С. Банах, досліджуючи історико-правові особливості цього явища, також пов’язує його розвиток із загальними змінами способів накопичення, передавання та використання відомостей у правоохоронній сфері [3, с. 14]. Отже, технічна складова є необхідною, проте не визначальною ознакою інформаційного забезпечення, оскільки сама по собі наявність інформаційних систем не гарантує законності, достовірності, своєчасності й придатності відомостей для виконання правоохоронних завдань.

У науковій літературі підходи до розуміння інформаційного забезпечення правоохоронної діяльності відрізняються насамперед за тим, який його складник визнається провідним. У межах управлінського підходу інформаційне забезпечення розглядається як умова підготовки, прийняття та реалізації обґрунтованих правоохоронних рішень. Діяльнісний підхід акцентує увагу на послідовності операцій з інформацією: її одержанні, перевірці, реєстрації, накопиченні, систематизації, зберіганні, пошуку, зіставленні, аналізі, передаванні, використанні та захисті. Системний підхід дає змогу охопити суб’єктів, інформаційні ресурси, правові приписи, організаційні зв’язки,

технічну інфраструктуру та процедури контролю як взаємопов’язані елементи єдиного механізму. На нашу думку, зазначені підходи не суперечать один одному, а розкривають різні рівні одного правового явища: управлінський підхід пояснює його призначення, діяльнісний – внутрішню послідовність інформаційних процесів, системний – будову, зв’язки та межі функціонування.

Саме поєднання таких підходів дозволяє уникнути спрощеного розуміння інформаційного забезпечення правоохоронної діяльності як механічного накопичення даних. Для правоохоронної сфери, особливо в умовах воєнного стану, принципове значення має не лише наявність відомостей, а й можливість встановити їх походження, перевірити достовірність, забезпечити своєчасний доступ уповноваженого працівника, простежити шлях використання інформації у конкретному правоохоронному рішенні та визначити відповідальність за наслідки такого використання. У цьому контексті інформаційне забезпечення виступає не допоміжним технічним процесом, а організаційно-правовою передумовою ефективного виконання правоохоронних завдань, зокрема щодо запобігання кримінальним правопорушенням, їх виявлення, припинення, документування, розслідування та забезпечення взаємодії між уповноваженими суб’єктами.

Інформаційно-аналітичне забезпечення доцільно розглядати як функціонально поглиблену складову інформаційного забезпечення правоохоронної діяльності. Його призначення полягає не лише у впорядкуванні масиву даних, а й у формуванні аналітично опрацьованого знання, придатного для підготовки правоохоронного рішення. Таким результатом може бути аналітична довідка, оцінка ризику, прогноз розвитку криміногенної ситуації, встановлення зв’язків між подіями, особами, об’єктами, територіями, способами вчинення правопорушень або каналами протиправної діяльності. Як обґрунтовує В. Терехов, інформаційно-аналітичне дослідження має творчо-інтелектуальний характер і спрямоване на одержання нового аналітичного продукту на підставі зібраних та оброблених даних [115, с. 103–106]. Такий підхід заслуговує на підтримку, оскільки в правоохоронній діяльності значення має не будь-яке

накопичення відомостей, а їх перетворення на перевірену, структуровану й придатну для практичного використання інформаційну основу.

Водночас аналітичний висновок не слід ототожнювати з управлінським, оперативно-службовим або процесуальним рішенням. Він може обґрунтовувати напрям подальшої перевірки, вказувати на ризики, підтверджувати або спростовувати інформаційну версію, однак не замінює компетенцію уповноваженої службової особи. Таке розмежування має принципове значення для правоохоронної діяльності, особливо в умовах воєнного стану, коли зростає обсяг цифрових даних, повідомлень з відкритих джерел, результатів автоматизованої обробки та міжвідомчого інформаційного обміну. За цих обставин аналітичний продукт повинен залишатися перевірюваним за джерелом походження, способом отримання, логікою обробки та межами допустимого використання, а юридично значуще рішення має бути персоніфікованим, мотивованим і прийнятим уповноваженим суб’єктом у межах його повноважень.

Не збігаються за змістом також інформаційне забезпечення та інформаційна безпека правоохоронного органу. Інформаційне забезпечення спрямоване на задоволення інформаційних потреб правоохоронної діяльності та створення належної основи для своєчасного, законного й обґрунтованого виконання правоохоронних завдань. Інформаційна безпека, у свою чергу, характеризує стан захищеності інформації, інформаційних ресурсів, інформаційно-комунікаційних систем і процесів від випадкових та умисних загроз. В. П. Маковій і Г. О. Усата пов’язують інформаційно-аналітичну підтримку поліції з організаційно-правовими й технічними заходами забезпечення інформаційної безпеки держави [48, с. 62]. Погоджуючись із взаємозалежністю цих категорій, вважаємо методологічно неправильним поглинати одну іншою, оскільки інформаційна безпека визначає режим захищеності інформаційного середовища, а інформаційне забезпечення характеризує організовану діяльність із формування, обробки та використання відомостей для досягнення правоохоронної мети.

Для правоохоронної сфери принципове значення має збалансованість між

доступністю інформації та її захищеністю. Надмірне обмеження доступу заради безпеки може знизити оперативність реагування, ускладнити міжвідомчу взаємодію та негативно вплинути на своєчасність виконання правоохоронних завдань. Водночас необґрунтоване розширення доступу створює ризики витоку, спотворення, незаконного поширення або використання даних не за призначенням. Належна організація інформаційного забезпечення має гарантувати одночасно доступність інформації для уповноваженого користувача, її цілісність, достовірність, актуальність, конфіденційність, захищеність і простежуваність усіх дій з нею.

Інформаційне забезпечення правоохоронної діяльності слід розглядати не як допоміжну технічну функцію, а як наскрізний напрям організації та здійснення правоохоронної діяльності, яке супроводжує запобігання правопорушенням, їх виявлення і припинення, досудове розслідування, оперативно-розшукову діяльність, охорону публічної безпеки і порядку, розшук осіб, прикордонний та митний контроль, протидію корупції, забезпечення економічної безпеки, документування правопорушень, пов’язаних зі збройною агресією проти України, а також управління силами й засобами в ускладнених безпекових умовах. Результати анкетування підтверджують практичну значущість такого підходу: 64,7 % опитаних вважають інформаційне забезпечення визначальною умовою своєчасного й обґрунтованого правоохоронного рішення, а ще 28,0 % пов’язують його результативність з організаційними умовами діяльності органу правопорядку (додаток Б). У кожному з названих напрямів відрізняються правові підстави роботи з інформацією, склад відомостей, строки їх зберігання, коло користувачів, режими доступу та допустимі способи оброблення. Спільними залишаються вимоги законності, цільового призначення, достатності, достовірності, своєчасності, захищеності, підконтрольності та відповідальності за використання інформації.

Саме за цими ознаками інформаційне забезпечення набуває правоохоронної специфіки й відрізняється від загального інформаційного супроводу діяльності органів публічної адміністрації. У правоохоронній сфері

інформація безпосередньо пов’язана з реалізацією владних повноважень, обмеженням прав і свобод людини у встановлених законом випадках, прийняттям рішень щодо реагування на правопорушення, застосуванням заходів примусу, забезпеченням доказування, розшуком осіб, захистом публічної безпеки та виконанням міжнародних зобов’язань України. Тому інформаційне забезпечення правоохоронної діяльності повинно оцінюватися не лише за швидкістю доступу до даних або технічними можливостями інформаційних систем, а й за здатністю забезпечити законність, обґрунтованість, перевірюваність і правомірність використання відомостей.

У сучасному навчальному посібнику В. А. Кудінова та К. В. Ярового інформаційне забезпечення розглядається як системна умова виконання правоохоронних завдань [46]. Як стверджує Т. І. Демчук, інформаційно-аналітичні й організаційні методи мають застосовуватися у взаємозв’язку, оскільки якість відомостей без належної організації їх опрацювання не забезпечує обґрунтованого рішення [18, с. 430–436]. На підставі узагальнення доктринальних позицій пропонуємо розуміти *інформаційне забезпечення правоохоронної діяльності як нормативно врегульовану, організаційно узгоджену й технічно підтримувану діяльність уповноважених суб’єктів щодо визначення інформаційних потреб, одержання, перевірки, реєстрації, накопичення, систематизації, зберігання, пошуку, зіставлення, аналізу, передавання, використання та захисту відомостей, необхідних для своєчасного, законного й обґрунтованого виконання правоохоронних завдань*.

Запропоноване визначення охоплює п’ять взаємопов’язаних складників: правовий, суб’єктний, ресурсний, діяльнісний і технічний. Правовий складник визначає підстави, межі, режими доступу та відповідальність за використання інформації. Суб’єктний складник характеризує коло органів, посадових осіб та інших уповноважених учасників, які створюють, отримують, обробляють, передають або використовують відповідні відомості. Ресурсний складник охоплює інформаційні масиви, обліки, реєстри, бази даних, документи та інші джерела інформації. Діяльнісний складник відображає послідовність операцій з

інформацією від визначення потреби до її використання і захисту. Технічний складник забезпечує функціонування інформаційних систем, каналів зв'язку, засобів захисту та інструментів обробки даних. Перевага такого підходу полягає в тому, що кінцевим результатом інформаційного забезпечення визнається не функціонування бази даних саме по собі, а належне виконання правоохоронного завдання з дотриманням законності, прав людини та вимог інформаційної безпеки.

У додержавний період передумови майбутньої правоохоронної функції формувалися в межах родоплемінної організації суспільства. Дотримання звичаїв, заборон і традиційних правил поведінки сприймалося як обов'язкова умова існування роду чи племені, а їх порушення тягнуло громадський осуд, відплату або інші форми примусу. Виявлення порушника, передавання відомостей про вчинене діяння та застосування до нього санкції ґрунтувалися переважно на усній інформації, колективній пам'яті громади, особистому впізнанні та авторитеті старійшин або представників родоплемінної верхівки. Тому інформаційне забезпечення такої діяльності ще не мало самостійного характеру, проте вже виконувало орієнтуючу, розшукову й попереджувальну функції.

У період Київської Русі, за умов становлення державної організації, майнового розшарування населення та формування привілейованих соціальних груп, правоохоронна функція поступово набувала публічного змісту. Спеціалізовані правоохоронні органи в сучасному розумінні ще не існували, однак окремі завдання щодо охорони правопорядку, розгляду правопорушень, стягнення штрафів і забезпечення князівської влади виконували князь, його дружина та уповноважені представники – вірники, мечники, тіуни та інші посадові особи. Їх доцільно розглядати не як правоохоронців у сучасному значенні, а як історичних попередників суб'єктів правоохоронної діяльності.

За виконання відповідних функцій і участь у розгляді правопорушень такі особи отримували забезпечення від місцевого населення [12, с. 54]. Правоохоронна практика Київської Русі значною мірою залежала від князівської

влади, а розслідування найбільш значущих діянь поєднувало усне збирання відомостей із початковими формами письмової фіксації. Інформаційну підтримку таких процесів могли забезпечувати писарі при князівському дворі та в осередках місцевої адміністрації, які заносили окремі відомості до книг або інших письмових джерел.

Занепад Київської Русі у 30-х роках XII ст. був пов'язаний із комплексом політичних, економічних і територіальних чинників. У Галицько-Волинському князівстві, яке стало одним із головних спадкоємців державно-правових традицій Русі, зберігалися окремі елементи судово-розшукової практики попереднього періоду [11, с. 218]. Уже з XIII ст. поступово використовувалися найпростіші способи ідентифікації правопорушників, серед яких згадуються зовнішні описи, клеймування, тілесне позначення або інші форми впізнавання осіб, причетних до протиправних діянь.

У Великому князівстві Литовському державно-правові традиції Русі не були повністю перервані, а зазнали подальшої адаптації до нових політичних і правових умов. Право Великого князівства Литовського розвивалося на основі староруських правових джерел, місцевої звичаєвої практики та поступового нормативного впорядкування судово-адміністративної діяльності. Визначення суб'єктів, уповноважених забезпечувати правопорядок, відповідало загальному напряму внутрішньої політики держави, що полягала у прагненні зберегти усталений соціальний, політичний і правовий порядок на приєднаних землях [23].

Важливим етапом розвитку правоохоронних інституцій на українських землях став литовсько-польський період. Політичне зближення Литви й Польщі сприяло ускладненню судової організації, розвитку процесуальних процедур і поступовому відокремленню процесуального права як самостійної сфери юридичного регулювання. У контексті інформаційного забезпечення це мало значення тому, що правопорушення, рішення, свідчення, майнові спори та інші юридично значущі обставини дедалі частіше потребували письмової фіксації, обліку й використання в подальшому розгляді справ [109, с. 91].

Українсько-козацька доба істотно вплинула на формування уявлень про правопорядок, справедливість і відповідальність у національній правовій традиції. У цей період правоохоронна функція реалізовувалася через діяльність органів військово-адміністративної влади, козацького судочинства та громадського контролю. Джерелами відомостей у кримінально-процесуальній практиці виступали пояснення сторін, показання свідків, присяга, документи, речові докази, допити, а також інші засоби встановлення обставин події [108, с. 84]. Зокрема, Соборне уложення 1649 року закріплювало окремі елементи розшукової діяльності, а функції охорони порядку та виявлення правопорушників покладалися, зокрема, на губних старост і земську поліцію [123, с. 29].

Упродовж XVII–XX ст. правоохоронні інституції поступово набували більш визначеної організаційної структури, спеціалізації та функціонального розподілу. До відповідної системи в різні історичні періоди належали поліція, прокуратура, жандармерія, органи державної безпеки та інші суб’єкти, діяльність яких була спрямована на охорону державного механізму, правопорядку й політичного режиму [11, с. 219]. Ускладнення їхніх функцій зумовлювало потребу у більш сталих способах збирання, обліку, зберігання та передавання відомостей.

Витоки автоматизованих інформаційних систем у правоохоронній сфері пов’язані з розвитком картотечних обліків, які історично передували електронним базам даних. Перші систематизовані обліки осіб, причетних до злочинної діяльності, почали формуватися в європейській поліцейській практиці ще в ранньомодерний період. Значний вплив на розвиток кримінальної реєстрації справила діяльність французького поліцейського службовця А. Бертільона, який у 1882 році запропонував антропометричний метод ідентифікації злочинців [51, с. 53–58]. У другій половині XIX ст. такі підходи сприяли створенню картотек з описом зовнішності, антропометричних ознак та інших індивідуалізуючих характеристик особи. Подальший розвиток технічних засобів обліку привів до появи у 1953 році в США однієї з перших

автоматизованих інформаційних систем поліції, призначеної для прискорення пошуку викрадених автомобілів.

На початковому етапі розвитку інформаційно-аналітичної роботи, що охоплює період від початку XVIII ст. до жовтня 1917 року, формувалися перші систематизовані знання про способи боротьби зі злочинністю, кримінальну реєстрацію, проведення окремих слідчих дій та використання спеціальних знань. У цей час правоохоронна практика поступово переходила від переважно усного передавання відомостей до їх письмової фіксації, реєстрації та зіставлення, що створювало передумови для подальшого розвитку криміналістичних обліків.

Починаючи з XVII ст., у працях із кримінального судочинства з'являлися рекомендації щодо використання спеціальних знань для розпізнавання почерку, виявлення отрут і встановлення обставин, які потребували медичних або інших фахових відомостей. У Франції та Італії були опубліковані праці Ф. Демеля, К. Бальді, Є. Равено, присвячені дослідженню почерку. Значення таких напрацювань полягало в тому, що вони поступово утверджували у правоохоронній практиці потребу не лише в отриманні повідомлення, а й у його перевірці за допомогою спеціальних знань.

З 60-х років XIX ст. у поліцейській реєстрації почали активно використовувати фотографію. На українських землях одне з перших поліцейських фотоательє було відкрито у 1864 році в місті Бобринці Одеської губернії, що нині належить до Кіровоградської області. Згодом аналогічні підходи поширювалися й в інших адміністративних центрах. На початку XX ст. поліція вела обліки окремих категорій осіб, які мали значення для охорони порядку, зокрема швейцарів, двірників, працівників питних закладів і візників. Важливого значення набув також облік за способом учинення злочину, відомий як *modus operandi*, який використовувався для виявлення професійних злочинців, у тому числі осіб, що переміщувалися між різними місцевостями.

Другий етап розвитку інформаційно-аналітичної роботи, який охоплює період від жовтня 1917 року до середини 1950-х років, характеризувався поєднанням попередніх криміналістичних напрацювань із новими

організаційними формами діяльності правоохоронних органів. У 1917–1921 роках на території України діяли різні за правовою природою правоохоронні й безпекові інституції: жандармерія, варта Гетьманату, народна міліція Директорії, органи розвідки, контррозвідки, прокуратури, безпеки та інші спеціальні служби. Їх діяльність була спрямована на боротьбу зі злочинністю, охорону правопорядку та забезпечення функціонування державної влади. Поряд з агентурною роботою, зовнішнім спостереженням та іншими оперативними методами застосовувалося збирання, накопичення й аналіз відомостей про осіб, події, організації та загрози.

Порівняно з періодом Центральної Ради, за Гетьманату Павла Скоропадського було сформовано більш організаційно визначену правоохоронну систему, центральне місце в якій посідала Державна варта. У її структурі діяв освідомчий відділ, місцеві підрозділи якого мали автономні повноваження та підпорядковувалися головам місцевих адміністрацій. Крім завдань, пов’язаних із протидією злочинності, вони збирали відомості про загрози державному ладу, політичні виступи, страйки, діяльність партій і їхніх представників [23, с. 35]. Такий досвід засвідчує поступове оформлення інформаційної роботи як окремого напряму забезпечення правоохоронної та безпекової діяльності.

За часів Директорії (Другої Української Народної Республіки) відбулося розширення компетенцій Міністерства внутрішніх справ, хоча це не сприяло значному покращенню боротьби зі злочинністю, яка набувала масового характеру. Окрім контролю за роботою місцевих комісарів, цей державний орган відповідав за забезпечення громадського порядку та керівництво міліцією. Структурним підрозділом МВС був департамент політичної інформації, що займався оперативною розвідкою. На додаток до основних обов’язків, міліція здійснювала облік населення в певних регіонах, а також складала протоколи та акти про різні надзвичайні події та прояви насильства. Серед негативних аспектів діяльності правоохоронних структур періоду українських визвольних змагань 1917-1921 років були: брак кваліфікованих кадрів, відсутність фінансового

забезпечення працівників, а також проблеми зі зв'язком та транспортом [12, с. 54].

В Росії після Жовтневої революції, 28 жовтня 1917 р. (за старим стилем), згідно з постановою НКВС «Про робітничу міліцію», було засновано робітничу міліцію. 5 жовтня 1918 р. Колегія НКВС схвалила Положення про організацію в органах внутрішніх справ РРФСР кримінально-пошукових установ, що стало початком формування обліково-реєстраційної служби в міліцейських підрозділах. 1919 року в Радянській Росії та на підконтрольних українських територіях було створено Центральне реєстраційне бюро, а також реєстраційні бюро у республіканських та губернських відділах і відділеннях карного розшуку.

В Україні діяло 40 реєстраційно-дактилоскопічних бюро. У великих адміністративних центрах, зокрема Харкові, Києві, Одесі та Дніпропетровську, реєстраційний апарат було передано до міських управлінь міліції та розшукових підрозділів. Такий організаційний крок засвідчив поступовий перехід від розрізненого збирання відомостей до спеціалізованого обліку осіб, подій і криміналістично значущих ознак.

У 1920 році було запроваджено централізований облік осіб, які розшукувалися за вчинення злочинів, а також зниклих безвісти. Одночасно сформовано деталізовану класифікацію злочинців, яка мала не лише прикладне, а й пізнавальне значення для подальшого розвитку кримінальної реєстрації. При Науково-технічному підвідділі Центру розшуку функціонувало статистичне бюро, діяльність якого спрямовувалася на вивчення стану злочинності, узагальнення показників розкриття злочинів і підготовку інформації, необхідної для організації розшукової роботи [1, с. 58].

На початку 1930-х років із підрозділів карного розшуку почали виокремлюватися науково-технічні підрозділи, які у 1948 році вони набули статусу окремих структурних підрозділів міліції, що свідчило про поступове інституційне оформлення спеціальної роботи з криміналістично значущою інформацією.

Третій етап розвитку інформаційно-аналітичної діяльності, що охоплює

період від середини 1950-х до початку 1990-х років, пов’язаний із поширенням обчислювальної техніки та поступовою автоматизацією збирання, оброблення, систематизації, аналізу й використання оперативно-розшукової інформації. Його початок співвідноситься з розвитком теоретичних засад оперативно-розшукової діяльності, зокрема зі створенням 23 жовтня 1956 року у Вищій школі МВС СРСР окремої кафедри оперативної роботи. Для централізації оперативно-розшукової інформації було розгорнуто систему інформаційних центрів [1, с. 60].

До 1960 року в Україні не існувало єдиної системи обліку у відділах внутрішніх справ. У 1961 році МВС запровадило Інструкцію з обліку в органах внутрішніх справ, що стало важливим кроком до уніфікації реєстраційної роботи. Науково-практичні засади інформаційного забезпечення правоохоронних органів України почали активно формуватися на початку 1970-х років, коли було створено Республіканський науково-дослідний інформаційний центр МВС УРСР. До основних напрямів його діяльності належали забезпечення оперативною, довідковою, розшуковою, статистичною та іншою інформацією; збирання, оброблення, зберігання й аналіз відомостей про злочини та осіб, які їх учинили; розгляд матеріалів щодо оголошення і припинення розшуку безвісти зниклих осіб, обліку невпізнаних трупів та інших категорій інформації, необхідної для розшукової роботи.

У подальшому було створено мережу інформаційно-обчислювальних центрів у регіонах, насамперед в обласних управліннях внутрішніх справ. Такі підрозділи оснащувалися електронно-обчислювальними машинами типів «Мінськ-32», «Мінськ-22», «СМ» та «ЄС». До перших автоматизованих інформаційних систем належали «Профілактика-Розшук», «Розшук», «Статистика» та інші інформаційні ресурси, орієнтовані на підтримку облікової, розшукової й аналітичної роботи [19].

Інформаційні центри поступово перетворилися на організаційні вузли накопичення, оброблення і технічного супроводження значних масивів правоохоронної інформації. На початку 1980-х років було сформульовано підхід

до автоматизації інформаційного забезпечення управлінської діяльності, в основі якого перебувала ідея автоматизованого робочого місця працівника органів внутрішніх справ. У 1985 році започатковано створення єдиного автоматизованого банку даних, призначеного для акумулювання інформації, необхідної для виконання правоохоронних функцій. Використання ЕОМ дало змогу автоматизувати однотипні й трудомісткі операції, пришвидшити пошук відомостей та розширити можливості управлінського апарату. У цей період застосовувалися автоматизовані інформаційні системи «Адмінпрактика», «Профілактика-розшук», «Скарга», «Статистика», «Автомобіль», «Аналіз господарської діяльності», «Номерні речі», «Патруль», «Нормативно-правові акти» та інші. Розроблення галузевої інформаційної системи «Нормативно-правові акти» згодом стало підґрунтям для формування систем «Право», «Законодавство», «Нормативно-правові акти України» [122, с. 58].

Четвертий етап розвитку інформаційно-аналітичної діяльності охоплює період від початку 1990-х років до 19 листопада 2012 року. Його початок пов’язаний із проголошенням незалежності України, прийняттям Закону України «Про оперативно-розшукову діяльність» та організаційною перебудовою системи органів внутрішніх справ. У цей час формувалася нова модель інформаційно-аналітичного забезпечення оперативно-розшукової діяльності. Характерними ознаками періоду стали створення міжвідомчих обліків, розширення міждержавного обміну, використання інтегрованих банків даних Інтерполу, розвиток аналітичних і комп’ютерних розвідувальних технологій, застосування мультимедійних засобів в оперативній практиці, а також опрацювання технологій інформаційно-аналітичної роботи у транспортних, телекомунікаційних та електронних інформаційних мережах.

Наприкінці XX ст. інформатизація органів внутрішніх справ України перебувала на початковому етапі активного впровадження. З 1991 року почали створюватися перші локальні обчислювальні мережі, доступ до яких мали керівництво МВС та окремі управлінські підрозділи. У 1992 році розпочалося формування єдиної системи інформаційного забезпечення органів внутрішніх

справ МВС України як системи оброблення даних за стандартизованими правилами. До 2000 року інформаційна мережа складалася з локальних обчислювальних мереж структурних підрозділів МВС України та управлінь МВС в областях, об'єднаних у спільне інформаційне середовище [51, с. 55].

У 2002 році було створено Департамент інформаційно-аналітичного забезпечення МВС, який функціонував як структурний підрозділ апарату Міністерства та відповідав за розроблення і впровадження інформаційних технологій у діяльність органів внутрішніх справ України [126, с. 80]. Його діяльність охоплювала формування електронних версій персональних обліків МВС, зокрема за напрямами «Зниклі громадяни», «Особи, які переховуються від органів влади», «Неопізнані трупи», «Культурні цінності», «Мобільні телефони», «Транспортні засоби у розшуку», «Зброя у розшуку» тощо. У 2006 році на базі цього департаменту передбачалося створення Оперативно-аналітичного департаменту, покликаного забезпечити розбудову оперативно-аналітичних структур у центральному апараті та регіональних підрозділах. У 2007 році його було реорганізовано у Департамент стратегічного аналізу і прогнозування, а в регіональних, міських, районних та лінійних органах внутрішніх справ створено сектори інформаційних технологій.

П'ятий етап розвитку інформаційно-аналітичної роботи розпочався 20 листопада 2012 року і триває дотепер. Його початок зумовлений набранням чинності КПК України, запровадженням негласних слідчих (розшукових) дій та зміною організації інформаційно-аналітичної роботи в оперативно-розшуковій діяльності. Після створення Національної поліції України інформаційно-аналітичне та інформаційно-пошукове забезпечення набуло нового інституційного оформлення. Наказом Національної поліції України від 30 грудня 2015 р. № 228 було створено Департамент інформаційної підтримки та координації поліції «102», діяльність якого спрямована на організацію та реалізацію передбачених законодавством заходів інформаційно-аналітичного й інформаційно-пошукового забезпечення правоохоронної діяльності, а також захист персональних даних під час їх оброблення у структурних підрозділах

апарату Національної поліції України.

Наведений історичний матеріал дає підстави уточнити періодизацію розвитку інформаційного забезпечення правоохоронної діяльності в Україні. Критерієм розмежування етапів, на нашу думку, має бути не лише поява нового технічного засобу або організаційного підрозділу. Більш переконливим є сукупний критерій, що охоплює: спосіб фіксації й передавання відомостей; ступінь централізації обліків; правове оформлення інформаційних процесів; характер використання результатів оброблення; рівень міжвідомчої та міжнародної взаємодії; гарантії захисту прав особи. Такий підхід дає змогу відокремити справжні якісні зміни від звичайного оновлення техніки та показати поступовий перехід від розрізненого обліку фактів до взаємопов’язаного інформаційно-аналітичного середовища.

Перший, протореєстраційний етап охоплює додержавний період і ранні державні утворення на українських землях. Інформація передавалася переважно усно, а її носіями були пам’ять членів громади, звичаї, повідомлення свідків, прикмети особи та відомості про подію. Поява писемних актів, судових записів і документів не утворила самостійної системи правоохоронних обліків, однак започаткувала фіксацію юридично значущих фактів. Основною рисою етапу була невідокремленість інформаційної функції від судової, військової та адміністративної діяльності. Відомості збиралися у зв’язку з конкретною справою і майже не використовувалися для системного прогнозування або пошуку за аналогією.

Другий, документально-обліковий етап доцільно пов’язати з розвитком централізованих адміністративних і поліцейських установ у XVIII – першій половині XIX ст. Формуються письмові реєстри, книги, списки розшукуваних осіб, службові донесення та архіви. Інформація поступово набуває стандартизованої форми, а її рух підпорядковується вертикалі управління. Водночас обліки залишалися відомчо замкненими, пошук здійснювався вручну, а правові гарантії особи під час збирання і використання відомостей були мінімальними. Значення етапу полягає у виокремленні реєстраційної роботи як

постійної складової діяльності органів охорони правопорядку.

Третій, криміналістично-ідентифікаційний етап охоплює другу половину XIX – початок XX ст. Його зміст визначили фотографічні, антропометричні, дактилоскопічні та описові обліки, що надали можливість ідентифікувати особу за відносно стійкими ознаками. Інформація почала накопичуватися не лише для документування окремого провадження, а й для повторного використання під час розшуку та розкриття правопорушень. Праці А. Бертільона та розвиток дактилоскопії змінили саму логіку поліцейської реєстрації: суб'єктивний опис поступово доповнювався вимірюваними й порівнюваними відомостями. Для українських земель цей процес відбувався у межах різних державних систем, що пояснює нерівномірність організаційного розвитку.

Четвертий, централізовано-картотечний етап припадає на 1920-ті – середину 1950-х років. Характерними стали централізовані обліки розшукуваних, засуджених і зниклих безвісти осіб, уніфіковані картки, класифікатори, алфавітні та дактилоскопічні картотеки. Централізація прискорила міжтериторіальний пошук, проте інформаційна система функціонувала в умовах надмірної таємності, політичного контролю й слабких гарантій прав людини. Історична оцінка цього періоду має враховувати подвійний результат: організаційне вдосконалення обліково-реєстраційної роботи поєднувалося з можливістю використання накопичених даних для репресивних цілей. Відтак технічна результативність без правових обмежень не може визнаватися достатнім критерієм належного інформаційного забезпечення.

П'ятий, автоматизовано-обчислювальний етап тривав із середини 1950-х до початку 1990-х років. Використання електронно-обчислювальної техніки, створення інформаційно-обчислювальних центрів та автоматизованих систем пришвидшили пошук, оброблення статистики й обмін між територіальними підрозділами. Поступово формувалися загальновідомчі банки даних, а інформація стала використовуватися для планування й оцінювання оперативної обстановки. Водночас технічна несумісність окремих систем, дублювання відомостей і переважно відомчий характер регулювання обмежували можливості

комплексного аналізу. Правовий режим даних визначався здебільшого закритими підзаконними актами, що не відповідало сучасним вимогам прозорості й підконтрольності.

Шостий, національно-інформаційний етап охоплює 1991–2012 роки. Проголошення незалежності України зумовило формування власної нормативної основи, розвиток локальних і відомчих мереж, переведення картотек в електронну форму та створення інформаційно-аналітичних підрозділів. Закони України «Про інформацію» [86], «Про оперативно-розшукову діяльність» [91], «Про захист інформації в інформаційно-комунікаційних системах» [83] і «Про захист персональних даних» [84] заклали загальні правові межі оброблення відомостей. Проте успадкована відомча роз’єднаність зберігалася: інформаційні ресурси створювалися під потреби окремих органів, використовували різні класифікатори й не завжди мали належні механізми взаємного доступу.

Сьомий, інтеграційно-цифровий етап розпочався у 2012 році з набранням чинності Кримінальним процесуальним кодексом України та створенням Єдиного реєстру досудових розслідувань. Подальше утворення Національної поліції, Державного бюро розслідувань, Бюро економічної безпеки, розвиток Єдиної інформаційної системи МВС, Інформаційного порталу Національної поліції та електронної міжвідомчої взаємодії змінили масштаб і швидкість інформаційних процесів. Аналітична діяльність дедалі більше спирається на зіставлення масивів даних, геоінформаційні засоби, біометричну ідентифікацію та автоматизоване виявлення зв’язків. Разом із новими можливостями зросли ризики масового неправомірного доступу, помилкового поєднання відомостей і непрозорого використання автоматизованих висновків.

У межах сьомого етапу доцільно виокремити сучасний воєнно-інтеграційний період, початок якого пов’язаний із повномасштабною збройною агресією Російської Федерації у 2022 році та набуттям Україною статусу кандидата на членство в Європейському Союзі. Інформаційне забезпечення правоохоронної діяльності одночасно виконує завдання документування

воєнних злочинів, розшуку зниклих осіб, ідентифікації загиблих, протидії диверсійній діяльності, кіберзагрозам і незаконному обігу зброї. Комплексний стратегічний план реформування органів правопорядку на 2023–2027 роки прямо орієнтує систему на керованість, цифровізацію, обмін даними та наближення до стандартів Європейського Союзу [87]. Визначальною рисою періоду є потреба поєднати оперативність роботи в умовах загроз із належним документуванням походження даних, контролем доступу та можливістю їх подальшого доказового використання.

Запропонована періодизація показує, що розвиток інформаційного забезпечення має не лінійний, а накопичувальний характер. Усна передача відомостей не зникла після появи письмових реєстрів; картотеки продовжували функціонувати поряд з автоматизованими системами; сучасні аналітичні засоби залежать від якості первинного внесення даних. Тому кожен наступний етап не повністю замінює попередній, а включає його окремі елементи в нове організаційно-правове середовище. Головним напрямом еволюції є перехід від епізодичного збирання відомостей до безперервного керованого циклу даних, у якому встановлено відповідального суб’єкта, правову мету, строки зберігання, правила доступу, порядок перевірки та способи виправлення помилок.

Інформаційне забезпечення управління в правоохоронних органах охоплює визначення змісту, обсягу, якості та цільового призначення відомостей, необхідних для прийняття управлінських рішень, а також організацію їх збирання, перевірки, систематизації, накопичення, оброблення й використання за допомогою відповідних методів, методик і технічних засобів. За таким підходом інформаційне забезпечення управління створює умови для комплексного вирішення правоохоронних завдань і надання суб’єктам управління обґрунтованої інформації, придатної для планування, координації, контролю та оцінювання результатів діяльності.

Інформаційно-аналітичне забезпечення правоохоронних органів України доцільно розглядати через три взаємопов’язані складові: по-перше, інформаційні системи, у межах яких здійснюється збирання, накопичення, системна обробка,

зберігання та надання користувачеві необхідних відомостей; по-друге, аналітичну роботу, що передбачає застосування організаційних заходів і методичних прийомів для опрацювання, зіставлення та узагальнення оперативної й іншої правоохоронно значущої інформації; по-третє, управлінську діяльність, у межах якої аналітично опрацьовані відомості використовуються для вироблення стратегічних і тактичних рішень щодо протидії злочинності [11, с. 182–193].

У науковій літературі інформаційно-аналітичне забезпечення також визначається як сукупність заходів щодо збирання, отримання, зберігання, використання, оброблення та накопичення інформації з її подальшим аналізом для прогнозування, підбиття підсумків діяльності й коригування подальших управлінських рішень [37, с. 8]. Такий підхід дозволяє підкреслити, що аналітичний компонент не завершується описом наявної ситуації, а має бути спрямований на підготовку рішення, оцінку ризиків і прогнозування можливого розвитку подій.

Діяльність поліції здійснюється на засадах верховенства права, поваги до прав і свобод людини, законності, відкритості та прозорості, політичної нейтральності, взаємодії з населенням на засадах партнерства і безперервності. У сфері управління ці загальні засади доповнюються спеціальними принципами інформаційно-аналітичного забезпечення, оскільки для управлінського рішення важливе не лише своєчасне одержання первинних відомостей, а й здатність завчасно виявити проблемну ситуацію, оцінити її розвиток і запропонувати обґрунтований варіант реагування.

До спеціальних принципів інформаційно-аналітичного забезпечення управління в поліції належать об’єктивність, достовірність, безперервність, системність, активність, актуальність, ініціативність, цілеспрямованість, повнота та обґрунтованість. Принцип об’єктивності означає неупереджене ставлення до інформації, її джерела та результатів аналітичного опрацювання. Його значення полягає у зменшенні впливу суб’єктивних оцінок на управлінське рішення, оскільки аналітик має спиратися на факти, перевірені дані та професійні

знання. Принцип достовірності передбачає відповідність інформації реальному стану подій і можливість її перевірки.

Принцип безперервності вимагає постійного здійснення інформаційно-аналітичної роботи, що особливо важливо для поліції як органу, який забезпечує реагування на правопорушення та події у цілодобовому режимі. Принцип системності полягає у тому, що інформаційно-аналітичне забезпечення охоплює не окремі розрізнені дії, а послідовний процес одержання, оброблення, зіставлення, аналізу та використання відомостей. Принцип активності орієнтує правоохоронні органи на ініціативне виявлення інформаційних потреб, ризиків і проблем, а не лише на пасивне сприйняття повідомлень, що надходять.

Принцип актуальності означає відповідність інформації часу, місцю, умовам і характеру завдання, для вирішення якого вона використовується. Інформація має передувати прийняттю рішення, а не лише фіксувати подію після її завершення, тому аналітична робота повинна мати прогностичний і попереджувальний зміст. Принцип ініціативності передбачає здатність працівників, які здійснюють інформаційно-аналітичну підтримку, самостійно виявляти проблемні ситуації, пропонувати варіанти їх вирішення та творчо використовувати наявні методики в умовах зміни оперативної обстановки.

Принцип цілеспрямованості забезпечує зв’язок інформаційно-аналітичної роботи з конкретними завданнями органів і підрозділів поліції. На загальнодержавному рівні йдеться про підтримку державної політики у сфері захисту прав і свобод людини, власності, інтересів суспільства й держави, протидії злочинності, розкриття та розслідування кримінальних правопорушень, охорони публічного порядку і забезпечення публічної безпеки. На місцевому рівні цей принцип реалізується через інформаційне супроводження розкриття конкретних злочинів, профілактичної роботи, встановлення причин та умов учинення правопорушень і підготовки заходів щодо їх усунення.

Принцип повноти передбачає використання всіх релевантних відомостей, необхідних для вирішення відповідної управлінської або правоохоронної проблеми. Водночас повнота не повинна ототожнюватися з надмірним

накопиченням даних, оскільки значення має саме достатність інформації для обґрунтованого рішення. Принцип обґрунтованості вимагає, щоб результати інформаційно-аналітичної діяльності підтверджувалися фактичними даними, відповідали реальним обставинам і спиралися на сучасні наукові підходи, методики та засоби аналітичної роботи [17, с. 208].

На нашу думку, ефективність інформаційно-аналітичного забезпечення управління в правоохоронних органах досягається лише за умови взаємного поєднання зазначених принципів. Ізольоване застосування окремого принципу не забезпечує належної якості управлінського рішення, оскільки достовірна, але несвоєчасна інформація втрачає практичне значення, повна, але неперевірена інформація створює ризик помилки, а актуальна, але однобічно оцінена інформація може призвести до необґрунтованого рішення. Саме системне дотримання цих принципів забезпечує придатність інформаційно-аналітичного результату для ефективного управління правоохоронною діяльністю.

1.2. Міжнародно-правові стандарти та зарубіжний досвід інформаційного забезпечення правоохоронної діяльності

Інформаційне забезпечення правоохоронної діяльності за своєю природою виходить за межі внутрішньодержавного регулювання. Транскордонний характер організованої злочинності, незаконного обігу зброї та наркотичних засобів, торгівлі людьми, кіберзлочинності, фінансування тероризму й воєнних злочинів зумовлює постійний обмін даними між національними правоохоронними органами, міжнародними організаціями та установами Європейського Союзу. Водночас збільшення обсягу доступної інформації, застосування біометричної ідентифікації, автоматизованого зіставлення даних і прогнозного аналізу створюють небезпеку надмірного втручання у приватне життя, використання недостовірних відомостей та прийняття рішень, правові наслідки яких неможливо належно перевірити. Тому міжнародно-правові

стандарти в досліджуваній сфері виконують подвійну функцію: забезпечують оперативність інформаційної взаємодії та встановлюють межі, за яких така взаємодія залишається законною, необхідною і пропорційною.

Зміст міжнародних стандартів не можна зводити лише до сукупності вимог щодо захисту персональних даних, позаяк їх нормативне призначення є ширшим і охоплює визначення правової мети збирання відомостей, розмежування повноважень органу-джерела та органу-користувача, перевірку достовірності інформації, установлення строків її зберігання, документування операцій, забезпечення інформаційної безпеки, незалежний нагляд і поновлення прав особи. Сукупність зазначених вимог формує правовий режим повного життєвого циклу правоохоронної інформації – від її первинного одержання до виправлення, архівування або видалення. За такого підходу швидкість доступу до відомостей оцінюється не відокремлено, а разом із можливістю встановити їх походження, ступінь перевіреності, правову підставу використання та посадову особу, відповідальну за прийняте рішення.

Основу міжнародно-правового регулювання інформаційного забезпечення правоохоронної діяльності становлять загальновизнані гарантії прав людини, оскільки збирання, зберігання, зіставлення, передавання та використання відомостей про особу безпосередньо пов’язані зі сферою її приватного життя. Право на невтручання в особисте і сімейне життя, недоторканність житла та таємницю кореспонденції закріплено в Загальній декларації прав людини, Міжнародному пакті про громадянські і політичні права та Конвенції про захист прав людини і основоположних свобод. Для правоохоронної діяльності принципове значення має не лише формальне визнання права на приватність, а й вироблений у міжнародній практиці підхід до оцінювання допустимості втручання в це право. Збирання, перевірка, зіставлення, зберігання та передавання відомостей про особу повинні мати доступну й передбачувану правову основу, переслідувати легітимну мету, бути необхідними в демократичному суспільстві та супроводжуватися належними гарантіями від свавільного використання інформації.

Зазначені вимоги мають безпосереднє значення для інформаційного забезпечення правоохоронної діяльності, оскільки правоохоронні органи оперують значним обсягом персональних, службових, оперативно значущих та інших відомостей, необхідних для запобігання, виявлення, припинення й розслідування правопорушень. Йдеться, зокрема, про дані щодо особи, її зв'язків, місця перебування, пересування, комунікацій, майнового стану, біометричних ознак, участі у кримінальному провадженні, перебування в розшуку або зв'язку з подіями, що мають значення для правоохоронної діяльності. Тому закон, який лише загально дозволяє створення інформаційних ресурсів або обмін даними між правоохоронними органами, але не визначає категорій відомостей, кола користувачів, правових підстав доступу, строків зберігання, порядку перевірки актуальності та способів контролю, не забезпечує належної передбачуваності втручання. В умовах воєнного стану така вимога не втрачає значення, а навпаки посилюється, оскільки зростання безпекових потреб не може виправдовувати невизначеність правового режиму інформації.

Практика Європейського суду з прав людини послідовно виходить із того, що саме зберігання державним органом відомостей про приватне життя становить втручання у право, гарантоване статтею 8 Конвенції, незалежно від того, чи були ці відомості надалі використані проти особи. Інтенсивність такого втручання залежить від характеру даних, способу їх одержання, можливості зіставлення з іншими інформаційними масивами, строку зберігання, кола користувачів і наслідків, які може спричинити їх використання. Особливої обережності потребують біометричні, генетичні, телекомунікаційні, геолокаційні та інші відомості, які забезпечують однозначну ідентифікацію людини або дають змогу відтворити істотні аспекти її поведінки, зв'язків чи пересування. Правоохоронна потреба не усуває вимоги правової визначеності, а підвищує її значення: чим ширшими є владні повноваження органу та технологічні можливості зіставлення різних категорій даних, тим чіткішими мають бути правила доступу, використання, зберігання, передавання, видалення й контролю.

Спеціальне міжнародне регулювання захисту інформації сформувалося насамперед у межах Ради Європи. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних 1981 року стала першим юридично обов'язковим міжнародним договором у цій сфері [39]. Її положення закріпили вимоги законного й добросовісного одержання даних, їх відповідності визначеним цілям, точності, актуальності, пропорційності та обмеження строку зберігання. Значення Конвенції для правоохоронної діяльності полягає у визнанні того, що автоматизація обробки відомостей не змінює природи юридичної відповідальності: орган, який використовує інформаційну систему, залишається відповідальним за правомірність кожної операції, якість даних і наслідки їх використання у правоохоронному рішенні.

Протокол CETS № 223, ухвалений у 2018 році, модернізував положення Конвенції та пристосував їх до умов розподіленого оброблення значних масивів даних [166]. Оновлений підхід посилив вимоги прозорості, пропорційності, підзвітності, оцінювання ризиків, документування операцій та незалежного нагляду. Оброблення генетичних і біометричних даних, відомостей про кримінальні правопорушення, кримінальні провадження та засудження допускається лише за наявності належних гарантій від дискримінації, помилкової ідентифікації, необґрунтованого обмеження прав людини або використання інформації з іншою метою. Для України зазначені положення важливі не лише як орієнтир законодавчого зближення з європейськими стандартами, а й як критерій оцінювання вже створених відомчих реєстрів та інформаційних систем. Технічна працездатність системи не свідчить про належний рівень її правового врегулювання, якщо неможливо встановити, хто, коли, з якою метою і на якій підставі вніс запис, кому він був доступний, коли перевірялася його актуальність та за яких умов відповідні відомості підлягають виправленню, архівуванню або видаленню.

Окремий розвиток загальні положення Конвенції одержали в Рекомендації Комітету міністрів Ради Європи № R (87) 15 щодо використання персональних даних у поліцейському секторі та Практичному посібнику 2018 року [133]. У цих

документах поліцейська інформація розглядається не як однорідний масив, а як сукупність відомостей різного походження, ступеня достовірності, процесуального або оперативного значення та допустимих напрямів використання. Підтверджений факт, показання свідка, оперативне повідомлення, припущення аналітика, інформація з відкритого джерела і результат автоматизованого збігу не можуть позначатися й використовуватися однаково. Відсутність такого розмежування перетворює інформаційну систему з інструменту пізнання та організації правоохоронної діяльності на джерело відтворення первинної помилки.

З огляду на це під час створення або модернізації українських правоохоронних інформаційних ресурсів необхідно нормативно закріпити обов'язкові позначки про джерело походження відомостей, правову підставу їх одержання, категорію даних, ступінь перевіреності, дату оновлення, допустимі напрями використання, режим доступу та службову особу або орган, відповідальний за внесення й актуальність інформації. Такий підхід дасть змогу поєднати оперативність інформаційного обміну з вимогами законності, захисту прав людини, доказової придатності відомостей і підконтрольності правоохоронної діяльності, що є особливо важливим в умовах воєнного стану та поглиблення міжнародної взаємодії України у сфері безпеки.

Істотний вплив на становлення міжнародних стандартів здійснило право Європейського Союзу. Директива 95/46/ЄС від 24 жовтня 1995 року забезпечила зближення національних підходів до оброблення персональних даних і сформувала понятійний апарат, який тривалий час визначав розвиток європейського інформаційного права [138]. До оброблення було віднесено збирання, реєстрацію, упорядкування, зберігання, зміну, пошук, використання, передавання та видалення відомостей. Принципове значення мало поширення вимог не лише на автоматизовані бази, а й на впорядковані неавтоматизовані картотеки. Унаслідок цього юридична оцінка пов'язувалася не з видом носія, а зі способом організації та використання інформації.

Розвиток європейського регулювання відбувався одночасно за двома

взаємопов’язаними напрямами: гарантування конфіденційності та формування сумісного середовища електронної взаємодії. Директива 97/66/ЄС поширила вимоги захисту приватності на телекомунікаційний сектор, закріпивши таємницю повідомлень і заборону несанкціонованого прослуховування, перехоплення або іншого втручання [139]. Для правоохоронної діяльності значення відповідних положень полягає в тому, що технічна доступність електронного повідомлення не утворює самостійної підстави його одержання. Доступ до змісту комунікацій та пов’язаних із ними даних має здійснюватися в установленому законом порядку, відповідати конкретній меті та супроводжуватися процесуальними гарантіями, співмірними з інтенсивністю втручання.

Рішення Європейського Парламенту та Ради № 1719/1999/ЄС і № 1720/1999/ЄС започаткували правові та організаційні передумови розвитку транс’європейських мереж електронного обміну між адміністраціями [135; 136]. Передбачалося узгодження національних мереж, визначення спільних технічних вимог і сервісів, скорочення витрат на підтримання відокремлених рішень та забезпечення безпечного передавання даних. Хоча зазначені акти не були спеціально спрямовані на поліцейське співробітництво, закладена в них ідея сумісності набула подальшого розвитку в інформаційних системах простору свободи, безпеки та правосуддя. Правовий зміст сумісності охоплює не лише здатність технічних засобів передати повідомлення, а й однакове розуміння реквізитів, статусу відомостей, обмежень доступу та відповідальності за їх подальше використання.

Співвідношення конфіденційності й сумісності дає змогу виявити закономірність європейського регулювання: розширення інформаційного обміну супроводжується деталізацією гарантій, а нові можливості автоматизованого пошуку – установленням додаткових процедур перевірки. Гармонізація за таких умов не зводиться до технічного приєднання національного ресурсу до міжнародної мережі. Вона потребує попереднього узгодження категорій даних, цілей оброблення, правил зберігання, повноважень користувачів і порядку

реагування на помилковий збіг. За відсутності правової сумісності швидкий обмін лише переміщує інформаційну невизначеність з однієї юрисдикції до іншої.

Історичне значення Директиви 95/46/ЄС не дає підстав розглядати її як чинний спеціальний стандарт правоохоронного оброблення. Із 25 травня 2018 року цей акт замінено Регламентом (ЄС) 2016/679, відомим як Загальний регламент про захист даних [167]. Регламент закріпив принципи законності, справедливості й прозорості, обмеження мети, мінімізації даних, точності, обмеження строків зберігання, цілісності, конфіденційності та підзвітності. Водночас його дія за загальним правилом не охоплює оброблення компетентними органами даних для запобігання, виявлення, розслідування кримінальних правопорушень, кримінального переслідування або виконання покарань. Відповідні відносини регулює спеціальна Директива (ЄС) 2016/680 [140]. Розмежування сфер дії двох актів має принципове значення для української правотворчості, оскільки механічне перенесення загальних правил, розрахованих переважно на цивільний та адміністративний обіг даних, не враховує владної природи правоохоронної діяльності.

Спеціальний режим Директиви (ЄС) 2016/680 зумовлений тим, що згода особи здебільшого не може бути правовою підставою збирання правоохоронної інформації. Дані одержуються під час виконання законних повноважень, а тому визначальними стають нормативна передбаченість, необхідність і пропорційність оброблення. Компетентний орган повинен збирати лише ті відомості, які мають зв’язок із конкретною правоохоронною метою, не використовувати їх несумісно з первинним призначенням та забезпечувати своєчасне виправлення неточних записів. Директива також вимагає, наскільки це можливо, розмежовувати дані підозрюваних, засуджених, потерпілих, свідків та інших осіб, а підтверджені факти – від особистих оцінок [140]. У практичній площині йдеться про недопустимість ситуації, коли неперевірене оперативне повідомлення без додаткового позначення відображається в усіх відомчих системах як установлений факт і тривалий час впливає на рішення щодо людини.

Підзвітність за Директивою (ЄС) 2016/680 забезпечується не декларацією про захист інформації, а сукупністю процедур. До них належать ведення журналів операцій зі збирання, перегляду, зміни, розкриття, поєднання і видалення даних; визначення строків їх зберігання або періодичного перегляду; оцінювання ризиків; захист інформації під час проєктування системи та за початковими налаштуваннями; повідомлення про порушення безпеки; незалежний нагляд. Журналювання має давати змогу встановити мету операції, час її проведення та особу користувача. За відсутності таких відомостей неможливо достовірно з'ясувати причину витоку, незаконного перегляду або прийняття помилкового рішення.

Вимога точності даних у правоохоронній сфері має складніший зміст, ніж звичайне виправлення технічної або фактичної помилки. Значна частина відомостей, які використовуються правоохоронними органами, формується в умовах інформаційної невизначеності, обмеженого часу, неповноти джерел або необхідності оперативного реагування, тому не завжди може бути остаточно підтверджена на момент первинного внесення. Директива не забороняє опрацьовувати такі повідомлення, однак вимагає чіткого відмежування неперевіреної інформації від установлених фактів. У зв'язку з цим якість даних охоплює не лише правильність їх змісту, а й повноту необхідних реквізитів, актуальність, достовірність джерела, правову підставу одержання та коректне позначення ступеня перевіреності. Запис може формально точно відтворювати одержане повідомлення, однак залишатися непридатним для безпосереднього прийняття правоохоронного рішення, якщо не встановлено надійність його походження, межі допустимого використання та зв'язок із конкретним правоохоронним завданням.

Самостійне значення має визначення строків зберігання правоохоронної інформації. Єдиний строк для всіх категорій даних не відповідає принципу пропорційності, оскільки оперативне повідомлення, матеріали кримінального провадження, інформація про розшук особи або статистичний набір мають різну мету оброблення, рівень втручання у приватне життя та наслідки подальшого

використання. Законодавство повинно визначати або конкретні строки зберігання, або зрозумілі критерії їх обчислення, продовження та періодичного перегляду. Завершення кримінального провадження, скасування розшуку, виправдання особи, встановлення помилкової ідентифікації або втрата актуальності оперативної інформації мають бути підставами для обов'язкової перевірки пов'язаних записів у тих інформаційних ресурсах, до яких відповідні відомості були внесені або передані.

Передавання даних третій країні або міжнародній організації потребує попереднього оцінювання правового режиму, який застосовуватиметься після їх одержання. Компетентний орган має враховувати мету запиту, категорію інформації, правову підставу її передавання, передбачуваний спосіб використання, можливість подальшого поширення та наявність дієвих засобів захисту від неправомірного доступу чи використання не за призначенням. У разі встановлення спеціальних обмежень щодо використання переданих відомостей такі обмеження повинні бути належно доведені до одержувача та забезпечені організаційними і технічними засобами. Зазначена вимога безпосередньо пов'язана із запропонованим принципом еквівалентного захисту, відповідно до якого міжнародне співробітництво розширює коло законних користувачів інформації, однак не припиняє дії гарантій, установлених для її первинного оброблення.

На нашу думку, імплементація зазначених вимог в Україні повинна здійснюватися через правове врегулювання, зокрема відповідний запис повинен містити відомості про джерело походження, дату одержання, правову підставу, мету оброблення, ступінь перевіреності, строк актуальності, коло дозволених користувачів, установлені обмеження та суттєві операції з ним. За такого підходу інформаційне забезпечення охоплює не лише накопичення й пошук даних, а й перевірку їх якості, виправлення неточностей, перегляд необхідності подальшого зберігання, зміну режиму доступу та припинення активного використання. Запровадження такого підходу посилить результативність правоохоронної діяльності, оскільки уповноважений працівник одержуватиме не

відокремлене повідомлення, а відомості з установленим походженням, визначеним правовим режимом, належним ступенем перевіреності та зрозумілою доказовою або аналітичною цінністю.

Поряд із захистом персональних даних право Європейського Союзу встановлює організаційні правила транскордонного інформаційного обміну. Директива (ЄС) 2023/977 спрямована на забезпечення належного і швидкого передавання відомостей між правоохоронними органами держав-членів [142]. Такий нормативно-правовий акт передбачає функціонування єдиного контактного пункту, застосування електронної системи ведення справ та використання захищеної мережі SIENA як основного каналу обміну. Важливим є принцип рівноцінного доступу, згідно з яким інформація, доступна одному національному правоохоронному органу, за загальним правилом повинна надаватися у відповідь на належно обґрунтований запит іншої держави на не менш сприятливих умовах. Водночас Директива не зобов'язує державу одержувати інформацію із застосуванням примусових заходів лише для задоволення іноземного запиту або накопичувати її виключно для можливого подальшого передавання.

Правове значення Директиви (ЄС) 2023/977 полягає у поєднанні оперативності інформаційного обміну з процедурною визначеністю дій компетентних органів. Запит про надання інформації повинен містити достатнє обґрунтування, а відмова у його виконанні має спиратися на встановлені правові підстави і стосуватися лише тієї частини відомостей, передавання якої є неприпустимим або потребує додаткових гарантій. Такий порядок запобігає двом однаково небезпечним для правоохоронної діяльності підходам: необґрунтованому блокуванню міжнародної взаємодії та автоматичному передаванню всього масиву даних без оцінювання мети, необхідності, пропорційності й подальшого режиму використання. Для України зазначений досвід доцільно реалізувати шляхом створення постійно діючого міжвідомчого контактного осередку, здатного забезпечувати цілодобове опрацювання запитів, застосування погоджених форматів відомостей, фіксацію підстав доступу,

строків реагування та прийнятих рішень. Функціонування такого осередку не повинно підміняти компетенцію окремих правоохоронних органів, а має усунути дублювання запитів, невизначеність відповідального виконавця, неоднаковість підходів до оформлення відповідей та втрату контролю за подальшим використанням переданих даних. Таку позицію підтримують і результати опитування: 43,0 % респондентів визначили збереження правового режиму, мети та обмежень використання інформації основною гарантією міжнародного правоохоронного обміну, тоді як 26,5 % надали пріоритет відповідальності органу-джерела за достовірність і актуальність переданих відомостей (додаток Б).

Інституційним центром європейського поліцейського інформаційного обміну є Європол. Захищена мережа SIENA використовується для передавання оперативних і стратегічних відомостей між національними компетентними органами, Європолом та уповноваженими партнерами [177]. У 2023 році через неї було передано 1,79 млн повідомлень, а до мережі під’єднано близько трьох тисяч компетентних органів [155]. Наведені показники свідчать не лише про технічну потужність відповідного інструменту, а й про значення уніфікованого захищеного каналу, який забезпечує документування обміну, позначення обмежень щодо подальшого використання відомостей, збереження відповідальності органу-джерела та можливість подальшої перевірки правомірності інформаційної операції. Угода між Україною та Європейським поліцейським офісом про оперативне та стратегічне співробітництво створює правову основу для обміну інформацією, спільного аналізу і підтримки розслідувань [117]. Перспективним для України є не досягнення програмної тотожності національних інформаційних систем із SIENA, а забезпечення сумісності правил класифікації, перевірки, захисту, фіксації та простежуваності переданих відомостей.

Еволюція інформаційних засобів Європолу засвідчує поступовий перехід від накопичення відомостей у спеціалізованих аналітичних масивах до захищеного обміну структурованими даними між широким колом компетентних

органів. Учасник обміну визначає мету повідомлення, категорію доступу, допустимість подальшого поширення та необхідність одержання згоди органу-джерела. Інформаційні обмеження мають супроводжувати відомості після їх передавання, унаслідок чого одержувач не набуває необмеженого права розпоряджатися ними або використовувати їх поза визначеною метою. В українських правоохоронних інформаційних системах аналогічний порядок може бути забезпечений через нормативне закріплення і технічну реалізацію позначок правового режиму даних, які відображатимуть підставу доступу, мету передавання, дозволене коло користувачів, обмеження подальшого поширення та необхідність погодження з органом-джерелом.

Аналітична діяльність Європолу розкриває також відмінність між первинними даними та інформацією, одержаною внаслідок їх опрацювання. Установлення зв’язку між особами, подіями, засобами зв’язку, фінансовими операціями, маршрутами переміщення або іншими об’єктами правоохоронного інтересу утворює новий інформаційний результат, який повинен містити відомості про використані джерела, спосіб аналізу, ступінь обґрунтованості висновку та межі його допустимого використання. Втрата зв’язку з первинними даними унеможливлює перевірку аналітичного продукту і створює ризик його некритичного сприйняття як установленого факту. Розвиток інформаційно-аналітичних підрозділів в Україні має супроводжуватися уніфікацією правил документування аналітичних висновків, зазначенням рівня їх достовірності та чітким відмежуванням аналітичної оцінки від фактичних відомостей, що особливо важливо під час розслідування кримінальних правопорушень в умовах воєнного стану та інтенсивного міжнародного обміну інформацією. Показовим є те, що 80,6 % опитаних підтримали розуміння автоматизованого збігу, ризикового профілю або іншого аналітичного результату лише як орієнтира, який потребує перевірки уповноваженим працівником, і лише 2,5 % респондентів допустили можливість використання такого результату як самостійної підстави для остаточного рішення (додаток Б).

Шенгенська інформаційна система становить інший різновид міжнародної

інформаційної взаємодії. Її становлення було пов’язане з необхідністю компенсувати скасування контролю на внутрішніх кордонах Шенгенського простору. Сучасний правовий режим визначають, зокрема, Регламенти (ЄС) 2018/1861 і 2018/1862, які регулюють використання системи для прикордонних перевірок, поліцейського та судового співробітництва [168; 169]. SIS містить сигнали щодо розшукуваних і зниклих осіб, осіб, які потребують захисту, транспортних засобів, документів, зброї та інших предметів. Додаткова інформація передається через національні бюро SIRENE, що забезпечують перевірку збігу, уточнення відомостей і координацію необхідних дій.

Функціональна побудова SIS відображає перехід від звичайного міждержавного запиту до постійно доступного спільного пошукового середовища. Національний орган одержує первинний результат без звернення дипломатичними або тривалими відомчими каналами, однак подальша дія залежить від виду сигналу та додаткових відомостей. Відповідний порядок забезпечує оперативність реагування, зберігаючи можливість змістовної перевірки. Особа або предмет не ототожнюються з даними системи автоматично: установчі ознаки зіставляються, а компетентний орган уточнює чинність сигналу та передбачену правову дію.

Правовий режим доступу до SIS ґрунтується на функціональній компетенції. Користувач одержує лише ту категорію інформації, яка необхідна для виконання визначених завдань, а перелік уповноважених органів і межі їх доступу підлягають нормативному встановленню. Така конструкція відрізняється від загального відомчого дозволу, за якого кожен працівник органу потенційно може переглядати весь ресурс. Для України обґрунтованим є закріплення функціональних профілів доступу, пов’язаних із видом завдання, процесуальним або оперативним статусом матеріалу та строком, протягом якого доступ залишається необхідним.

Нагляд за функціонуванням Шенгенської інформаційної системи поєднує національний і наднаціональний рівні. Національні органи контролюють законність операцій у відповідній частині системи, тоді як європейські інституції

забезпечують узгоджене застосування правил і перевірку центральної інфраструктури. Особа має право домагатися доступу до відомостей, їх виправлення або видалення у випадках, установлених законодавством. Поєднання технічної децентралізації з узгодженим контролем підтверджує можливість спільного пошуку без втрати відповідальності кожної держави за внесені нею дані.

Організаційна цінність SIS полягає у розподілі відповідальності між учасниками. Держава, яка створила сигнал, відповідає за законність, точність і актуальність внесених даних; орган-користувач – за правомірність запиту, перевірку збігу та подальше використання інформації. Автоматизоване повідомлення не підміняє професійного рішення, оскільки подібність установчих даних або біометричних ознак потребує підтвердження. Саме така конструкція заслуговує на врахування в Україні. Об’єднання доступу до реєстрів без визначення відповідального джерела створює ситуацію, за якої помилковий запис поширюється між органами, але жоден із них не вважає себе зобов’язаним його виправити.

Розвиток автоматизованого транскордонного пошуку пов’язаний із Прюмським механізмом. Регламент (ЄС) 2024/982 розширив можливості зіставлення профілів ДНК, дактилоскопічних даних, реєстраційних відомостей про транспортні засоби, зображень облич і поліцейських записів [173]. Механізм побудовано у два етапи: автоматизований пошук указує на можливий збіг, після чого компетентні органи перевіряють результат і надають додаткові відомості відповідно до встановленої процедури. З юридичного погляду така послідовність має запобіжне значення. Автоматичний збіг є підставою для подальшої перевірки, а не самостійним доказом тотожності особи або вчинення нею правопорушення. Українські біометричні ресурси повинні розвиватися з урахуванням аналогічного розмежування між технічним результатом і юридично значущим висновком.

Міжнародний обмін у межах Інтерполу підпорядковано Правилам оброблення даних, які регулюють внесення, використання, зберігання,

виправлення та видалення відомостей в Інформаційній системі організації [149]. Визначальними є законність, відповідність меті міжнародного поліцейського співробітництва, точність, пропорційність, безпека та відповідальність джерела. Контрольна комісія Інтерполу здійснює нагляд за дотриманням цих правил і розглядає звернення щодо доступу, виправлення або видалення даних. Наявність спеціального незалежного механізму підтверджує, що ефективність міжнародного розшуку залежить не лише від швидкості поширення повідомлення, а й від можливості усунути неправомірний або застарілий запис.

Для українських органів практичне значення має Інструкція 2020 року про порядок використання можливостей Національного центрального бюро Інтерполу [72]. Передавання відомостей із національного обліку до міжнародної системи не може бути механічним. Ініціатор повинен перевірити наявність правової підстави, достатність і точність інформації, відповідність цілям Інтерполу та відсутність політичного, військового, релігійного або расового характеру переслідування. Подальше використання одержаних відомостей також обмежується метою, з якою їх було надано. Звідси випливає загальніше положення: міжнародний канал не змінює правової природи інформації, а передавання іншому суб’єкту не звільняє орган-джерело від відповідальності за її якість.

Відомості, одержані через Інтерпол, SIS, SIENA або інший міжнародний канал, необхідно відмежовувати від доказів у кримінальному провадженні. Інформаційний збіг, повідомлення про місцезнаходження особи чи аналітичний зв’язок можуть бути підставою для проведення перевірки, направлення запиту про міжнародну правову допомогу або прийняття іншого рішення в межах компетенції. Набуття відповідними матеріалами доказового значення залежить від додержання вимог кримінального процесуального законодавства щодо джерела, форми одержання та перевірки. Змішування інформаційного й доказового режимів створює ризик використання оперативного повідомлення без належної процесуальної легалізації.

Міжнародні системи водночас забезпечують збереження історії

інформаційної взаємодії. Відомості про ініціатора, адресата, час, мету та результат запиту дають змогу оцінити послідовність дій органів різних держав і встановити відповідальність у разі порушення. Для України така простежуваність набуває значення під час документування воєнних злочинів, розшуку активів, ідентифікації осіб та перевірки транскордонних зв'язків. Єдиний журнал міжнародних запитів, побудований із дотриманням вимог таємності, дозволив би зменшити дублювання, виявляти прострочені відповіді й забезпечувати наступний контроль за використанням одержаної інформації.

Розглянуті міжнародно-правові акти та інституційні механізми утворюють узгоджену систему вимог, в якій основою виступає правомірна і визначена мета; необхідність та пропорційність оброблення; мінімізація відомостей; розмежування категорій осіб, фактів і оцінок; відповідальність джерела; контроль доступу за службовою необхідністю; журналювання операцій; перевірка актуальності; незалежний нагляд; можливість виправлення або видалення помилкових даних. Пропонуємо позначати поєднання цих вимог поняттям «принцип еквівалентного захисту». Його зміст полягає в тому, що передавання інформації іншому органові, державі або міжнародній організації не повинно знижувати рівень правових гарантій, які супроводжували її первинне одержання. Застосування цього принципу дає змогу оцінювати правомірність не лише початкового збирання, а й кожної наступної зміни мети, одержувача або способу використання.

Міжнародні стандарти встановлюють обов'язкові межі інформаційної діяльності, однак способи їх організаційного і технічного втілення відрізняються в окремих державах. Тому зарубіжний досвід доцільно досліджувати з урахуванням взаємозв'язку правового регулювання, структури правоохоронної системи, порядку управління даними та засобів контролю. Одна й та сама інформаційна система не забезпечить однакових результатів у централізованій та децентралізованій поліції, а технологічне рішення, яке спирається на сталі довірчі відносини між установами, не може бути перенесене без відповідних організаційних передумов. Предметом запозичення мають бути насамперед

принципи розподілу відповідальності, процедури перевірки та способи документування рішень, а не назви програм або зовнішній вигляд електронних сервісів.

Досвід Сполученого Королівства демонструє значення поєднання інформаційної підтримки з уніфікованою послідовністю прийняття поліцейських рішень. Національна схема прийняття рішень вимагає послідовно оцінити наявну інформацію, ризики, повноваження, можливі заходи та їх наслідки [131]. Інформація в такому порядку не сприймається як готова відповідь, а включається до процесу професійної оцінки. Працівник повинен з'ясувати, які відомості підтверджено, яких даних бракує, наскільки надійним є джерело та чи відповідає обраний захід установленим ризикам. Після вчинення дій рішення підлягає перегляду з урахуванням отриманого результату.

Для України цінним є обов'язок фіксувати не лише кінцеве рішення, а й інформаційну основу, критерії оцінювання та причини вибору певного заходу. Така вимога особливо важлива під час використання систем розпізнавання обличчя, автоматизованого визначення ризиків і прогнозного аналізу. Непрозорість вихідних даних або неможливість установити версію програми може приховати помилку та унеможливити наступний контроль. Запозичення британського підходу доцільно здійснювати через закріплення єдиної послідовності документування інформаційно обумовлених рішень у відомчих правилах і програмах професійної підготовки.

Інший напрям британського досвіду пов'язаний із взаємодією поліції та населення. Офіційні електронні ресурси дають змогу повідомити про злочин, шахрайство, зникнення особи, дорожньо-транспортну пригоду або антисоціальну поведінку, одержати відомості про територіальний підрозділ і криміногенну обстановку [154]. Електронне звернення виконує не лише сервісну, а й інформаційну функцію, оскільки створює структуроване первинне повідомлення, придатне для реєстрації, маршрутизації та подальшого аналізу. Водночас його впровадження в Україні потребує чіткого розмежування між консультаційним зверненням, повідомленням про кримінальне правопорушення

та викликом екстреної допомоги. Зручність інтерфейсу не повинна створювати невизначеність щодо процесуального статусу поданої інформації та моменту виникнення обов’язку уповноваженого органу відреагувати.

Упорядкуванню відомостей у британській поліції сприяло застосування корпоративного опису даних, за якого кожний інформаційний об’єкт визначається через його ознаки та зв’язки з іншими об’єктами [25, с. 85]. Подія, особа, документ, транспортний засіб або адреса в такому середовищі мають уніфікований зміст незалежно від підрозділу, який створив запис. Уніфікація не усуває змістових відмінностей між оперативною, криміналістичною, процесуальною та адміністративною інформацією, але забезпечує їх коректне зіставлення. Для українських правоохоронних органів аналогічне завдання пов’язане з розробленням міжвідомчої системи метаданих, яка визначатиме обов’язкові реквізити, допустимі значення, правила встановлення зв’язків та ознаки завершення життєвого циклу запису.

Британська практика водночас підтверджує необхідність розмежування відкритої інформації про стан правопорядку та відомостей, здатних ідентифікувати потерпілого, свідка або особу, щодо якої здійснюється перевірка. Відображення кримінальних подій на електронній карті має здійснюватися з таким рівнем просторового узагальнення, який забезпечує суспільну поінформованість, але не дозволяє встановити конкретну особу або точне місце її проживання. Відповідне співвідношення відкритості й приватності є актуальним для українських публічних інформаційних панелей. Публікація статистики повинна ґрунтуватися на попередньому оцінюванні ризику повторної ідентифікації внаслідок поєднання кількох відкритих наборів.

Практика США відображає особливості децентралізованої правоохоронної системи. Відсутність єдиного національного поліцейського органу компенсується функціонуванням спільних інформаційних ресурсів і стандартів обміну. Національний центр кримінальної інформації ФБР забезпечує цілодобовий доступ до відомостей про розшукуваних осіб, викрадене майно, транспортні засоби, зброю та інші об’єкти [157]. Національна система обміну

даними N-DEx дає змогу шукати, зіставляти й аналізувати матеріали, отримані від федеральних, штатних, місцевих і племінних установ, та встановлювати зв’язки між особами, місцями, предметами й подіями [158]. Розподіленість джерел не перешкоджає пошуку за умови стандартизованого опису записів і визначення відповідальності установи, яка їх надала.

Американський досвід виявляє також ризики великого інформаційного охоплення. Поєднання відомостей із різних проваджень може надати нове знання, але водночас посилити наслідки помилкової або застарілої інформації. Тому принципове значення мають перевірка записів, обмеження доступу, професійна підготовка користувачів і регулярне підтвердження актуальності даних органом-джерелом. Для України доцільним є правило, за яким запис, що може впливати на рішення щодо особи, не повинен необмежено зберігати активний статус без періодичної перевірки. Закінчення строку актуальності не обов’язково означає фізичне знищення документа, однак повинно припиняти його автоматичне відображення як чинної підстави для оперативного реагування.

Окрему роль у США відіграє система CompStat, застосування якої пов’язане з регулярним аналізом відомостей про кримінальні події, визначенням територіальних і часових закономірностей, оперативним розподілом ресурсів та оцінюванням результатів. Її значення полягає не у створенні ще однієї статистичної бази, а у включенні актуальної інформації до управлінського циклу. Показники розглядаються як підстава для постановки запитань щодо причин зміни обстановки та результативності вжитих заходів, а не як самодостатній доказ належної роботи. Вітчизняна практика може використати цей підхід за умови відмови від оцінювання підрозділів лише за кількісною динамікою зареєстрованих правопорушень.

Управлінська цінність CompStat пов’язана з коротким проміжком між реєстрацією події, її аналітичним опрацюванням і прийняттям організаційного рішення. Оперативність даних при цьому не тотожна їх остаточності: первинні показники можуть уточнюватися в міру перевірки обставин. В інформаційній

системі необхідно зберігати історію таких уточнень, оскільки заміна первинного запису без фіксації змін унеможливлює оцінювання якості початкової інформації та причин управлінської реакції. Упровадження відповідної практики в Україні потребує розмежування оперативної статистики, офіційної звітності й аналітичного прогнозу, кожен із яких має різне призначення та ступінь завершеності.

Децентралізація американської системи зумовлює істотну роль організаційних угод, стандартів інформаційної безпеки та атестації користувачів. Право доступу до спільного ресурсу пов’язується з додержанням правил введення, перевірки й використання відомостей. Установа, яка не забезпечує належної якості або захисту даних, створює ризик не лише для власного провадження, а й для всієї мережі. Такий підхід обґрунтовує запровадження в Україні періодичної перевірки інформаційної спроможності органів-учасників міжвідомчого обміну, що охоплюватиме правові процедури, захищеність технічних засобів, якість записів і підготовку персоналу.

У Канаді співвідношення відкритості діяльності органів влади та захисту приватності врегульовано двома взаємопов’язаними законодавчими актами. Закон Канади «Про доступ до інформації» закріплює право одержувати документи, що перебувають під контролем урядових установ, а Закон Канади «Про конфіденційність» регулює збирання, використання, розкриття й доступ особи до власних персональних даних [127; 165]. Відмінність предметів їх регулювання дає змогу забезпечити відкритість правоохоронного органу без необмеженого розголошення оперативних або персональних відомостей і водночас не допускає використання посилання на конфіденційність як універсальної підстави приховування всього документа.

Закон Канади «Про захист персональної інформації та електронних документів» поширив гарантії на відомості, що збираються, використовуються або розкриваються під час електронної взаємодії [163]. Як слушно зауважують В. І. Теремецький та Д. В. Цвірюк, визначення персональних даних незалежно від форми їх фіксації дає змогу охопити не лише традиційні документи й реєстри,

а й біометричні ідентифікатори [114, с. 73–82]. Такий підхід зберігає актуальність за зміни технічного носія: поява нового способу запису не виводить інформацію з-під правового захисту.

Важливою рисою канадської системи є інституційне розмежування функцій контролю. Уповноважений з питань інформації розглядає скарги на порушення доступу до урядових документів, тоді як Уповноважений з питань конфіденційності забезпечує нагляд за обробленням персональних даних. На рівні провінцій діють власні закони, які враховують особливості місцевого управління [156]. Для України практичне значення має застосування тесту шкоди й суспільного інтересу до конкретної інформації. Правовий режим повинен визначатися змістом відомостей, а не лише назвою документа або органом, у якому він створений. Такий підхід дає змогу узгодити прозорість із захистом таємниці досудового розслідування, оперативно-розшукової діяльності та персональних даних.

Процедура часткового доступу, закріплена в законодавстві Канади, зобов’язує відокремити інформацію, розголошення якої може завдати визначеної законом шкоди, від решти документа. Відмова у доступі до всього матеріалу є виправданою лише тоді, коли таке відокремлення неможливе або позбавляє документ змісту. Для української правоохоронної практики зазначене положення має методологічне значення. Інформація з обмеженим доступом повинна визначатися на рівні конкретних відомостей, а не шляхом автоматичного присвоєння обмежувального грифа всьому масиву, у якому вони містяться. Застосування цього правила підвищить прозорість діяльності органів правопорядку без розголошення охоронюваної законом таємниці.

Німецький досвід підтверджує можливість централізованої координації за збереження компетенції земель. Інформаційна система INPOL забезпечує обмін між Федеральним відомством кримінальної поліції, федеральною поліцією та поліцейськими органами земель. Її організаційна перевага полягає у спільних правилах опису даних і розмежуванні відповідальності, а не в повному зосередженні всіх ресурсів в одному органі. Кожен учасник зберігає визначені

повноваження, але може одержувати необхідну інформацію через погоджені процедури.

Федеративна побудова правоохоронної системи Німеччини зумовлює необхідність розрізняти координацію, спільний пошук і безпосереднє розпорядження даними. Федеральний рівень забезпечує функціонування загальних засобів і стандартів, тоді як поліцейські органи земель залишаються відповідальними за відомості, одержані під час виконання власних повноважень. Такий розподіл запобігає втраті зв'язку між записом і первинним матеріалом. Якщо інформація потребує уточнення, запит спрямовується до органу, який може перевірити обставини її виникнення, а не до технічного адміністратора системи.

Інформаційне забезпечення німецької поліції включає також відкриті електронні ресурси, за допомогою яких громадяни одержують нормативні роз'яснення, подають звернення та встановлюють компетентний підрозділ [129; 128]. Розвиток зовнішніх сервісів не змішується з режимом спеціальних поліцейських систем. Публічний портал виконує інформаційно-комунікаційну функцію, тоді як доступ до оперативних масивів здійснюється в захищеному середовищі. Для України таке розмежування має запобігти технічному поєднанню відкритого інтерфейсу з внутрішніми ресурсами без додаткового рівня перевірки та захисту.

Подібний принцип відповідає потребам України, де інформаційні ресурси належать різним правоохоронним органам і створюються для неоднакових завдань. Інтеграція не повинна означати безконтрольного фізичного об'єднання всіх масивів. Доцільніше забезпечити пошук і передавання необхідного мінімуму відомостей між автономними системами на підставі конкретного повноваження. При цьому кожен запит має журналюватися, а власник ресурсу – зберігати відповідальність за якість первинного запису. Така організація зменшує дублювання, не руйнуючи функціонального розмежування органів.

Естонський досвід розвиває ідею розподіленої інформаційної взаємодії. Захищений шар обміну X-tee забезпечує передавання даних між інформаційними

системами без необхідності створювати єдину всеохопну базу [182]. Відомості зберігаються у відповідального розпорядника, а інший учасник одержує їх через уніфікований ідентифікований запит. Технічне середовище доповнюється організаційними правилами під'єднання, електронною ідентифікацією користувача та можливістю перевірити здійснені операції. Розподілений підхід зменшує кількість копій одного масиву й полегшує виправлення помилки в першоджерелі.

Запровадження подібного способу взаємодії в українській правоохоронній сфері потребує попереднього нормативного визначення мети кожного обміну, переліку доступних полів, категорій користувачів і випадків, коли необхідне додаткове рішення уповноваженої особи. Технічна можливість одержати відомості не може автоматично перетворюватися на юридичне право доступу. Саме розмежування технічної та правової доступності становить одну з найцінніших рис естонської практики. Загальний захищений канал забезпечує взаємодію, але не скасовує спеціальних правових режимів окремих реєстрів.

Досвід Швеції, Данії та інших північноєвропейських держав розкриває сервісний напрям інформаційного забезпечення. Офіційні електронні ресурси поліції Швеції дають змогу повідомляти про окремі види правопорушень, одержувати поради щодо запобігання злочинам, стежити за перебігом розгляду звернення та користуватися інформацією, пристосованою до потреб різних груп населення [164]. Взаємодія ґрунтується на довірі, яка підтримується не рекламними повідомленнями, а передбачуваністю процедури, доступністю пояснень і можливістю одержати зворотний зв'язок. Інформаційна відкритість у такому розумінні є складником превентивної діяльності: громадянин краще розуміє ризики, порядок звернення та межі повноважень поліції.

Шведська практика проблемно орієнтованої поліцейської діяльності пов'язує інформаційний ресурс із потребами конкретної територіальної громади. Відомості про повторювані події, звернення населення та локальні чинники небезпеки використовуються для визначення причин проблеми й вибору превентивних заходів. Якість інформаційного забезпечення оцінюється не

кількістю створених записів, а здатністю перетворити їх на обґрунтоване рішення та пояснити його громаді. В українських умовах цей підхід може бути реалізований шляхом поєднання статистичних даних поліції з результатами опитувань населення, повідомленнями органів місцевого самоврядування та аналізом повторних звернень.

Під час масових заходів шведська поліція застосовує інформаційно-комунікаційний підхід, у межах якого спеціально підготовлені працівники підтримують діалог з організаторами й учасниками [178, с. 77; 137]. Одержана інформація дає змогу своєчасно оцінювати зміну обстановки та відмежовувати поведінку окремих правопорушників від дій мирних учасників. Для інформаційного забезпечення принциповим є документування не лише ризикових ознак, а й обставин, які свідчать про мирний характер поведінки. Однобічне накопичення негативних сигналів викривлює оцінку і може спричинити непропорційне застосування поліцейських заходів.

Данська практика пов’язана з послідовним розвитком електронного урядування, захищеної ідентифікації та міжвідомчого документообігу. Портал Borger.dk, створений у 2003 році, поступово перейшов від розміщення довідкових матеріалів до надання транзакційних послуг [124]. Єдиний засіб електронної ідентифікації забезпечив доступ до державних і приватних сервісів, а взаємодія центральних органів, місцевого самоврядування та фінансового сектору створила спільне середовище довіри. Державна поліція Данії також розвивала електронні послуги, пов’язані з документуванням особи та захищеним використанням установчих даних [134].

Послідовність данської цифрової трансформації свідчить про залежність складних електронних послуг від базової інфраструктури ідентифікації, електронного підпису та захищеного документообігу. Перехід до операцій, що породжують юридичні наслідки, відбувся після формування надійного механізму підтвердження особи та взаємного визнання електронних дій різними установами. Для правоохоронної сфери зазначена послідовність має особливе значення, оскільки помилка в електронній ідентифікації заявника або працівника

може вплинути на реєстрацію повідомлення, доступ до матеріалів і достовірність подальших дій.

Для українських правоохоронних органів значення північноєвропейського досвіду не обмежується збільшенням кількості послуг. Вирішальними є однозначна електронна ідентифікація, доступність для осіб з інвалідністю, фіксація статусу звернення та однократне подання відомостей, які вже перебувають у розпорядженні держави. Водночас принцип однократності не може виправдовувати необмежене передавання даних між органами. Повторне витребування від громадянина усувається лише тоді, коли інший орган має законну мету та визначене повноваження одержати відповідні відомості.

Електронні послуги становлять зовнішній, орієнтований на громадянина складник інформаційного забезпечення правоохоронної діяльності. Вони охоплюють електронні звернення, повідомлення про події, перевірку стану розгляду, одержання довідок, запис на прийом, сплату адміністративних платежів та доступ до відкритої статистичної інформації. Їх розвиток зменшує організаційне навантаження і розширює доступ до органів правопорядку, особливо в умовах воєнного стану, переміщення населення та небезпеки особистого відвідування установ. Проте електронна форма не повинна знижувати процесуальні гарантії або перекладати на заявника ризик технічної несправності. Система має підтверджувати прийняття повідомлення, фіксувати час, забезпечувати маршрутизацію за компетенцією та повідомляти про подальший статус.

Порівняння розглянутих національних практик дає підстави виокремити дві організаційні форми інформаційного забезпечення. Перша ґрунтується на великих централізованих або спільних ресурсах, як у випадку NCIC, N-DEx, SIS чи окремих систем Європолу. Друга використовує розподілене зберігання та уніфікований захищений обмін, прикладом чого є X-tee та німецька координація між федеральним і земельним рівнями. Жодна з форм не має безумовної переваги. Централізація спрощує пошук, але збільшує наслідки несанкціонованого доступу та помилки; розподіленість зберігає відповідальність

власника, проте потребує високої сумісності й чітких правил запиту. Вибір повинен залежати від характеру даних, мети використання і допустимого рівня ризику. Анкетування засвідчило близькість цієї позиції до професійного сприйняття проблеми: 39,4 % респондентів найбільш придатною для України визнали естонську модель розподіленого захищеного обміну, а 23,0 % підтримали комбінований підхід, який поєднує централізовані ресурси з відповідальністю органу-джерела та уніфікованими правилами доступу (додаток Б).

Для України прийнятною є поєднана архітектура. Базові довідники, засоби ідентифікації користувачів, правила обміну й журнали взаємодії мають бути уніфікованими, тоді як спеціальні масиви доцільно залишати у віданні компетентних органів. Пошук повинен надавати рівно той обсяг відомостей, який необхідний для виконання конкретного завдання. Розширений доступ до змісту оперативних, розвідувальних або процесуальних матеріалів має потребувати окремого обґрунтування. Такий порядок дозволить поєднати оперативність із відомчою відповідальністю та не допустити ситуації, коли належність працівника до певного органу автоматично відкриває всі наявні державні ресурси.

Порівняння досліджених підходів із чинним регулюванням в Україні засвідчує відсутність єдиних вимог до міжвідомчого обміну правоохоронною інформацією. Повноваження щодо одержання, перевірки, зберігання й передавання відомостей визначено законами про окремі правоохоронні органи та підзаконними актами, які неоднаково регулюють подібні за змістом операції. Наслідками є дублювання записів, відмінність правил доступу, невизначеність відповідального за виправлення помилки та неоднаковий рівень захисту прав особи залежно від відомчої належності інформаційного ресурсу.

Вирішення зазначеної проблеми вбачаємо в ухваленні міжвідомчого нормативно-правового акта про інформаційну взаємодію органів правопорядку. Його положення повинні визначати принципи обміну, категорії учасників, правові підстави і зміст запиту, строки опрацювання, формати даних, правила

перевірки, підстави повної або часткової відмови, порядок журналювання, виправлення, обмеження використання та видалення відомостей. Такий нормативно-правовий акт не має підміняти спеціальні закони або розкривати негласні способи роботи, а його призначення полягає у встановленні спільних організаційних правил і правових гарантій, які діятимуть незалежно від технічної платформи та відомчої належності ресурсу.

Першочергового значення набуває формування єдиного понятійного й класифікаційного середовища. Відомості про осіб, події, предмети, території, види правопорушень і ступені достовірності повинні описуватися за погодженими довідниками. Йдеться не про уніфікацію змісту всіх обліків, а про забезпечення однакового розуміння ключових реквізитів під час обміну. Якщо різні органи неоднаково позначають статус особи, завершення розшуку або рівень перевіреності повідомлення, технічне з’єднання систем лише прискорює поширення неоднозначності.

Другим напрямом має стати міжвідомче керування якістю даних. За кожним первинним записом необхідно закріпити орган-джерело, відповідальний за точність, своєчасне оновлення і виправлення. Строк актуальності повинен визначатися з урахуванням виду інформації та можливих наслідків її використання. Відомості про чинний розшук потребують частішого підтвердження, ніж архівні статистичні дані. Користувач, який виявив невідповідність, має отримати передбачений канал повідомлення джерела та можливість тимчасово позначити запис як такий, що перевіряється. Без цього помилка продовжуватиме відтворюватися в нових рішеннях.

Третій напрям пов’язаний із переходом від доступу за посадою до доступу за службовою необхідністю і конкретним завданням. Належність працівника до правоохоронного органу сама по собі не обґрунтовує перегляд усіх наявних відомостей. Інформаційна система повинна враховувати компетенцію підрозділу, вид провадження, роль користувача та мету запиту. Для невідкладних випадків може встановлюватися спеціальний порядок розширеного доступу з обов’язковим наступним контролем. Виняткова

процедура не повинна перетворюватися на звичайний спосіб обходу обмежень.

Четвертий напрям становить розвиток внутрішнього й незалежного нагляду. Автоматизовані журнали операцій мають використовуватися не лише після витоку, а й для регулярного виявлення нетипових запитів, масового перегляду, звернень до даних осіб, не пов’язаних із завданням, та інших ознак зловживання. Внутрішній контроль повинен доповнюватися зовнішнім наглядом органу, який має достатні повноваження, професійну спроможність і незалежність. Особа, права якої порушено, повинна мати дієвий спосіб домогтися перевірки, виправлення або припинення неправомірного використання інформації без розкриття законно охоронюваних способів правоохоронної діяльності.

Застосування автоматизованого аналізу та систем штучного інтелекту потребує додаткових гарантій. Регламент Європейського Союзу про штучний інтелект відносить низку правоохоронних застосувань до систем високого ризику та забороняє окремі способи використання [172]. Алгоритмічний результат у правоохоронній діяльності доцільно визнавати рекомендаційною інформацією, а не самостійною юридичною підставою обмеження прав. Обов’язковими мають бути перевірка якості навчальних даних, оцінювання ризику дискримінаційного впливу, можливість змістовного перегляду працівником, документування версії програмного засобу та пояснення основних чинників, що вплинули на результат. Відповідні вимоги необхідно враховувати вже на стадії закупівлі та дослідної експлуатації, а не після виникнення негативних наслідків.

Підготовка користувачів є самостійною складовою інформаційного забезпечення. Працівник повинен розуміти правову мету оброблення, відрізняти факт від аналітичної оцінки, перевіряти походження відомостей, правильно визначати ступінь доступу та фіксувати власні дії. Навчання доцільно будувати на практичних ситуаціях: помилковому збігу біометричних даних, застарілому записі про розшук, міжнародному запиті з недостатнім обґрунтуванням, необхідності термінового доступу за наявності загрози життю, витоку облікового

запису. Результатом підготовки має бути не формальне проходження курсу, а здатність ухвалити законне й обґрунтоване рішення та відтворити інформаційний шлях, який до нього привів.

Воєнний стан і збройна агресія проти України надають розглянутим положенням додаткового змісту. Документування воєнних злочинів, розшук зниклих безвісти, ідентифікація загиблих, протидія диверсійній діяльності та кібератакам потребують швидкого поєднання відомостей із різних національних і міжнародних джерел. Водночас значні масиви біометричних даних, матеріалів фото- і відеофіксації та інформації про потерпілих мають підвищену чутливість. Їх витік може загрожувати життю людей, безпеці операцій і можливості подальшого використання матеріалів у кримінальному провадженні. Тому воєнна необхідність обґрунтовує прискорення законної взаємодії, але не усунення правил перевірки, цільового використання й захисту.

Проведене дослідження засвідчує, що придатність міжнародного та зарубіжного досвіду для України визначається узгодженістю правових, організаційних і технічних складників інформаційної взаємодії. Взаємосумісність ресурсів повинна поєднуватися з відповідальністю органу-джерела, доступом у межах службової необхідності, перевірюваністю операцій, регулярним підтвердженням актуальності відомостей, можливістю виправлення помилки та незалежним наглядом. Недодержання цих вимог призводить або до масштабування неправомірного втручання засобами сучасних технологій, або до уповільнення законного обміну внаслідок невизначеності процедур.

Інформаційне забезпечення правоохоронної діяльності в міжнародному та національному вимірах запропоновано розуміти як нормативно врегульовану, організаційно узгоджену й технічно підтримувану систему керування відомостями, у межах якої оперативність доступу забезпечується одночасно з установленням походження даних, перевіркою їх якості, дотриманням визначеної мети, документуванням дій користувача та гарантуванням поновлення порушеного права. Розвиток такої системи в Україні має ґрунтуватися на розподіленій відповідальності за інформаційні ресурси та

взаємосумісності правил їх використання. Інформаційний суверенітет держави за цього підходу характеризує її спроможність визначати правові підстави доступу, контролювати транскордонний рух відомостей, установлювати відповідальність кожного учасника обміну та забезпечувати припинення використання неправомірного або помилкового запису.

Висновки до розділу 1

1. Генеза інформаційного забезпечення правоохоронної діяльності в Україні відбувалася шляхом послідовного ускладнення способів одержання, фіксації, перевірки, накопичення, систематизації, передавання та використання відомостей, а також поступового формування правових гарантій їх належного оброблення. Періодизація становлення та розвитку інформаційного забезпечення правоохоронної діяльності в Україні охоплює такі історичні етапи: I. *протореєстраційний* (від найдавніших часів до сер. XIV ст.), для якого характерними були усне передавання відомостей, звичаєві способи розпізнавання правопорушника, колективна пам'ять громади та ситуативний розшук; II. *документально-обліковий* (сер. XIV ст. – перша пол. XIX ст.), пов'язаний із поширенням письмової фіксації правопорушень, судових рішень, описів осіб і майна, формуванням локальних реєстрів та закріпленням обов'язку посадових осіб документувати юридично значущі обставини; III. *криміналістично-ідентифікаційний* (друга половина XIX ст. – 1917 р.), що характеризувався професіоналізацією розшукової діяльності, розвитком фотографування, дактилоскопії, антропометрії, систематизованих описів зовнішності та карткових обліків; IV. *централізовано-картотечний* (1917 р. – сер. 1950-х рр.), пов'язаний з уніфікацією форм обліку, централізацією картотек розшукуваних, засуджених і зниклих безвісти осіб, створенням міжтериторіальних каналів обміну за умов надмірної закритості та недостатніх гарантій прав людини; V. *автоматизовано-обчислювальний* (сер. 1950-х –

1991 р.), що відзначався застосуванням обчислювальної техніки, переходом від ручних картотек до автоматизованого пошуку, формуванням спеціалізованих інформаційних центрів і первинною стандартизацією машинного оброблення даних; VI. *національно-інформаційний* (1991 р. – 2010 р.), у межах якого сформовано законодавчу основу інформаційних відносин незалежної України, розвинуто відомчі інформаційні системи, електронні обліки та міжнародне поліцейське співробітництво, однак збережено проблему відомчої роз'єднаності, дублювання інформаційних масивів і неоднакових правил доступу; VII. *інтеграційно-цифровий* (2011 р. і дотепер), змістом якого є перехід до міжвідомчої електронної взаємодії, розподілених реєстрів, біометричної ідентифікації, автоматизованої аналітики, електронних послуг та адаптації національного законодавства до стандартів Європейського Союзу. У межах цього етапу виокремлено *воєнно-інтеграційний* підетап (з 2022 р.), зумовлений повномасштабною збройною агресією проти України, зміст якого визначають документування воєнних злочинів, розшук зниклих безвісти, ідентифікація загиблих, протидія диверсійній діяльності, кіберзагрозам і колабораційним проявам, опрацювання значних масивів цифрових, біометричних та оперативно значущих даних, поглиблення міжнародного інформаційного обміну й одночасне посилення вимог до законності, достовірності, захищеності та доказової придатності інформації.

2. Інформаційне забезпечення правоохоронної діяльності запропоновано розуміти як нормативно врегульовану, організаційно узгоджену й технічно підтримувану систему діяльності уповноважених суб'єктів щодо визначення інформаційних потреб та здійснення повного життєвого циклу відомостей: одержання, перевірки, реєстрації, систематизації, зберігання, пошуку, зіставлення, аналізу, передавання, використання, перегляду актуальності, виправлення, архівування або видалення для своєчасного, законного й обґрунтованого виконання правоохоронних завдань.

3. Доведено, що інформаційно-аналітичне забезпечення є функціонально поглибленою складовою інформаційного забезпечення, результатом якої

виступає нове знання, необхідне для підготовки правоохоронного рішення, тоді як інформаційна безпека характеризує стан захищеності відповідних ресурсів, систем і процесів. Сформульовано доктринальне положення про інформаційне забезпечення як наскрізну організаційно-правову гарантію правоохоронної діяльності, рівень зрілості якої визначається не обсягом накопичених даних, а можливістю встановити їх походження, перевірити якість, відтворити інформаційний шлях до прийнятого рішення та персоніфікувати відповідальність за наслідки використання.

4. Встановлено, що міжнародно-правові стандарти інформаційного забезпечення правоохоронної діяльності формують багаторівневу систему, яка охоплює загальні принципи прав людини, стандарти Ради Європи, право Європейського Союзу, правила міжнародних поліцейських організацій та двосторонні й багатосторонні механізми обміну, зокрема Директива (ЄС) 2023/977 про обмін інформацією між правоохоронними органами держав-членів, регламенти щодо Шенгенської інформаційної системи, оновлений Прюмський механізм автоматизованого пошуку, правила Європолу, Інтерполу та модернізовані стандарти Ради Європи. Системний аналіз таких нормативно-правових актів дозволив сформулювати принцип еквівалентного захисту, відповідно до якого передавання інформації іншій державі або міжнародній організації не повинно знижувати рівень правових гарантій, що супроводжували її первинне збирання.

5. Зарубіжний досвід засвідчив наявність різних організаційно-правових підходів до інформаційного забезпечення правоохоронної діяльності: у Сполученому Королівстві пріоритет надано послідовному оцінюванню інформації, ризику, повноважень і наслідків поліцейського рішення; у Німеччині – координації та спільним правилам роботи з даними зі збереженням компетенції земель; в Естонії – розподіленому обміну через захищений уніфікований шар без багаторазового копіювання одного масиву; у Канаді – розмежуванню відкритості публічної інформації та захисту приватності із застосуванням тесту шкоди й суспільного інтересу; у Сполучених Штатах Америки – функціонуванню

великих розподілених ресурсів за умови стандартизованого введення, перевірки та регулярного підтвердження актуальності записів. Спільним для результативних зарубіжних практик є не максимальна концентрація відомостей в одній базі, а сумісність класифікаторів, відповідальність органу-джерела, доступ за службовою необхідністю, захищені канали обміну, простежуваність запитів, можливість виправлення помилок та незалежний контроль.

РОЗДІЛ 2. ТЕОРЕТИЧНІ ЗАСАДИ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ В УКРАЇНІ

У сучасних умовах інформаційне забезпечення правоохоронної діяльності набуває значення однієї з базових організаційно-правових передумов належного виконання правоохоронних завдань. Від якості, повноти, своєчасності, достовірності, актуальності та захищеності інформації, що надходить до правоохоронних органів, залежить не лише результативність запобігання, виявлення, припинення й розслідування правопорушень, а й здатність держави підтримувати публічну безпеку, протидіяти організованій злочинності, кіберзагрозам, диверсійній діяльності, незаконному обігу зброї, корупційним проявам та іншим загрозам, що особливо посилилися в умовах воєнного стану. У правоохоронній сфері інформація не може розглядатися лише як допоміжне повідомлення про певну подію. Вона набуває значення правового, організаційного й аналітичного ресурсу, від належного режиму формування, перевірки, використання та захисту якого залежить законність, обґрунтованість і перевірюваність прийнятого правоохоронного рішення.

Теоретичне осмислення інформаційного забезпечення правоохоронної діяльності має принципове значення для визначення його змісту, структури, функцій, принципів, інструментів та меж використання інформаційних ресурсів у діяльності правоохоронних органів. Водночас у науковій літературі зазначене явище нерідко розглядається фрагментарно: крізь призму інформатизації, електронних реєстрів, інформаційно-аналітичної діяльності, захисту інформації, кримінального аналізу або технічної модернізації. Такий підхід є корисним для характеристики окремих складових, однак не повною мірою розкриває інформаційне забезпечення як цілісне правоохоронне явище. На думку І. П. Катеринчука, правова природа інформаційного забезпечення правоохоронних органів розкривається через поєднання правового регулювання, організаційних процедур, інформаційних ресурсів і діяльності уповноважених суб’єктів [35, с. 10]. Як стверджують В. А. Кудінов і К. В. Яровий, інформаційне забезпечення

правоохоронної діяльності охоплює інформаційні процеси, ресурси, технології та правила безпечної роботи з відомостями, що мають безпосереднє значення для виконання правоохоронних завдань [46, с. 6–9].

З огляду на це теоретичні засади інформаційного забезпечення правоохоронної діяльності доцільно розглядати як систему взаємопов'язаних наукових положень про електронну готовність правоохоронних органів, інструменти роботи з інформацією та повноваження суб'єктів, які створюють, отримують, перевіряють, реєструють, накопичують, аналізують, передають, використовують і захищають відповідні відомості. Такий підхід узгоджується з положеннями Комплексного стратегічного плану реформування органів правопорядку як частини сектору безпеки і оборони України на 2023–2027 рр, у якому цифрова трансформація органів правопорядку визначена одним із важливих напрямів їх модернізації, підвищення ефективності, прозорості та спроможності діяти відповідно до сучасних безпекових викликів [87].

Інформаційне забезпечення правоохоронної діяльності слід аналізувати через три взаємопов'язані рівні. Перший рівень становить інформаційна потреба, що виникає у зв'язку з конкретним правоохоронним завданням: перевіркою повідомлення про правопорушення, встановленням особи, розшуком, аналізом ризику, документуванням події, плануванням оперативних заходів, забезпеченням публічної безпеки або підготовкою процесуального рішення. Другий рівень охоплює правомірне одержання, перевірку, реєстрацію, накопичення, систематизацію, зберігання, пошук, зіставлення, аналіз, передавання, використання та захист відомостей. Третій рівень пов'язаний із використанням інформаційного результату у правоохоронному рішенні, яке має бути законним, мотивованим, персоніфікованим і таким, що може бути перевірене з погляду джерела інформації, способу її отримання, достовірності та допустимості використання. За такого підходу інформаційне забезпечення виступає не допоміжним технічним елементом, а самостійною організаційно-правовою основою правоохоронної діяльності.

В умовах воєнного стану значення інформаційного забезпечення

правоохоронної діяльності істотно зростає. Правоохоронні органи одночасно виконують завдання щодо протидії загальнокримінальній та організованій злочинності, документування воєнних злочинів, установлення осіб, причетних до колабораційної діяльності, розшуку безвісти зниклих, ідентифікації загиблих, контролю за переміщенням зброї, протидії диверсійним і кіберзагрозам, захисту критичної інфраструктури та взаємодії з міжнародними партнерами. За таких умов помилка в інформаційному ресурсі, несвоєчасне оновлення відомостей, відсутність фіксації доступу або неконтрольоване використання даних можуть спричинити не лише організаційні, а й процесуальні, правозахисні та безпекові наслідки. Саме тому інформаційне забезпечення правоохоронної діяльності має розглядатися як правомірно організований цикл роботи з відомостями, у межах якого кожна інформаційна дія повинна мати визначену мету, належну правову підставу, відповідального суб'єкта та можливість подальшої перевірки.

2.1. Характеристика електронної готовності впровадження сучасних практик інформаційного забезпечення правоохоронної діяльності в Україні

У контексті цифрової трансформації державного сектору електронна готовність правоохоронних органів є однією з визначальних умов упровадження сучасних практик інформаційного забезпечення правоохоронної діяльності. Її зміст не може зводитися лише до наявності комп'ютерної техніки, каналів зв'язку, доступу до мережі Інтернет або окремих інформаційно-комунікаційних систем. Для правоохоронної сфери електронна готовність має комплексний організаційно-правовий характер і охоплює нормативну, управлінську, технічну, кадрову, аналітичну та безпекову спроможність уповноважених органів працювати з інформацією у спосіб, що забезпечує своєчасність реагування, законність доступу, достовірність і актуальність відомостей, захист персональних даних, фіксацію інформаційних операцій та придатність результатів оброблення для виконання правоохоронних завдань.

У науковій літературі електронну готовність здебільшого пов’язують із готовністю державних інституцій застосовувати інформаційно-комунікаційні технології для надання адміністративних послуг, внутрішнього управління, електронного документообігу та взаємодії із суспільством. Для правоохоронної діяльності такий підхід потребує суттєвого уточнення, оскільки правоохоронні органи використовують інформацію не лише в адміністративно-організаційних процесах, а й у запобіганні правопорушенням, оперативному реагуванні, розшуку осіб, документуванні кримінальних правопорушень, управлінні силами і засобами, кримінальному аналізі, підтримці досудового розслідування та міжнародній правоохоронній взаємодії. На думку А. В. Мовчана, інформаційно-аналітичне забезпечення оперативно-розшукової діяльності передбачає цілеспрямоване опрацювання для оцінювання оперативної обстановки та підготовки управлінських і тактичних рішень [52, с. 184–187]. К. Ю. Ісмайлов також пов’язує проблеми інформаційно-аналітичної діяльності Національної поліції з необхідністю належного теоретико-правового осмислення її організації, функціонального призначення та правових меж [32, с. 109–115]. З огляду на це електронна готовність правоохоронного органу має оцінюватися не за кількістю програмних засобів або електронних ресурсів, а за його здатністю правомірно перетворювати дані на перевірену інформаційну основу правоохоронних дій і рішень.

На нашу думку, *електронну готовність правоохоронних органів України до впровадження сучасних практик інформаційного забезпечення доцільно визначати як стан нормативної, організаційної, кадрової, технічної, аналітичної та безпекової спроможності уповноважених суб’єктів використовувати інформаційні ресурси, інформаційно-комунікаційні системи й цифрові інструменти для своєчасного, законного, обґрунтованого та підконтрольного виконання правоохоронних завдань*. У такому розумінні електронна готовність є не тільки показником технічного оснащення, а якісною характеристикою функціонування правоохоронної системи, що залежить від стану законодавства, узгодженості відомчих процедур, сумісності

інформаційних ресурсів, підготовки персоналу, рівня кіберзахисту, якості даних та реальної практики міжвідомчої взаємодії.

На відміну від загальнодержавного розуміння електронної готовності, у правоохоронній сфері така має оцінюватися крізь призму правоохоронної придатності інформації. Орган може мати розвинену технічну інфраструктуру, проте залишатися недостатньо готовим до сучасного інформаційного забезпечення, якщо користувачі не розуміють правового режиму даних, реєстри не узгоджені між собою, обліки ведуться за різними класифікаторами, доступ надається без належного обґрунтування, а результати автоматизованого пошуку не перевіряються уповноваженим працівником. Водночас навіть обмежені технічні ресурси можуть забезпечити належний рівень правоохоронної роботи за умови існування чітких правил внесення, перевірки, актуалізації, використання, передавання, журналювання та захисту даних. Тому електронна готовність повинна характеризувати спроможність правоохоронного органу забезпечити законний і контрольований рух інформації від первинного повідомлення до правоохоронного рішення.

Методологічно електронну готовність правоохоронних органів доцільно розглядати як поєднання шести взаємопов’язаних складових. *Нормативна* складова визначає правові підстави створення інформаційного ресурсу, категорії відомостей, що можуть до нього вноситися, коло користувачів, порядок доступу, строки зберігання та гарантії захисту. *Організаційна* охоплює розподіл відповідальності між суб’єктами, маршрути руху інформації, порядок міжвідомчої взаємодії, внутрішній контроль і реагування на помилки в інформаційних ресурсах. *Технічна* включає програмні, телекомунікаційні, криптографічні та інші засоби, необхідні для безперервності, сумісності й захищеності роботи інформаційних систем. *Кадрова* пов’язана із професійною здатністю працівників працювати з цифровими інструментами без порушення правового режиму інформації, службової дисципліни та прав людини. *Аналітична* забезпечує перехід від окремого запису чи повідомлення до обґрунтованого висновку, оцінки ризику або інформаційної підстави для

прийняття рішення. *Безпекова* спрямована на захист інформаційних ресурсів від витоку, спотворення, втрати, несанкціонованого доступу, неправомірного копіювання та використання поза визначеною правоохоронною метою.

У сучасних умовах до зазначених складових електронної готовності правоохоронних органів доцільно додати критерій функціональної стійкості. Його зміст полягає у здатності правоохоронного органу забезпечувати безперервну, законну й контрольовану роботу з інформаційними ресурсами під час кібератак, пошкодження або руйнування інфраструктури, евакуації підрозділів, тимчасового обмеження зв'язку, зміни територіальної підслідності, переміщення матеріалів кримінальних проваджень, а також за необхідності невідкладної взаємодії з іншими органами сектору безпеки і оборони. Стратегія кібербезпеки України [96] пов'язує захищеність цифрового середовища з національною безпекою, а Комплексний стратегічний план реформування органів правопорядку на 2023–2027 роки визначає цифрову трансформацію одним із напрямів модернізації органів правопорядку [87]. Для правоохоронної діяльності наведені положення означають, що електронна готовність має охоплювати не лише можливість доступу до даних у звичайних умовах, а й спроможність зберегти керованість інформаційних процесів, цілісність відомостей, фіксацію дій користувачів та придатність інформації для подальшого використання у правоохоронному рішенні під час кризових обставин.

Нормативна складова електронної готовності полягає у наявності правових підстав для створення, ведення, використання, взаємодії, інтеграції та захисту інформаційних ресурсів. Основне значення у цій сфері мають Закон України «Про інформацію» [86], Закон України «Про захист персональних даних» [84], Закон України «Про захист інформації в інформаційно-комунікаційних системах» [83], Закон України «Про основні засади забезпечення кібербезпеки України» [92], а також спеціальні закони, що визначають інформаційні повноваження Національної поліції України [90], СБУ [99], ДБР [61], БЕБ [60], НАБУ [89], ДПСУ [62] та інших суб'єктів

правоохоронної діяльності. Водночас значна кількість нормативно-правових актів не завжди свідчить про належний рівень правового регулювання, якщо відповідні акти не формують узгодженого порядку доступу до відомостей, їх обміну, фіксації, перевірки, виправлення, актуалізації, зберігання та припинення використання.

Нормативна основа електронної готовності правоохоронних органів має будуватися за логікою повного життєвого циклу даних. Закон України «Про інформацію» [86] закріплює загальні засади інформаційних відносин, Закон України «Про захист персональних даних» [84] визначає вимоги до оброблення відомостей про особу, Закон України «Про захист інформації в інформаційно-комунікаційних системах» [83] встановлює правові засади захисту інформації в інформаційних системах, а Закон України «Про публічні електронні реєстри» [95] формує загальні правила створення, ведення, взаємодії та адміністрування публічних електронних реєстрів. У правоохоронній діяльності зазначені акти не можуть застосовуватися відокремлено один від одного, оскільки інформаційний ресурс одночасно є об’єктом правового режиму інформації, персональних даних, технічного захисту, електронної взаємодії та службового використання. Саме тому нормативне регулювання має забезпечувати єдиний порядок визначення інформаційної потреби, правової підстави доступу, категорії даних, мети оброблення, строку зберігання, порядку виправлення помилок, обмеження доступу, контролю за використанням і відповідальності за порушення встановлених правил.

Закон України «Про публічні електронні реєстри» орієнтує правове регулювання на реєстрацію, взаємодію, ідентифікацію суб’єктів, облік дій, визначеність держателя й адміністратора реєстру, а також використання реєстрової інформації у межах установлених законом повноважень [95]. Водночас реєстр не може сприйматися як сховище відомостей, а виступає правовим інструментом, у межах якого кожен запис повинен мати встановлене походження, автора, дату створення, підставу внесення, режим доступу, строк актуальності та визначені межі подальшого використання. Відсутність таких

реквізитів ускладнює перевірку інформації, створює ризик повторного використання помилкового або застарілого запису та знижує придатність відомостей для прийняття законного й обґрунтованого правоохоронного рішення.

Окрему роль у формуванні нормативної основи електронної готовності відіграють закони про електронні документи, електронний документообіг та електронну ідентифікацію. Закон України «Про електронні документи та електронний документообіг» [65] визначає правовий статус електронного документа, а Закон України «Про електронну ідентифікацію та електронні довірчі послуги» [67] встановлює засади електронної ідентифікації, автентифікації та використання довірчих послуг. Для інформаційного забезпечення правоохоронної діяльності такі нормативно-правові акти мають значення не лише як елементи загальної цифровізації документообігу. Електронний документ, електронний підпис, електронна позначка часу, ідентифікація користувача та фіксація дії в системі виконують гарантійну функцію, оскільки підтверджують походження відомостей, цілісність інформації, час її створення або зміни та належність відповідної дії конкретному суб’єкту. У кримінальному провадженні, оперативно-розшуковій діяльності, розшуковій роботі, міжнародному інформаційному обміні та управлінні силами і засобами така перевірка має безпосереднє значення для законності подальших правоохоронних дій.

Організаційна складова електронної готовності виявляється у здатності правоохоронних органів забезпечити належний розподіл функцій між підрозділами, визначити відповідальних осіб за ведення інформаційних ресурсів, установити порядок взаємодії з іншими органами та забезпечити контроль за використанням інформації. Д. В. Федотов стверджує, що інформаційна безпека в Національній поліції України потребує чіткого адміністративно-правового механізму, у межах якого компетенція суб’єктів, правовий режим інформації, внутрішній контроль і відповідальність мають бути взаємопов’язаними [119, с. 42]. В. П. Маковій і Г. О. Усата також розглядають інформаційно-аналітичну

підтримку поліції через поєднання організаційно-правових і технічних засобів забезпечення інформаційної безпеки [47, с. 65]. Звідси випливає, що електронна готовність не може зводитися до технічної модернізації без належної організації роботи користувачів, адміністраторів, керівників і підрозділів контролю.

Технічна складова електронної готовності охоплює наявність інформаційно-комунікаційної інфраструктури, захищених каналів зв'язку, засобів електронної ідентифікації, систем авторизації, журнал дій користувачів, резервного копіювання, відновлення доступу, криптографічного й технічного захисту інформації. Положення про єдину інформаційну систему Міністерства внутрішніх справ визначає її як багатофункціональну інтегровану автоматизовану систему, що забезпечує реалізацію функцій суб'єктів, інформаційну підтримку їх діяльності, обробку, захист інформації та внутрішню і зовнішню інформаційну взаємодію [75]. У цьому положенні важливим є не лише факт існування ЄІС МВС, а й нормативне закріплення її як середовища, у якому поєднуються функціональні підсистеми, програмно-інформаційні комплекси, технічні засоби телекомунікацій і правила доступу.

ЄІС МВС доцільно розглядати як одну з ключових організаційно-технічних основ електронної готовності у правоохоронній сфері. Положення про таку систему визначає її як багатофункціональну інтегровану автоматизовану систему, що забезпечує реалізацію функцій суб'єктів, інформаційну підтримку їх діяльності, оброблення, захист інформації та внутрішню і зовнішню інформаційну взаємодію [75]. Така характеристика має не лише технічне, а й теоретико-правове значення. Вона свідчить про поступовий перехід від окремих відомчих баз до інтегрованого інформаційного середовища, у якому дані мають обслуговувати не один підрозділ, а взаємопов'язані правоохоронні, адміністративні, безпекові та сервісні функції.

Важливим є те, що у межах ЄІС МВС функціонують різні за правовим режимом і призначенням інформаційні ресурси. Одні забезпечують оперативний пошук і реагування, інші пов'язані з адміністративною практикою, дозвільними процедурами, реєстраційними діями, управлінням силами та засобами,

прикордонним контролем, міграційними процесами або захистом інформації. Унаслідок цього технічна сумісність не може означати однаковий доступ для всіх користувачів. Навпаки, інтегрована система потребує більш чіткого розмежування прав доступу, оскільки об'єднання різних ресурсів підвищує ризик використання інформації поза первинною метою. Належна електронна готовність передбачає, що користувач бачить лише ті відомості, які потрібні для виконання конкретного завдання, а система фіксує підставу, час, користувача, обсяг доступу і подальшу операцію.

Технічна складова повинна також охоплювати шляхи відновлення. В умовах воєнного стану правоохоронні органи можуть працювати в умовах пошкодження мереж, тимчасового переміщення підрозділів, загрози фізичного захоплення обладнання, масованих кібератак або потреби швидкого відновлення доступу до критичних ресурсів. Тому технічний механізм не вичерпується наявністю серверів і програмного забезпечення, а включає резервування даних, розподілення доступу, захищені канали, контроль адміністраторів, журнали технічних подій, плани відновлення роботи та процедури збереження цілісності інформації. Без таких елементів електронна система може формально існувати, але не забезпечувати реальної правоохоронної спроможності.

Практичним проявом електронної готовності у діяльності Національної поліції України є функціонування інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України». Відповідне положення визначає завдання, призначення, суб'єктів і структуру цієї системи, а також умови її функціонування [76]. Значення ІПНП полягає у формуванні інформаційних ресурсів ЄІС МВС, обробленні відомостей, що утворюються у процесі діяльності поліції, наданні оперативного доступу до інформаційних ресурсів, забезпеченні пошукових і аналітичних функцій, електронного документообігу, геоінформаційних можливостей, автоматизації управління силами і засобами, комплексного захисту інформації та розмежування доступу [76]. У межах такого підходу електронна готовність поліції виявляється не в наявності окремого порталу, а в здатності забезпечити правомірний рух

інформації від первинної події до управлінського, оперативно-службового або процесуального рішення.

Інформаційний портал Національної поліції України має значення не лише як відомча система доступу до даних, а як середовище щоденної правоохоронної роботи. Положення про ІПНП визначає його завдання, призначення, суб'єктів та структуру, а також передбачає оброблення інформації, що утворюється у процесі діяльності поліції, надання доступу до інформаційних ресурсів, забезпечення пошукових і аналітичних функцій, автоматизацію окремих процесів та захист інформації [76]. З огляду на це портал слід розглядати як практичний прояв переходу від паперово-відомчої логіки обліку до цифрового середовища, у якому повідомлення, перевірка, реагування, розшук, адміністративне провадження, оперативна інформація та управління силами можуть бути пов'язані між собою.

Разом із тим ІПНП ставить перед інформаційним забезпеченням низку складних питань. По-перше, необхідно визначити межі використання відомостей, які надходять до порталу з різних джерел і мають неоднаковий ступінь перевіреності. По-друге, слід розмежувати доступ користувачів залежно від посадових обов'язків, територіальної належності, виду завдання і правового режиму інформації. По-третє, важливо забезпечити технічну фіксацію кожного звернення до даних, оскільки саме журнал доступу дає змогу встановити службову необхідність, виявити зловживання або підтвердити правомірність використання інформації. По-четверте, потрібна процедура виправлення помилок, адже некоректний запис у поліцейському ресурсі може вплинути на перевірку особи, розшук, адміністративне рішення або хід кримінального провадження.

У структурі ІПНП особливе місце займають спеціалізовані інформаційні підсистеми. Інформаційна підсистема «Єдиний облік» [69] забезпечує формування та ведення відомостей про заяви і повідомлення, інформаційна підсистема «СЛІД» спрямована на облік слідової інформації [70], «Custody Records» пов'язана з фіксацією дій щодо затриманих осіб [71], а «Електронна розшукова справа» забезпечує цифрове ведення розшукової інформації [77].

Кожна з цих підсистем має власне функціональне призначення, проте всі вони підтверджують загальну закономірність: сучасне правоохоронне інформаційне забезпечення рухається від обліку факту до документування процесу роботи з ним. Для наукового дослідження важливо, що такий процес повинен бути не лише швидким, а й правомірним, контрольованим та придатним для подальшої перевірки.

Важливе значення має також автоматизована інформаційна система оперативного призначення ЄІС МВС, яка призначена для накопичення й оброблення відомостей, що утворюються у процесі оперативно-розшукової діяльності Національної поліції України [73]. Основним її завданнями є підвищення якості інформаційно-аналітичного забезпечення оперативно-розшукової діяльності, підтримка прийняття управлінських рішень, об’єднання даних в єдиному інформаційному середовищі та протидія злочинності [73]. На відміну від загальних адміністративних реєстрів, така система працює з інформацією, що може мати обмежений доступ, оперативне значення, підвищені вимоги до конфіденційності та необхідність суворого контролю за кожним зверненням до даних.

Електронна готовність органів правопорядку безпосередньо пов’язана з електронізацією кримінального провадження. Єдиний реєстр досудових розслідувань забезпечує реєстрацію кримінальних правопорушень, облік кримінальних проваджень, фіксацію основних процесуальних рішень та інформаційний зв’язок між початком досудового розслідування і подальшими процесуальними діями [74]. Інформаційно-телекомунікаційна система досудового розслідування «іКейс», запроваджена для антикорупційної інфраструктури, засвідчує перехід від електронного обліку до електронного середовища процесуальної взаємодії, у якому документи, дії, погодження та обмін із судовою системою можуть фіксуватися в цифровій формі [85]. Наукові дослідження останніх років пов’язують розвиток ЄРДР та «іКейс» із потребою забезпечити швидкість кримінального провадження, повноту фіксації даних, збереження процесуальної інформації та контроль за доступом [110].

Електронізація кримінального провадження має подвійне значення для інформаційного забезпечення. З одного боку, вона підвищує швидкість реєстрації, пошуку, передачі та використання процесуальної інформації. З іншого – посилює вимоги до точності, повноти, автентичності та захищеності кожної інформаційної дії. ЄРДР фіксує початок досудового розслідування, рух кримінального провадження, процесуальні рішення та інші дані, що мають значення для реалізації прав учасників кримінального провадження [74]. Неповне або несвоєчасне внесення відомостей до ЄРДР може вплинути на можливість ефективного розслідування, процесуальний статус особи, строки провадження та судовий контроль. Тому ЄРДР слід розглядати як один із базових інструментів процесуальної визначеності.

ІТС «іКейс» забезпечує не лише збереження процесуальних документів, а й організацію електронної взаємодії між суб'єктами антикорупційного кримінального провадження [85]. Її значення полягає у можливості фіксувати підготовку, погодження, направлення та використання процесуальної інформації в цифровій формі. Для правоохоронної діяльності такий підхід є перспективним, проте його поширення потребує вирішення трьох питань. Перше питання стосується процесуальної форми електронного документа та доказового значення електронних дій. Друге питання пов'язане з електронною ідентифікацією, правами доступу та захистом від несанкціонованого втручання. Третє питання полягає у забезпеченні сумісності між ЄРДР, системами досудового розслідування, судовими інформаційними ресурсами та відомчими базами правоохоронних органів.

На думку О. М. Дуфенюк, використання цифрових технологій у кримінальному провадженні створює нові виклики, пов'язані з електронними доказами, технічними помилками, збереженням даних, правами учасників і належною процесуальною формою [24]. Погоджуючись із таким підходом, слід підкреслити, що електронна готовність у кримінальному провадженні не може оцінюватися лише за швидкістю обміну документами. Вирішальне значення має здатність підтвердити, хто створив документ, коли і на якій підставі його

підписано, чи змінювався він після створення, кому і коли був доступний, яким чином забезпечено збереження та чи може суд перевірити його походження. Саме такі критерії перетворюють цифровий документ на правомірний елемент інформаційного забезпечення правоохоронної діяльності.

Кадрова складова електронної готовності охоплює здатність працівників правоохоронних органів працювати з інформаційними системами, розуміти правові режими інформації, правильно оцінювати результати автоматизованої обробки, використовувати інструменти кримінального аналізу, забезпечувати конфіденційність і не допускати неправомірного поширення відомостей. І. А. Федчак наголошує, що результативність аналітичної роботи залежить не лише від джерел інформації, а й від методики її перевірки, структурування та представлення у формі, придатній для прийняття рішень [121, с. 25]. Звідси випливає, що електронна готовність правоохоронного органу є неможливою без спеціальної підготовки користувачів, аналітиків, керівників і працівників, відповідальних за захист інформації.

Аналітична складова електронної готовності полягає у здатності правоохоронних органів не лише отримувати доступ до інформації, а й зіставляти, оцінювати, перевіряти та інтерпретувати її. Основи кримінального аналізу, розроблені у вітчизняній правоохоронній науці, передбачають роботу з подіями, особами, зв’язками, маршрутами, телефонними з’єднаннями, фінансовими операціями, часовими рядами та іншими даними, які можуть мати значення для виявлення закономірностей злочинної діяльності [57, с. 35]. Однак аналітичний результат не може замінити правоохоронне рішення й виконує допоміжну функцію, а його використання повинно супроводжуватися зазначенням джерел, методу аналізу, ступеня перевіреності й меж допустимого застосування.

Безпекова складова електронної готовності набула особливого значення після початку повномасштабної збройної агресії проти України. Стратегія кібербезпеки України визначає кібербезпеку як одну з умов захисту національних інтересів [92], а Закон України «Про основні засади забезпечення

кібербезпеки України» закріплює організаційні й правові основи захисту життєво важливих інтересів людини, суспільства і держави в кіберпросторі [96]. Електронна готовність має включати не лише можливість цифрового доступу, а й стійкість інформаційних систем до кібератак, несанкціонованого втручання, втрати даних, підміни записів, витоку інформації та блокування критичних сервісів.

Кіберстійкість правоохоронних інформаційних ресурсів у сучасних умовах має розглядатися як невід'ємна складова публічної безпеки. Інформаційна система, що містить відомості про кримінальні провадження, розшук осіб, зброю, транспортні засоби, оперативно значущі дані або персональні дані працівників і громадян, може бути об'єктом кібератак, спрямованих на викрадення, знищення, підміну або блокування інформації. Наслідком такого втручання може стати не лише витік конфіденційних відомостей, а й ускладнення розслідування, розшуку, помилкова ідентифікація, дезорганізація реагування або створення умов для уникнення відповідальності. Тому захист інформаційних ресурсів правоохоронних органів повинен розглядатися як складова належного виконання правоохоронних завдань.

Адміністративно-правовий механізм забезпечення інформаційної безпеки в Національній поліції України, як обґрунтовує Д. В. Федотов, має поєднувати нормативне регулювання, компетенцію суб'єктів, організаційні процедури, технічний захист, контроль і відповідальність [119, с. 44]. Тому безпекову складову електронної готовності не можна зводити лише до технічного захисту мережі, позаяк вона охоплює порядок допуску користувачів, навчання персоналу, оцінювання ризиків, реагування на інциденти, перевірку дій адміністраторів, документування порушень, відновлення даних і правові наслідки неправомірного доступу. Наявність захищеної системи не має значення, якщо працівник передає пароль, використовує дані поза службовою потребою або не фіксує підставу запиту.

В умовах воєнного стану безпекова складова набуває додаткового значення. Правоохоронні інформаційні ресурси можуть використовуватися для

документування воєнних злочинів, встановлення кола потерпілих, перевірки колаборaційних ризиків, розшуку осіб, протидії незаконному обігу зброї, виявлення диверсійних груп і захисту критичної інфраструктури. Водночас такі ресурси містять дані, витік яких може поставити під загрозу потерпілих, свідків, працівників правоохоронних органів, військовослужбовців або осіб, які перебувають на тимчасово окупованих територіях. Тому електронна готовність у воєнних умовах має включати не лише доступність інформації для уповноваженого користувача, а й здатність забезпечити її обмеження, шифрування, резервування, контроль поширення та швидке припинення неправомірного доступу.

Умови воєнного стану змінюють практичний зміст електронної готовності. Правоохоронні органи одночасно виконують традиційні завдання протидії злочинності та нові або істотно посилені завдання, пов’язані з документуванням воєнних злочинів, розшуком зниклих безвісти, ідентифікацією загиблих, перевіркою осіб на блокпостах, протидією диверсійній діяльності, кіберзагрозам, колаборaційним проявам, незаконному обігу зброї, торгівлі людьми та інформаційним операціям держави-агресора. За таких умов електронна готовність повинна оцінюватися здатністю органів правопорядку швидко отримувати необхідну інформацію, перевіряти її походження, забезпечувати сумісність даних між органами, зберігати доказову придатність відомостей і не допустити їх неправомірного використання.

Комплексний стратегічний план реформування органів правопорядку на 2023-2027 роки безпосередньо пов’язує модернізацію органів правопорядку з цифровою трансформацією. Серед визначених у ньому напрямів виокремлено впровадження електронної системи управління кримінальними провадженнями, забезпечення сумісності ІТ-систем, підвищення доступності й повноти інформації, захист персональних даних відповідно до стандартів ЄС, безпечні системи зв’язку, уніфіковану систему особистої автентифікації, біометричне зіставлення, використання ШІ, хмарних обчислень та інших інноваційних рішень [87]. Отже, державна політика фактично визнає електронну готовність органів

правопорядку одним із критеріїв їх інституційної спроможності.

Зміст Комплексного стратегічного плану дає підстави розглядати цифрову трансформацію як засіб підвищення якості правоохоронної діяльності [87]. У такому нормативно-правову акті йдеться про електронну систему управління кримінальним провадженням, електронний документообіг, захищені канали обміну інформацією, інформаційно-аналітичну підтримку, систему особистої автентифікації, біометричні системи, використання ШІ та інші інноваційні рішення. Для наукового аналізу важливо, що кожен із цих напрямів повинен оцінюватися через його зв'язок із конкретною правоохоронною функцією: запобіганням правопорушенням, оперативним реагуванням, розшуком, документуванням, досудовим розслідуванням, координацією сил або міжнародним співробітництвом.

На нашу думку, реалізація цифрової трансформації органів правопорядку потребує системи показників, до яких слід віднести: частку інформаційних операцій, що мають зафіксовану правову підставу; час оброблення міжвідомчого запиту; кількість дублювань одного запису в різних ресурсах; частоту перегляду актуальності даних; наявність уніфікованих класифікаторів; частку користувачів, які пройшли спеціальну підготовку; кількість виявлених неправомірних доступів; можливість відтворення інформаційного шляху від первинного повідомлення до рішення. Саме такі критерії дозволяють оцінити реальну придатність інформаційних ресурсів для правоохоронної діяльності.

Окремого значення набуває питання взаємозв'язку цифровізації та довіри до правоохоронних органів. Інформаційна система, яка працює швидко, але не дозволяє перевірити походження даних або відповідального користувача, може породжувати сумніви в законності прийнятого рішення. Натомість система, у якій фіксуються правова підстава, мета доступу, користувач, джерело відомостей, операція, термін використання, створює основу для внутрішнього контролю, судової перевірки й захисту прав особи. Тому електронна готовність правоохоронних органів має оцінюватися не за принципом «чим більше даних, тим краще», а за здатністю забезпечити правомірне, достовірне, захищене й

контрольоване використання інформації.

Водночас електронна готовність в Україні залишається нерівномірною. Одні підрозділи вже активно використовують інформаційні системи, кримінальний аналіз, відеоаналітику, геоінформаційні інструменти, електронний документообіг і захищені канали зв'язку, тоді як інші стикаються з технічною застарілістю, нестачею фахівців, неоднаковим рівнем цифрової підготовки, фрагментарністю реєстрів, дублюванням інформації та складністю міжвідомчого доступу. Як зазначає С. В. Пеньков, інформаційно-аналітичне забезпечення діяльності Національної поліції потребує належної організації, правового врегулювання та узгодження діяльності відповідних підрозділів [58, с. 68]. Вказане положення є актуальним не лише для поліції, а й для всієї системи правоохоронних органів.

Суттєвою проблемою залишається відомча роз'єднаність інформаційних ресурсів. Формальне існування електронних баз даних не гарантує ефективної правоохоронної діяльності, якщо відомості дублюються, оновлюються несинхронно, мають різні класифікатори, неоднакові правила доступу й не супроводжуються достатніми даними про джерело походження та ступінь перевіреності. У таких випадках працівник може мати технічний доступ до інформації, але не мати впевненості в її актуальності, допустимості використання або зв'язку з конкретним правоохоронним завданням. Саме тому електронна готовність повинна передбачати не лише комп'ютеризацію, а й міжсистемну сумісність, стандарти якості даних і простежуваність кожної інформаційної операції.

На нашу думку, *електронну готовність правоохоронних органів України доцільно оцінювати за такими критеріями: наявність чітких правових підстав для оброблення інформації; сумісність інформаційних систем і класифікаторів; захищеність каналів обміну; ідентифікація та авторизація користувачів; фіксація кожної дії з інформацією; регулярне підтвердження актуальності даних; кадрова здатність працювати з цифровими інструментами; методична готовність до кримінального аналізу; можливість незалежного контролю;*

забезпечення прав особи у разі помилки, неправомірного доступу або необґрунтованого використання відомостей. Такий перелік відображає правоохоронну специфіку електронної готовності й дає змогу відмежувати її від загального рівня цифровізації публічної адміністрації. За результатами опитування, 60,3 % респондентів оцінили електронну готовність правоохоронних органів України як часткову й нерівномірну, а 21,1 % – як недостатню, що підтверджує потребу оцінювати її не за кількістю інформаційних систем, а за здатністю забезпечити законний, захищений і перевірюваний рух відомостей (додаток Б).

Зазначені критерії мають не лише теоретичний, а й прикладний характер. Правова визначеність дає змогу встановити, чи мав орган право створювати ресурс, отримувати відомості, передавати їх іншому суб'єкту або використовувати в конкретному провадженні. Міжсистемна сумісність забезпечує можливість обміну даними без втрати змісту, спотворення категорій або дублювання записів. Захищеність гарантує збереження конфіденційності, цілісності та доступності інформації. Кадрова спроможність відображає реальну здатність працівника працювати з інформаційними системами без порушення законодавства. Актуальність даних дозволяє уникнути прийняття рішень на підставі застарілих або скасованих відомостей. Аналітична придатність характеризує можливість зіставлення даних, встановлення зв'язків і формування обґрунтованого висновку. Підконтрольність доступу забезпечує можливість перевірити кожну дію користувача.

У практиці правоохоронної діяльності такі критерії мають застосовуватися разом. Наприклад, інформація про розшук особи може бути формально внесена до відповідного ресурсу, однак її використання буде проблемним, якщо не зрозуміло, хто є органом-джерелом, коли останній раз перевірялася актуальність запису, чи не скасовано розшук, хто саме звертався до даних і з якою метою. Дані про зброю можуть бути технічно доступними, проте їх значення для правоохоронного рішення залежить від правильності ідентифікаційних ознак, актуальності дозволу, зв'язку із власником, історії переміщення та правових

підстав обмеження доступу. Відомості з відкритих джерел можуть бути корисними для аналітики, але без фіксації походження, часу отримання і способу перевірки вони не повинні сприйматися як встановлений факт.

Узагальнюючи, електронна готовність правоохоронних органів України є постійним процесом приведення нормативних, організаційних, технічних, кадрових, аналітичних і безпекових можливостей у відповідність до реальних правоохоронних завдань. У мирний час її значення полягає у підвищенні результативності протидії злочинності та захисті прав людини. В умовах воєнного стану така додатково забезпечує стійкість правоохоронної системи, безперервність документування правопорушень, збереження цифрових слідів, взаємодію з органами сектору безпеки і оборони та можливість міжнародного використання зібраної інформації.

Отже, електронна готовність впровадження сучасних практик інформаційного забезпечення правоохоронної діяльності в Україні є складною організаційно-правовою характеристикою, яка охоплює не лише технічне оснащення, а й нормативну визначеність, якість інформаційних ресурсів, кадрову підготовку, аналітичну спроможність, кіберстійкість, міжвідомчу сумісність і підконтрольність роботи з даними. У сучасних умовах її належний рівень має забезпечувати швидке отримання інформації, перевірку її достовірності, захист від неправомірного доступу, використання у межах повноважень і збереження доказової або аналітичної цінності відомостей для виконання правоохоронних завдань.

Окремо слід підкреслити, що електронна готовність правоохоронних органів не може бути однаковою для всіх напрямів діяльності. Для патрульної поліції визначальними є швидкість доступу до даних, мобільність, зв’язок із черговими службами, можливість перевірки особи, транспортного засобу, документів і обставин події. Для слідчих підрозділів важливими є ЄРДР, електронний документообіг, збереження цифрових матеріалів, доступ до реєстрів, фіксація процесуальної інформації та можливість перевірити походження кожного документа. Для оперативних підрозділів ключове значення

мають оперативні обліки, аналітичні інструменти, конфіденційність, обмеження доступу та захищені канали. Для аналітичних підрозділів вирішальними є якість даних, сумісність класифікаторів, методика зіставлення і здатність формувати висновки з позначенням рівня достовірності. Тому електронна готовність має оцінюватися не загально, а з урахуванням функціонального призначення конкретного правоохоронного органу або підрозділу.

Для повнішої характеристики електронної готовності доцільно виокремити її внутрішні показники. Першим показником є нормативна завершеність, що виявляється у наявності зрозумілих правил створення, ведення, доступу, обміну, зберігання, виправлення та припинення активного використання даних. Другим показником є організаційна керованість, тобто здатність органу визначити відповідальних осіб, строки, маршрути руху інформації, порядок реагування на помилку і механізм контролю. Третім показником є якість даних, що охоплює достовірність, повноту, актуальність, правильність класифікації, наявність джерела та позначення ступеня перевіреності. Четвертим показником є технічна надійність, яка передбачає безперервність роботи, захищені канали, резервування, електронну ідентифікацію і відновлення доступу. П’ятим показником є професійна готовність користувачів. Шостим показником є підконтрольність, тобто можливість перевірити кожну інформаційну операцію.

У правоохоронній діяльності такі показники мають застосовуватися через конкретні службові ситуації. Під час реагування на повідомлення про правопорушення працівник повинен швидко отримати інформацію, але водночас система має зафіксувати підставу звернення, користувача і результат пошуку. Під час розшуку особи важлива не лише наявність запису, а й підтвердження його актуальності, відсутність скасування розшуку, правильність ідентифікаційних ознак і можливість взаємодії з іншими органами. Під час документування воєнного злочину необхідно зберегти цифрові матеріали, встановити їх походження, не допустити втрати метаданих, забезпечити зв’язок із ЄРДР і можливість подальшого використання у кримінальному провадженні.

Під час аналізу відкритих джерел потрібно відокремити неперевірене повідомлення від підтвердженого факту.

Складність електронної готовності полягає також у тому, що правоохоронний орган працює не лише з власними ресурсами. Для виконання завдань суб'єкт правоохоронної діяльності може потребувати інформації з державних реєстрів, ресурсів інших правоохоронних органів, судових, міграційних, прикордонних, податкових, митних, демографічних, транспортних, дозвільних та інших інформаційних систем. Отже, електронна готовність залежить не лише від внутрішнього стану конкретного органу, а й від загальної здатності державних інформаційних ресурсів взаємодіяти без втрати правового режиму даних. Якщо орган одержує відомості з іншого ресурсу, він повинен розуміти їх походження, актуальність, допустимість використання та обмеження подальшого поширення. Саме тому електронна готовність має міжвідомчий характер і потребує узгодженого регулювання.

Таким чином, електронну готовність доцільно оцінювати як постійний стан організаційно-правової готовності до правомірного використання інформації. Такий стан має підтримуватися через регулярне оновлення нормативних актів, аудит інформаційних ресурсів, навчання користувачів, перевірку журналів доступу, оцінювання кіберризиків, тестування резервних процедур, перегляд строків зберігання і виправлення помилок. Без постійного підтримання цих елементів будь-яка електронна система поступово втрачає придатність для належного інформаційного забезпечення правоохоронної діяльності.

Важливо також ураховувати територіальну нерівномірність цифрової спроможності. Підрозділи, які працюють у прифронтових областях, на деокупованих територіях або в умовах постійних обстрілів, мають інші організаційні й технічні потреби, ніж підрозділи в тилових регіонах. Для них особливо важливими є автономність доступу, резервні канали зв'язку, мобільні засоби фіксації, захищене передавання матеріалів, швидке відновлення доступу, збереження цифрових доказів і можливість взаємодії з військовими

адміністраціями, підрозділами сектору безпеки і оборони, органами місцевого самоврядування та міжнародними організаціями. У таких умовах електронна готовність повинна забезпечувати не лише технологічний комфорт, а й безперервність правоохоронної діяльності.

Науково обґрунтованим є висновок, що електронна готовність має бути пов’язана з плануванням ресурсів. Закупівля програмного забезпечення або створення нового реєстру без підготовки персоналу, регламентів доступу, правил перевірки даних, технічного захисту і контролю використання не розв’язує проблему інформаційного забезпечення. Водночас надмірна кількість окремих систем може ускладнювати роботу працівника, якщо вони не мають єдиних правил ідентифікації, авторизації, пошуку, класифікації та обміну. Тому розвиток електронної готовності потребує пріоритетності: спочатку мають бути визначені правоохоронні завдання, інформаційні потреби, правові підстави й ризики, а вже після цього - технічний інструмент, який забезпечує виконання відповідної функції.

2.2. Інструменти інформаційного забезпечення правоохоронної діяльності в Україні

Інструменти інформаційного забезпечення правоохоронної діяльності в Україні є сукупністю правових, організаційних, інформаційних, аналітичних, технічних, безпекових і кадрових засобів, за допомогою яких уповноважені суб’єкти визначають інформаційні потреби, отримують, перевіряють, систематизують, зберігають, аналізують, передають, використовують і захищають відомості, необхідні для виконання правоохоронних завдань. У межах цього підрозділу реєстри, бази даних, ШІ, OSINT, відеоаналітика, інформаційні підсистеми МВС і Національної поліції розглядаються не як ізольовані технічні засоби, а як елементи загальної системи інформаційного забезпечення.

Поняття «інструмент» у цьому контексті доцільно тлумачити через функціональне призначення у правоохоронній діяльності. Інструментом інформаційного забезпечення є не кожна програма, база даних або технічний пристрій, а лише той засіб, який має правову підставу застосування, визначене функціональне призначення, коло користувачів, режим доступу, порядок фіксації операцій і здатність забезпечити отримання інформаційного результату, придатного для правоохоронної мети. За відсутності цих ознак технічний засіб може залишатися корисним допоміжним ресурсом, але не набуває повноцінного значення інструменту інформаційного забезпечення правоохоронної діяльності.

На нашу думку, *інструменти інформаційного забезпечення правоохоронної діяльності доцільно систематизувати за такими групами: нормативно-правові, організаційні, інформаційно-ресурсні, інформаційно-аналітичні, техніко-технологічні, безпекові та кадрово-методичні*. Нормативно-правові інструменти визначають підстави, межі, процедури й відповідальність за роботу з інформацією. Організаційні інструменти забезпечують розподіл компетенції, порядок взаємодії, маршрутизацію запитів і контроль виконання. Інформаційно-ресурсні інструменти охоплюють реєстри, банки, бази даних, обліки, електронні документи й архіви. Інформаційно-аналітичні інструменти забезпечують перетворення даних на аналітичний результат. Техніко-технологічні інструменти охоплюють програмне забезпечення, мережі, засоби ідентифікації, геоінформаційні системи, відеоаналітику, системи розпізнавання та автоматизованої обробки. Безпекові інструменти спрямовані на захист інформації та інформаційних систем. Кадрово-методичні інструменти забезпечують професійну здатність працівників правильно застосовувати відповідні засоби. У той же час, найбільш значущими інструментами інформаційного забезпечення респонденти вважають електронні реєстри, бази даних та обліки – 35,4 %, інформаційно-аналітичні засоби й кримінальний аналіз – 30,4 %, захищені канали міжвідомчого обміну – 20,6 %, а також кадрово-методичну підготовку користувачів – 13,6 % (додаток Б).

Запропонована система дозволяє уникнути поширеної помилки, коли

інструментами інформаційного забезпечення визнаються лише технічні засоби або електронні бази даних. Для правоохоронної діяльності інструмент має цінність лише тоді, коли забезпечує правомірний інформаційний результат. Нормативно-правовий акт без організаційної процедури може залишитися декларацією. Реєстр без актуальних даних створює ризик помилкового рішення. Аналітична система без перевірки джерел може відтворювати первинну помилку. Захищений канал без службової необхідності доступу може стати засобом необґрунтованого поширення відомостей. Кадрова підготовка без методичних правил не забезпечує однакової практики. Тому всі групи інструментів повинні діяти не ізольовано, а як елементи повного циклу роботи з відомостями.

Теоретико-правове значення такої класифікації полягає також у можливості визначити відповідальність за кожний етап інформаційної роботи. Нормативно-правові інструменти визначають правову підставу і межі повноважень. Організаційні інструменти забезпечують розподіл функцій між органами та підрозділами. Інформаційно-ресурсні інструменти накопичують і структурують дані. Інформаційно-аналітичні інструменти формують нове знання. Техніко-технологічні інструменти забезпечують оброблення, передачу, пошук і зіставлення. Безпекові інструменти охороняють інформацію та інформаційні системи. Кадрово-методичні інструменти забезпечують правильне застосування всіх попередніх засобів. Відсутність одного з цих елементів порушує цілісність інформаційного забезпечення.

Практичне значення запропонованої систематизації особливо помітне під час воєнного стану. Документування воєнного злочину потребує правової підстави внесення відомостей, організації роботи слідчих, прокурорів, оперативних працівників, експертів і аналітиків, використання ЄРДР, цифрових матеріалів, фото- і відеофіксації, відкритих джерел, геоінформаційних даних, захищених каналів передачі та спеціальної підготовки працівників. Якщо хоча б один із цих елементів не працює належно, зібрана інформація може втратити доказову або аналітичну цінність. Отже, інструменти інформаційного

забезпечення мають оцінюватися не за технологічною складністю, а за здатністю забезпечити повний, законний і контрольований рух відомостей до правоохоронного рішення.

Нормативно-правові інструменти становлять вихідну основу всіх інших засобів інформаційного забезпечення правоохоронної діяльності, оскільки саме вони визначають межі допустимого одержання, оброблення, використання, передавання та захисту відомостей. Правоохоронний орган не може працювати з інформацією лише з огляду на технічну можливість отримати, накопичити або поєднати відповідні дані. Кожна інформаційна дія повинна мати належну правову підставу, відповідати визначеній правоохоронній меті, здійснюватися уповноваженим суб'єктом і залишатися підконтрольною. Такий підхід прямо простежується у ст. 25 Закону України «Про Національну поліцію», яка визначає повноваження поліції у сфері інформаційно-аналітичного забезпечення. Зокрема, відповідно до ч. 1 цієї статті поліція здійснює інформаційно-аналітичну діяльність виключно для реалізації своїх повноважень, визначених законом; частина друга передбачає формування реєстрів і баз даних, користування інформаційними ресурсами Міністерства внутрішніх справ України та інших органів державної влади, здійснення інформаційно-пошукової й інформаційно-аналітичної роботи, а також інформаційну взаємодію з органами державної влади України, органами правопорядку іноземних держав та міжнародними організаціями; частина третя встановлює обов'язкову фіксацію кожної дії щодо отримання інформації з відповідних інформаційних ресурсів у спеціальному електронному архіві [90]. Зазначені положення свідчать про перехід від загального дозволу на використання інформації до правового режиму цільового, службово обумовленого й простежуваного доступу, за якого технічна можливість отримання відомостей підпорядковується вимогам законності, обґрунтованості та подальшої перевірки.

Інформаційно-ресурсні інструменти становлять найбільшу частину інформаційного забезпечення. До них належать ЄРДР, ЄІС МВС, ІПНП, АІС ОП, інформаційні підсистеми Національної поліції, обліки розшукуваних осіб,

транспортних засобів, зброї, викрадених речей, адміністративних правопорушень, ДТП, осіб, щодо яких здійснюється профілактична робота, а також відомчі та міжвідомчі інформаційні ресурси інших правоохоронних органів. Значення таких інструментів полягає в тому, що вони забезпечують не лише накопичення відомостей, а й фіксацію подій, осіб, предметів, зв'язків, рішень і результатів правоохоронної діяльності. Водночас такі ресурси повинні мати чіткий правовий режим, інакше зібрані відомості можуть втратити доказову або аналітичну придатність.

До інформаційно-ресурсних інструментів необхідно віднести й функціональні підсистеми, які забезпечують конкретні напрями поліцейської діяльності. Інформаційна підсистема «Єдиний облік» призначена для формування та ведення відомостей про заяви і повідомлення, що надходять до поліції [69]. Її значення полягає у тому, що саме на стадії первинної реєстрації формується початковий інформаційний слід події. Помилка, неповнота або несвоєчасність такого запису може вплинути на подальшу перевірку, реагування, визначення підслідності, кваліфікацію, статистичний облік і права заявника. Тому Єдиний облік не можна розглядати як технічний журнал; він є початковою ланкою інформаційного забезпечення правоохоронної діяльності.

Інформаційна підсистема «СЛІД» має інше призначення, оскільки пов'язана з обліком слідової інформації [70] й демонструє важливість криміналістичної складової інформаційного забезпечення. Слідова інформація має цінність лише за умови збереження зв'язку між об'єктом, місцем, способом виявлення, процесуальною або організаційною дією, особою, яка її зафіксувала, та подальшим використанням. У разі втрати такого зв'язку інформація може залишатися у системі, але її доказове або пошукове значення істотно зменшується. Тому в межах цього ресурсу важливо забезпечити точність опису, стандартизовану класифікацію, фіксацію походження та можливість подальшого зіставлення з іншими масивами.

Інформаційна підсистема «Custody Records» має особливе правозахисне значення, оскільки спрямована на фіксацію дій щодо затриманих осіб [71]. Її

функціонування пов’язане не лише з внутрішнім контролем поліції, а й із гарантіями недопущення незаконного затримання, неналежного поводження, втрати інформації про фактичне перебування особи під контролем держави та порушення процесуальних прав. Інформація з цієї системи використовується не тільки для розкриття правопорушень, а й для контролю законності дій самого правоохоронного органу. Отже, інформаційне забезпечення виконує одночасно правоохоронну, управлінську й контрольну функції.

Підсистема «Електронна розшукова справа» [77] та функціональна підсистема «Єдиний реєстр зброї» [79] демонструють подальше розширення інформаційно-ресурсного інструментарію. Розшук осіб потребує актуальності даних, швидкого доступу, взаємодії з іншими органами та припинення активного використання запису після досягнення мети. Облік зброї в умовах воєнного стану набуває додаткового значення через ризики незаконного обігу, переміщення, втрати, використання у злочинній діяльності або необхідність перевірки власника. Обидва приклади підтверджують, що інформаційний ресурс повинен мати чітко визначені правила внесення, оновлення, перевірки, використання та видалення або архівування відомостей.

Національна поліція України використовує розгалужену систему інформаційних підсистем, що функціонують у межах ІПНП та ЄІС МВС. Окрім загальних обліків, у практиці застосовуються підсистеми щодо розшуку транспортних засобів, осіб, зброї, адміністративної практики, дорожньо-транспортних пригод, електронної розшукової справи, обліку кривдників, Custody Records, SOCTA та інші спеціалізовані ресурси [68; 76]. Є. В. Трофименко звертає увагу на значення інформаційно-аналітичного забезпечення Національної поліції як умови організації сучасної поліцейської діяльності [116, с. 247-248]. Такі підсистеми мають різне призначення, але їх об’єднує потреба у правовій визначеності доступу, актуальності записів, фіксації дій користувачів і відповідальності органу або підрозділу, який створює чи оновлює інформацію.

ЄРДР виконує особливу роль серед інструментів інформаційного

забезпечення, оскільки пов’язаний із початком кримінального провадження та подальшим рухом процесуальної інформації. ЄРДР – правовий інструмент фіксації відомостей про кримінальне правопорушення, процесуальні рішення, рух провадження і його зв’язок із суб’єктами кримінального процесу [74]. Саме тому достовірність, своєчасність і повнота внесення відомостей до ЄРДР мають безпосереднє значення для реалізації засад кримінального провадження, прав потерпілого, підозрюваного та інших учасників.

Інформаційно-телекомунікаційна система досудового розслідування «іКейс» демонструє інший рівень інструменталізації інформаційного забезпечення. Її значення полягає не лише у зберіганні документів, а й у забезпеченні електронного середовища досудового розслідування, погодження процесуальних документів, взаємодії між НАБУ, САП і Вищим антикорупційним судом, а також фіксації дій у цифровій формі [85]. Досвід функціонування цієї системи є важливим для ширшої цифровізації кримінального провадження, однак його поширення потребує одночасного вирішення питань процесуальної форми, електронного доказування, захисту інформації, автентифікації користувачів і збереження цілісності документів.

Інформаційно-аналітичні інструменти відрізняються від інформаційно-ресурсних тим, що їх результатом є не лише впорядкований запис, а нове знання. Кримінальний аналіз, аналітичні довідки, профілювання ризиків, аналіз телефонних з’єднань, фінансових потоків, маршрутів переміщення, зв’язків між особами та подіями забезпечують підготовку правоохоронних рішень і планування подальших дій. І. А. Федчак розглядає кримінальний аналіз як діяльність, спрямовану на виявлення зв’язків, закономірностей і тенденцій у злочинній діяльності на основі різних джерел інформації [121, с. 18]. О. Є. Користін також підкреслює значення аналітичних схем, матриць, часових ліній і зв’язків для організації роботи правоохоронних підрозділів [57, с. 74].

Кримінальний аналіз у системі інструментів інформаційного забезпечення доцільно розглядати як методично організовану діяльність із перетворення розрізнених даних на аналітичний висновок, придатний для планування й

реалізації правоохоронних заходів. Кримінальний аналіз спрямований на встановлення зв'язків, закономірностей, тенденцій та іншої інформації, яка має значення для протидії злочинності [121, с. 19]. На думку О. М. Гончарука, кримінальний аналіз у системі правоохоронних органів пов'язаний із виявленням зв'язків між подіями, особами, об'єктами і процесами, що дозволяє підвищити обґрунтованість управлінських та оперативних рішень [15]. Наведені позиції підтверджують, що аналітика є не додатком до бази даних, а окремим видом інформаційної роботи.

У правоохоронній практиці доцільно розмежовувати *оперативний*, *тактичний* і *стратегічний* кримінальний аналіз. Оперативний аналіз спрямований на підтримку конкретних дій: встановлення місцезнаходження особи, перевірку зв'язків, аналіз маршруту, телефонних з'єднань або подій, що мають значення для провадження. Тактичний аналіз забезпечує планування роботи підрозділу, розподіл сил, визначення пріоритетів реагування і виявлення серійності. Стратегічний аналіз спрямований на встановлення тенденцій злочинності, прогнозування ризиків, визначення криміногенних зон і формування управлінських рішень. Усі три рівні потребують різних джерел і методів, але мають спільну вимогу: аналітичний результат повинен містити вказівку на використані дані, спосіб їх перевірки, межі достовірності та можливі ризики помилки.

В умовах воєнного стану кримінальний аналіз виконує додаткові завдання, зокрема використовується для виявлення зв'язків між епізодами воєнних злочинів, зіставлення цифрових слідів, аналізу повідомлень з відкритих джерел, встановлення маршрутів переміщення осіб, перевірки логістичних ланцюгів незаконного обігу зброї, виявлення колабораційних ризиків і координації реагування на масові події. Р. П. Олійничук, аналізуючи аналітичну діяльність поліції в умовах воєнного стану, пов'язує її з потребою нових підходів до інформаційно-аналітичного забезпечення, прогнозування злочинності та формування стратегій протидії правопорушенням [56]. Вказане дає підстави стверджувати, що кримінальний аналіз у сучасних умовах є одним із основних

інструментів правоохоронного інформаційного забезпечення.

В умовах воєнного стану інформаційно-аналітичні інструменти набувають особливого значення, позаяк використовуються для встановлення зв’язків між епізодами воєнних злочинів, ідентифікації осіб, причетних до колабораційної діяльності, аналізу переміщення зброї, виявлення диверсійних ризиків, опрацювання повідомлень з відкритих джерел, аналізу цифрових слідів, перевірки осіб і транспортних засобів, а також координації реагування в кризових ситуаціях. Проте аналітичний висновок не повинен підміняти юридично значуще рішення. Працівник, який приймає рішення, має розуміти джерела даних, спосіб їх оброблення, ступінь перевіреності, межі використання та ризики помилки.

Серед сучасних техніко-технологічних інструментів особливе місце посідають системи відеоспостереження, автоматичної фіксації, розпізнавання номерних знаків, геоінформаційні підсистеми, засоби біометричної ідентифікації, аналітика відкритих джерел, інструменти оброблення великих масивів даних і ШІ [31, с. 190]. Р. І. Благута та А. В. Мовчан, аналізуючи новітні технології у розслідуванні злочинів, звертають увагу на їх потенціал, але водночас наголошують на потребі врахування процесуальних, організаційних і правових обмежень [10, с. 35].

ШІ у правоохоронній діяльності доцільно розглядати як інструмент автоматизованого аналізу, пошуку закономірностей, класифікації, порівняння, виявлення збігів або формування аналітичних припущень. ШІ може застосовуватися для опрацювання відео, зображень, аудіозаписів, текстів, повідомлень із відкритих джерел, геопросторових даних, фінансових операцій та інших масивів інформації. Водночас використання ШІ створює ризики помилкової ідентифікації, непрозорості алгоритму, дискримінаційного впливу, некоректного навчального набору, надмірної довіри до автоматизованого результату та незаконного втручання у приватність. Регламент Європейського Союзу 2024/1689 щодо штучного інтелекту відносить частину правоохоронних застосувань до високоризикових і пов’язує їх із вимогами якості даних,

людського нагляду, документування та управління ризиками [172].

Використання ШІ в правоохоронній діяльності потребує особливо обережного теоретико-правового підходу. Автоматизований засіб може швидко обробляти великі масиви відео, текстів, зображень, фінансових операцій, геоданих або відкритих повідомлень, однак швидкість оброблення не дорівнює правовій надійності результату. Регламент Європейського Союзу 2024/1689 встановлює підвищені вимоги до високоризикових систем ШІ, зокрема щодо якості даних, технічної документації, реєстрації подій, прозорості, людського нагляду, точності, стійкості та кібербезпеки [172]. Для України такі положення мають особливе праксеологічне значення, оскільки розвиток правоохоронних інформаційних систем уже фактично рухається до ширшого використання автоматизованого аналізу, розпізнавання, класифікації та прогнозування ризиків.

Головна небезпека автоматизованого аналізу полягає у змішуванні трьох різних категорій: фактичних даних, аналітичного припущення і правоохоронного рішення. Фактичні дані мають походження, джерело і спосіб фіксації. Аналітичне припущення є результатом оброблення цих даних за певним методом. Правоохоронне рішення приймає уповноважена службова особа в межах компетенції та з урахуванням правових підстав. Якщо автоматизований збіг або оцінка ризику сприймається як установлений факт, виникає загроза помилкової ідентифікації, дискримінаційного впливу, незаконного втручання у приватність або необґрунтованого обмеження прав людини. Тому штучний інтелект має бути лише допоміжним інструментом, а не самостійним джерелом юридично значущого висновку.

На нашу думку, використання ШІ в правоохоронних цілях повинно ґрунтуватися на обов’язкових гарантіях. По-перше, має бути визначена правова підстава і конкретна мета застосування. По-друге, повинні фіксуватися джерела даних, категорії оброблюваної інформації та обмеження щодо її використання. По-третє, необхідно забезпечити документування логіки оброблення на рівні, достатньому для подальшої перевірки. По-четверте, результат автоматизованого аналізу має оцінюватися уповноваженим працівником, який несе

відповідальність за його використання. По-п’яте, особа повинна мати реальну можливість оскаржити рішення, якщо воно було прийняте з урахуванням помилкових або неправомірно використаних даних. Без таких гарантій штучний інтелект може посилити не правоохоронну спроможність, а ризики неконтрольованого втручання.

На нашу думку, у правоохоронній діяльності ШІ не може визнаватися самостійним суб’єктом прийняття рішень. Його результат має бути лише аналітичним сигналом або допоміжною інформацією, яка підлягає перевірці уповноваженим працівником. Особливо небезпечним є використання автоматизованого збігу як встановленого факту без перевірки джерела, методики, похибки та контексту. Тому будь-яке застосування ШІ в інформаційному забезпеченні правоохоронної діяльності має супроводжуватися обов’язковим документуванням джерел даних, логіки оброблення, рівня достовірності результату, службової особи, яка його використала, та правової підстави подальшого рішення.

OSINT-інструменти, тобто збирання й аналіз інформації з відкритих джерел, мають значний потенціал для правоохоронної діяльності, особливо під час воєнного стану й можуть використовуватися для перевірки повідомлень про правопорушення, встановлення місця події, ідентифікації осіб, аналізу соціальних зв’язків, документування воєнних злочинів, виявлення дезінформаційних мереж і моніторингу криміногенних процесів. Водночас відкритість джерела не означає автоматичної правомірності будь-якого використання відомостей. Потрібно враховувати мету оброблення, достовірність джерела, спосіб фіксації, можливість перевірки, права особи, режим персональних даних і межі допустимого поширення. Саме тому OSINT має бути інтегрований у правоохоронну діяльність через методичні правила верифікації, фіксації та збереження інформації [13].

Відкриті джерела інформації в умовах воєнного стану стали одним із найдинамічніших джерел правоохоронних відомостей. Повідомлення у соціальних мережах, фото- і відеоматеріали, супутникові знімки, публічні

реєстри, медійні повідомлення, відкриті бази даних, цифрові сліди переміщень, зображення техніки або об’єктів можуть допомагати встановлювати час, місце, спосіб і учасників події. Разом із тим відкритий характер джерела не усуває вимоги правомірності. Інформація може бути неправдивою, змонтованою, вирваною з контексту, повторно опублікованою, створеною для дезінформації або такою, що містить персональні дані, використання яких потребує правової підстави. Тому робота з відкритими джерелами має підпорядковуватися не інформаційній цікавості, а конкретному правоохоронному завданню.

Методично правильне використання відомостей з відкритих джерел у правоохоронній діяльності передбачає не лише їх виявлення, а й належну фіксацію походження, змісту та умов отримання. Уповноважений працівник має зафіксувати первинне електронне посилання, час виявлення інформації, автора або власника ресурсу, технічні ознаки файлу, контекст публікації, спосіб збереження, результати перевірки автентичності та зв’язок відповідного повідомлення з іншими даними. Якщо відкрите повідомлення використовується лише для орієнтування, достатнім може бути його позначення як неперевіреної інформації, що потребує подальшого підтвердження. У разі використання таких відомостей для документування правопорушення необхідними є додаткові дії щодо збереження електронного сліду, перевірки достовірності, встановлення джерела походження та процесуального оформлення відповідно до вимог кримінального процесуального законодавства. Коли інформація стосується конкретної особи, правоохоронний орган повинен додатково враховувати режим персональних даних, межі службової необхідності, пропорційність втручання у приватне життя та ризик неправомірного поширення відомостей. Відтак відкритий характер джерела не усуває обов’язку правоохоронного органу діяти на правовій підставі, забезпечувати перевірюваність інформації та дотримуватися встановлених гарантій її подальшого використання.

У системі інструментів інформаційного забезпечення відкриті джерела мають допоміжний, перевірочний і аналітичний потенціал й дозволяють швидко виявляти події, зіставляти різні повідомлення, уточнювати місце, час, зв’язки,

маршрути, об’єкти, перевіряти офіційні дані або формувати аналітичні гіпотези. Водночас вони не повинні замінювати процесуальні джерела доказів, офіційні реєстри або результати слідчих (розшукових) дій. Науково обґрунтованим є підхід, за яким інформація з відкритих джерел може стати елементом інформаційного забезпечення лише після встановлення її походження, фіксації способу отримання, перевірки достовірності та визначення допустимих меж використання.

Безпекові інструменти інформаційного забезпечення охоплюють комплексну систему захисту інформації, розмежування доступу, електронну ідентифікацію користувачів, журнали доступу, резервування, криптографічний захист, порядок реагування на інциденти, внутрішній контроль і відповідальність за порушення режиму інформації. Адміністративно-правовий механізм забезпечення інформаційної безпеки в Національній поліції України повинен враховувати не лише внутрішній захист інформації, а й запобігання її витоку назовні, оскільки такий витік може порушити права і свободи людини [119, с. 44].

Кадрово-методичні інструменти мають не менш важливе значення, ніж технічні засоби. Навіть досконала інформаційна система не забезпечить належного результату, якщо користувач не розуміє правового режиму інформації, неправильно вводить дані, не позначає ступінь їх перевіреності, не оновлює записи, використовує інформацію поза службовою необхідністю або некритично сприймає автоматизований висновок. Тому підготовка працівників має охоплювати не лише технічні навички, а й правові засади доступу, захист персональних даних, інформаційну безпеку, кримінальний аналіз, роботу з відкритими джерелами, правила документування цифрової інформації та відповідальність за неправомірне використання відомостей.

Варто зазначити, що правоохоронні інформаційні системи використовують конкретні службові особи, які діють у межах компетенції та несуть відповідальність за наслідки інформаційних операцій. Працівник повинен розуміти різницю між перевіреним фактом, оперативним повідомленням,

аналітичним припущенням, автоматизованим збігом, статистичним показником і доказовою інформацією. Без такого розмежування навіть якісна система може використовуватися неправильно. Наприклад, результат пошуку за схожими ідентифікаційними ознаками не може автоматично підтверджувати особу; повідомлення з відкритого джерела не може без перевірки сприйматися як факт; застарілий запис у реєстрі не може бути підставою для правоохоронного реагування без перевірки актуальності.

Науково-методичне забезпечення має охоплювати стандарти введення даних, правила класифікації відомостей, порядок позначення джерела, критерії перевіреності, методики кримінального аналізу, правила роботи з відкритими джерелами, вимоги до використання штучного інтелекту, порядок фіксації інформаційних операцій і алгоритми реагування на помилку. Так, В. А. Кудінов інформаційно-аналітичне забезпечення правоохоронної діяльності розглядає через аналіз даних, державні реєстри, інформаційно-пошукові системи, відкриті джерела та кібербезпеку [45]. Такий підхід підтверджує, що підготовка працівників має поєднувати правові, організаційні, аналітичні й технічні знання.

Практична підготовка користувачів повинна бути диференційованою. Слідчий має розуміти процесуальне значення електронних відомостей, порядок їх фіксації та використання у кримінальному провадженні. Оперативний працівник повинен володіти правилами перевірки, пошуку, зіставлення й використання оперативно значущої інформації. Аналітик має вміти працювати з різними джерелами, будувати зв’язки, оцінювати ризики і формувати висновок із зазначенням рівня достовірності. Керівник повинен оцінювати інформаційний результат перед прийняттям рішення. Адміністратор системи має забезпечувати технічний доступ, захист і журналювання, не втручаючись у зміст правоохоронного рішення. Лише за такого розподілу кадрово-методичні інструменти виконуватимуть системоутворювальну функцію.

Важливою теоретичною проблемою є співвідношення інструментів інформаційного забезпечення та повноважень правоохоронних органів. Інструмент не може випереджати компетенцію суб’єкта. Наявність доступу до

реєстру, аналітичного програмного забезпечення або технічної можливості зіставити дані не означає правомірності такого використання. У правоохоронній діяльності технічна можливість повинна бути підпорядкована правовій підставі, меті, службовій необхідності, пропорційності та контролю. Інакше інструмент інформаційного забезпечення може перетворитися на джерело неправомірного втручання у права людини або на засіб неконтрольованого накопичення відомостей.

Отже, інструменти інформаційного забезпечення правоохоронної діяльності в Україні мають розглядатися як функціонально пов’язані засоби, що забезпечують повний цикл роботи з відомостями: від виникнення інформаційної потреби до правомірного використання результату. Їх систематизація дає змогу перейти від фрагментарного опису окремих баз даних і технологій до цілісного розуміння інформаційного забезпечення як механізму, у якому правове регулювання, організація, інформаційні ресурси, аналітика, технології, безпека й підготовка персоналу мають діяти узгоджено. У сучасних умовах головним критерієм ефективності таких інструментів є здатність забезпечити своєчасне, законне, обґрунтоване, захищене та перевірюване виконання правоохоронних завдань.

Якість інструментів інформаційного забезпечення залежить також від правил роботи з окремою інформаційною одиницею, зокрема повідомлення про подію, запис у реєстрі, фото, відео, біометричний шаблон, слідова інформація, аналітична позначка, електронний документ, результат пошуку, автоматизований збіг або відповідь на міжвідомчий запит. Кожна з них повинна мати мінімальний набір реквізитів: джерело, дату одержання, правову підставу, категорію даних, ступінь перевіреності, режим доступу, строк актуальності, відповідального суб’єкта та обмеження подальшого використання. Без цих реквізитів інформаційна одиниця може залишатися технічно доступною, але її використання у правоохоронній діяльності буде методологічно й правово вразливим.

Окрему групу становлять інструменти контролю якості інформації. У

правоохоронній діяльності якість даних не може зводитися до відсутності орфографічної або технічної помилки. Якісними слід визнавати такі відомості, які отримані на правовій підставі, походять із визначеного джерела, правильно класифіковані, мають позначений ступінь перевіреності, відповідають актуальному стану справи, доступні уповноваженому користувачу і можуть бути перевірені у разі використання. Якщо запис формально правильний, але не містить відомостей про джерело або дату останньої перевірки, його правоохоронна цінність обмежена. Якщо аналітичний висновок не містить методики і використаних джерел, він не повинен сприйматися як достатня основа для рішення.

У практиці правоохоронних органів контроль якості інформації має бути поєднаний із контролем допустимості її подальшого використання. Відомості можуть бути достовірними за змістом, але непридатними для певної мети через обмеження правового режиму, спеціальне походження, оперативний характер, конфіденційність джерела, обмеження міжнародного обміну або недостатність процесуального оформлення. Наприклад, інформація, отримана в межах оперативно-розшукової діяльності, може мати орієнтуюче значення, але її використання у кримінальному провадженні потребує дотримання процесуальної форми. Відомості з відкритих джерел можуть підтверджувати напрям перевірки, але без належної фіксації та верифікації не повинні замінювати доказову інформацію. Дані автоматизованого збігу можуть звужувати коло перевірки, але не можуть самостійно встановлювати винуватість особи.

У зв’язку з цим доцільно розмежовувати інформаційну, аналітичну і доказову придатність відомостей. Інформаційна придатність означає можливість використати дані для орієнтування, пошуку або первинної перевірки. Аналітична придатність передбачає можливість зіставлення відомостей з іншими масивами, встановлення зв’язків, тенденцій або ризиків. Доказова придатність вимагає дотримання процесуального порядку одержання, фіксації, збереження і подання інформації. Змішування цих рівнів створює ризик, коли орієнтуюча інформація

сприймається як доказ, аналітичне припущення - як факт, а автоматизований результат - як самостійна підстава правоохоронного рішення. Тому кожний інструмент інформаційного забезпечення має передбачати позначення функціонального статусу відомостей.

В умовах воєнного стану така диференціація набуває особливого значення. Масиви фото-, відео-, аудіо-, геолокаційних, біометричних, реєстрових та аналітичних даних можуть швидко надходити з різних джерел, зокрема від потерпілих, свідків, військових підрозділів, органів місцевого самоврядування, міжнародних партнерів, відкритих платформ і волонтерських ініціатив. Частина таких відомостей є цінною для негайного реагування, частина - для аналітичної перевірки, частина - для доказування у кримінальному провадженні. Належне інформаційне забезпечення повинно не змішувати ці масиви, а забезпечувати їх правове розмежування, маркування, перевірку і подальший рух відповідно до мети використання.

Управління якістю інформації має включати первинну перевірку, поточне оновлення, періодичний перегляд, виправлення, позначення сумнівних відомостей, обмеження використання застарілих записів і припинення активного використання даних після досягнення мети. Наприклад, завершення розшуку, закриття кримінального провадження, зміна правової кваліфікації, виправдання особи, скасування дозволу, втрата чинності документа або встановлення помилки в ідентифікації повинні ініціювати перевірку пов’язаних записів у тих інформаційних ресурсах, до яких вони були передані. Без такого зв’язку інформаційні системи можуть продовжувати відтворювати неактуальні відомості, створюючи ризик неправомірного втручання у права людини.

Інструменти контролю якості мають бути як організаційними, так і технічними. Організаційний рівень передбачає визначення підрозділу або посадової особи, відповідальної за ведення ресурсу, строки перевірки, порядок реагування на повідомлення про помилку і дисциплінарні наслідки недбалого внесення даних. Технічний рівень передбачає обов’язкові поля, автоматичні нагадування про перевірку актуальності, фіксацію змін, збереження історії

запису, блокування неповних форм, позначення неперевірених відомостей і можливість відстежити передачу даних іншим органам. Поєднання цих рівнів дозволяє забезпечити не лише накопичення, а й правову надійність інформації.

2.3. Характеристика та повноваження правоохоронних органів щодо інформаційного забезпечення правоохоронної діяльності в Україні

Характеристика повноважень правоохоронних органів щодо інформаційного забезпечення правоохоронної діяльності має принципове значення для розуміння меж правомірного використання інформації. Правоохоронні органи виступають не лише споживачами відомостей, а й їх джерелами, розпорядниками, користувачами, аналітичними обробниками, суб'єктами захисту та учасниками міжвідомчого й міжнародного інформаційного обміну. У зв'язку з цим їх інформаційні повноваження повинні аналізуватися як елементи загальної системи правоохоронної діяльності.

Для правильного розуміння повноважень необхідно виходити з того, що правоохоронний орган не є вільним користувачем усіх доступних державних даних. Його інформаційні повноваження мають похідний характер від основних завдань, визначених законом. Якщо орган уповноважений запобігати, виявляти, припиняти або розслідувати певні правопорушення, він може працювати з інформацією лише в обсязі, необхідному для виконання цих завдань. Такий підхід дозволяє відмежувати правомірний інформаційний доступ від необґрунтованого інформаційного втручання. Службова необхідність, компетенція, мета, правова підстава та фіксація запиту мають бути обов'язковими умовами використання інформаційних ресурсів.

Повноваження щодо інформаційного забезпечення слід розглядати за такими складовими:

– створення інформації: прийняття заяв, фіксації подій, реєстрації кримінальних правопорушень, ведення обліків, формування цифрових

документів, внесення даних до реєстрів;

– доступ і використання: пошук, перевірку, зіставлення, аналіз, отримання відомостей від інших органів, використання інформації під час реагування, оперативно-розшукової діяльності або досудового розслідування;

– захист і контроль: розмежуванням доступу, реєстрація дій, перевіркою правомірності, актуалізацією даних, виправленням помилок, обмеженням подальшого використання.

Сукупність таких складових утворює компетенційний зміст інформаційного забезпечення. Варто відзначити, що в умовах воєнного стану зміст інформаційних повноважень не може тлумачитися як підстава для безмежного розширення доступу до будь-яких даних. Навпаки, зростання загроз вимагає чіткішого визначення компетенції, тому що помилкове або незаконне використання інформації може завдати шкоди розслідуванню, потерпілим, свідкам, військовослужбовцям, працівникам правоохоронних органів і міжнародній співпраці. Тому повноваження мають здійснюватися за принципом необхідності: орган отримує не максимальний обсяг інформації, а саме ті відомості, які є достатніми для виконання конкретного завдання. Такий підхід поєднує оперативність правоохоронної діяльності з гарантіями прав людини та інформаційною безпекою.

В Україні функціонує розгалужена система органів, які виконують правоохоронні завдання і мають спеціальні інформаційні повноваження. До них належать Національна поліція України, СБУ, ДБР, БЕБ, НАБУ, органи прокуратури, ДПСУ, Державна митна служба України та інші суб’єкти, які в межах визначеної законом компетенції здійснюють запобігання, виявлення, припинення, документування й розслідування правопорушень або забезпечують публічну безпеку. Кожен із них має власні джерела інформації, правові підстави доступу, режими оброблення, порядок взаємодії та відповідальність за використання відомостей.

Наукове осмислення інформаційних повноважень правоохоронних органів потребує їх систематизації. На нашу думку, такі повноваження доцільно

поділяти на сім груп:

1) повноваження щодо створення і ведення інформаційних систем, реєстрів, баз даних та обліків;

2) повноваження щодо одержання інформації від фізичних, юридичних осіб, органів державної влади, органів місцевого самоврядування та міжнародних партнерів;

3) повноваження щодо доступу до інформаційних ресурсів інших суб'єктів;

4) повноваження щодо перевірки, аналізу, зіставлення та використання відомостей;

5) повноваження щодо передавання інформації в межах міжвідомчої або міжнародної взаємодії;

6) повноваження щодо захисту інформації, розмежування доступу й фіксації операцій;

7) контрольні повноваження щодо законності, актуальності, повноти та цільового використання даних.

Така класифікація дає змогу уникнути зведення інформаційного забезпечення до переліку баз даних і показує його компетенційний зміст.

Найбільш розгорнуто інформаційні повноваження врегульовані у Законі України «Про Національну поліцію» [90]. Поліція здійснює інформаційно-аналітичну діяльність виключно для реалізації своїх повноважень, формує бази даних, користується інформаційними ресурсами МВС та інших органів державної влади, здійснює інформаційний пошук, веде обліки, забезпечує захист інформації та фіксацію доступу [90]. Важливим є те, що законодавець пов'язує інформаційно-аналітичну діяльність поліції не з абстрактною потребою накопичення даних, а з реалізацією визначених законом повноважень. Отже, службова необхідність і межі компетенції є обов'язковими критеріями правомірності доступу поліцейського до інформації.

Закон України «Про Національну поліцію» визначає завдання поліції як надання поліцейських послуг у сферах забезпечення публічної безпеки і порядку,

охорони прав і свобод людини, інтересів суспільства і держави, протидії злочинності, а також допомоги особам, які з особистих, економічних, соціальних причин або внаслідок надзвичайних ситуацій потребують такої допомоги [90]. Усі ці напрями мають інформаційний вимір. Забезпечення публічної безпеки потребує даних про події, ризики, сили і засоби. Охорона прав і свобод людини потребує точної інформації про заявника, потерпілого, кривдника, затриману особу, обставини події та дії працівників поліції. Протидія злочинності неможлива без обліків, розшуку, кримінального аналізу, перевірки зв'язків і взаємодії з іншими органами. Допомога особам потребує оперативного доступу до відомостей, що дозволяють правильно оцінити ситуацію та обрати спосіб реагування.

Особливо важливою є ст. 27 Закону про використання поліцією інформаційних ресурсів [90]. Фіксація запиту дозволяє перевірити, хто, коли, з якою метою і до яких відомостей звертався. Такий механізм має запобігати неправомірному перегляду персональних даних, використанню інформації в приватних інтересах, витоку відомостей або прихованню порушень. У перспективі цей підхід доцільно поширювати на всі правоохоронні інформаційні ресурси, незалежно від їх відомчої належності.

Інформаційні повноваження Національної поліції реалізуються через ЄІС МВС, ІПНП, АІС ОП та інші інформаційні підсистеми. Поліція наповнює й підтримує в актуальному стані бази даних щодо осіб, стосовно яких здійснюється профілактична робота; виявлених кримінальних та адміністративних правопорушень; осіб, які їх вчинили; руху кримінальних проваджень; осіб, затриманих за підозрою у вчиненні правопорушень; корупційних правопорушень; іноземців та осіб без громадянства, затриманих за порушення правил перебування в Україні, та інших категорій, визначених законом [90]. У сучасних умовах такі повноваження мають оцінюватися крізь призму не лише повноти обліку, а й якості даних, актуальності записів, правового режиму доступу та можливості перевірити кожну інформаційну дію.

СБУ має інформаційні повноваження, обумовлені її завданнями у сфері

державної безпеки, контррозвідки, боротьби з тероризмом, захисту державного суверенітету, конституційного ладу й територіальної цілісності. Закон України «Про Службу безпеки України» передбачає право СБУ в інтересах контррозвідувальної та оперативно-розшукової діяльності створювати інформаційні системи і вести оперативний облік в обсязі та порядку, що визначаються її завданнями [99]. В умовах воєнного стану значення таких повноважень істотно зростає, оскільки СБУ працює з інформацією щодо диверсійної діяльності, колабораціонізму, терористичних загроз, кібероперацій, розвідувально-підривної діяльності та інших загроз національній безпеці.

ДБР є правоохоронним органом, який здійснює запобігання, виявлення, припинення, розкриття й розслідування кримінальних правопорушень, віднесених до його підслідності. Закон України «Про Державне бюро розслідувань» передбачає, зокрема, можливість створення інформаційних систем, ведення оперативного обліку, доступу як користувача до інформаційних систем органів державної влади та отримання інформації, необхідної для виконання завдань [61]. Специфіка інформаційного забезпечення ДБР полягає у поєднанні слідчої, оперативно-розшукової, аналітичної та внутрішньоконтрольної функцій, оскільки предметом діяльності ДБР часто є правопорушення, вчинені службовими особами, правоохоронцями, військовослужбовцями та іншими суб’єктами публічної влади.

БЕБ має особливе місце серед суб’єктів інформаційного забезпечення, оскільки закон прямо закріплює виконання ним правоохоронної, аналітичної, економічної, інформаційної та інших функцій. Відповідно до Закону України «Про Бюро економічної безпеки України», БЕБ здійснює інформаційно-аналітичну діяльність виключно для виконання своїх завдань [60]. Його діяльність пов’язана з аналізом економічних процесів, податкової, фінансової, митної та іншої інформації, що має значення для протидії кримінальним правопорушенням у сфері економіки. У цьому контексті БЕБ демонструє перехід від суто силового реагування до аналітичного виявлення ризиків і закономірностей, однак така діяльність потребує чітких правил доступу до

даних, перевірки їх походження та недопущення використання інформаційних інструментів для необґрунтованого тиску на бізнес.

Інформаційне забезпечення діяльності БЕБ має специфіку. Економічні кримінальні правопорушення часто виявляються не через безпосереднє повідомлення про подію, а через аналіз фінансових операцій, податкових показників, митної інформації, руху активів, господарських зв'язків, ризикових операцій, фіктивних суб'єктів, публічних закупівель або зміни економічної поведінки. Тому БЕБ за своєю природою потребує розвиненого інформаційно-аналітичного забезпечення. Закон прямо пов'язує діяльність БЕБ з аналітичною, економічною, інформаційною та правоохоронною функціями [60]. Вказане дозволяє говорити про переважно аналітичний характер виявлення багатьох кримінальних правопорушень у сфері економіки.

Разом із тим, наголошує О. А. Матвієць, широкий доступ до економічної інформації створює підвищені вимоги до правового режиму даних. Податкова, митна, банківська, фінансова, комерційна та інша інформація може містити відомості з обмеженим доступом, персональні дані, комерційну таємницю або інформацію, неправомірне використання якої здатне завдати шкоди суб'єкту господарювання. Тому інформаційні повноваження БЕБ мають здійснюватися за чіткими правилами службової необхідності, цільового призначення, перевірки джерела, обмеження подальшого поширення та документування аналітичного висновку. Аналітичний ризик не повинен автоматично перетворюватися на підставу для силового реагування без додаткової перевірки [50, с. 208].

На нашу думку, діяльність БЕБ показує загальну тенденцію розвитку правоохоронної системи: значна частина сучасних правопорушень виявляється не лише шляхом реагування на вже відому подію, а через аналіз інформаційних масивів. Такий підхід підвищує превентивні можливості держави, але водночас потребує сильних правових гарантій. Працівник, який використовує аналітичний продукт, повинен розуміти, з яких даних він сформований, який метод застосовано, який рівень достовірності висновку, які альтернативні пояснення можливі та чи достатньо інформації для подальшого правоохоронного рішення.

Без такого контролю аналітичний інструмент може стати джерелом необґрунтованого тиску або помилкового висновку.

НАБУ використовує інформаційні повноваження для запобігання, виявлення, припинення й розслідування корупційних та інших кримінальних правопорушень, віднесених до його підслідності. Закон України «Про Національне антикорупційне бюро України» передбачає можливість отримання необхідної інформації, доступу до державних інформаційних ресурсів у передбачених законом випадках, а також взаємодії з іншими органами [89]. Значення НАБУ в системі інформаційного забезпечення посилюється функціонуванням «іКейс», доступом до окремих реєстрів, аналітичною роботою з фінансовою, майновою, деклараційною та іншою інформацією, а також необхідністю забезпечувати процесуальну чистоту цифрових даних у кримінальному провадженні.

Органи прокуратури відіграють важливу роль у функціонуванні інформаційного забезпечення кримінального провадження, насамперед через організацію і процесуальне керівництво досудовим розслідуванням, підтримання публічного обвинувачення та ведення ЄРДР. Положення про ЄРДР визначає порядок його формування та ведення [74]. Для прокурора інформаційне забезпечення має не лише управлінське, а й процесуальне значення, оскільки від своєчасності внесення відомостей, повноти обліку, коректності процесуальних рішень і збереження даних залежить законність кримінального провадження та можливість судового контролю.

Інформаційне забезпечення діяльності прокуратури має особливий характер, оскільки прокурор не лише використовує відомості, а й забезпечує процесуальну законність їх руху у кримінальному провадженні. Ведення ЄРДР, організація досудового розслідування, процесуальне керівництво, погодження процесуальних рішень, підтримання публічного обвинувачення та представлення доказів у суді потребують повної, своєчасної, достовірної та належно оформленої інформації. Для прокурора важливо не тільки знати зміст запису або документа, а й перевірити його процесуальне походження, правову

підставу створення, належність до провадження, повноваження особи, яка його внесла, і можливість використання у суді.

ЄРДР у цьому контексті виконує роль не лише реєстру, а й інформаційної основи процесуального контролю [74]. Відомості про кримінальне правопорушення, дату внесення, кваліфікацію, рух провадження, процесуальні рішення та суб'єктів розслідування мають бути достатніми для перевірки законності досудового розслідування. Якщо дані внесено несвоєчасно, неповно або некоректно, порушується не лише статистичний облік, а й процесуальна визначеність. Саме тому інформаційна робота прокурора повинна включати контроль за своєчасністю внесення відомостей, коректністю кваліфікації, актуальністю процесуальних рішень, збереженням цифрових матеріалів і правомірністю доступу до інформації.

В умовах воєнного стану значення прокурорського інформаційного забезпечення зростає через масштабність документування воєнних злочинів, множинність епізодів, велику кількість потерпілих, свідків, цифрових матеріалів, експертиз, міжнародних запитів і потребу збереження інформації для майбутнього національного та міжнародного правосуддя. Помилки на рівні первинної реєстрації, втрати цифрових файлів, відсутність фіксації джерела або нечітке розмежування епізодів можуть ускладнити доказування. Тому прокуратура має виступати не лише користувачем інформаційних ресурсів, а й процесуальним гарантом належного інформаційного руху у кримінальному провадженні.

Державна прикордонна служба України здійснює інформаційні повноваження у сфері охорони державного кордону, прикордонного контролю, протидії незаконній міграції, переміщенню зброї, документів, транспортних засобів та осіб, які можуть становити загрозу національній безпеці. Закон України «Про Державну прикордонну службу України» передбачає створення і використання інформаційних систем та автоматизований обмін інформацією з іншими органами [62]. Окреме значення має порядок фіксації біометричних даних іноземців та осіб без громадянства під час прикордонного контролю, який

спрямований на забезпечення національної безпеки, посилення контролю за в'їздом в Україну, виїздом з України та додержанням правил перебування [81]. В умовах воєнного стану ці повноваження безпосередньо пов'язані з перевіркою осіб, контролем переміщень, розшуком, ідентифікацією та міжнародним обміном інформацією.

Інформаційні повноваження правоохоронних органів слід відрізняти від загального доступу органів публічної адміністрації до інформації. Правоохоронний доступ має підвищену інтенсивність втручання, оскільки може стосуватися персональних даних, оперативної інформації, відомостей про кримінальні провадження, розшук, фінансові операції, переміщення осіб і транспортних засобів, біометричні дані, зв'язки особи або інші дані, що можуть впливати на права і свободи людини. Тому реалізація інформаційних повноважень повинна супроводжуватися принципами законності, цільового призначення, службової необхідності, пропорційності, обмеження доступу, фіксації операцій, перевірки актуальності та відповідальності за неправомірне використання.

У сучасній системі правоохоронних органів України проблемним залишається не стільки брак інформаційних повноважень, скільки їх неоднакова деталізація та відомча фрагментарність. Для одних органів закон прямо визначає інформаційно-аналітичну діяльність, бази даних, доступ і фіксацію операцій; для інших відповідні питання розосереджені між спеціальними законами, підзаконними актами, внутрішніми положеннями та міжвідомчими угодами. Така ситуація ускладнює міжвідомчу взаємодію, створює ризики дублювання запитів, неоднакової класифікації даних, несвоєчасного оновлення записів і невизначеності щодо відповідального органу.

Відомча фрагментарність інформаційних повноважень ускладнює формування єдиного підходу до міжвідомчої взаємодії. Коли кожний орган самостійно визначає порядок доступу, формат запиту, перелік реквізитів, строки розгляду, правила передачі й обмеження подальшого використання, виникає ризик дублювання, затримки, втрати змісту або неоднакового розуміння одних і

тих самих даних. Для правоохоронної діяльності така ситуація особливо небезпечна, оскільки запит може стосуватися розшуку особи, документування злочину, реагування на загрозу, перевірки зброї, встановлення потерпілих або міжнародного співробітництва. Невизначеність відповідального органу здатна знизити оперативність і поставити під сумнів правомірність подальшого використання інформації.

На нашу думку, вирішення цієї проблеми потребує ухвалення *міжвідомчого нормативно-правового акта щодо порядку інформаційної взаємодії правоохоронних органів*. Такий нормативно-правовий акт має визначити базові поняття, суб'єктів інформаційної взаємодії, категорії інформації, правові підстави запитів, вимоги до обґрунтування службової необхідності, строки розгляду, формати даних, порядок фіксації операцій, відповідальність органу-джерела, обмеження подальшого використання, правила виправлення помилок і механізм контролю.

Також у такому акті має бути врахована й специфіка воєнного стану. Частина запитів потребує невідкладного реагування, частина стосується інформації з обмеженим доступом, частина пов'язана з міжнародною передачею відомостей або з даними потерпілих, свідків і військовослужбовців. Тому порядок взаємодії повинен передбачати звичайні та невідкладні процедури, можливість позначення обмежень щодо подальшого поширення, правила захисту чутливих категорій даних, фіксацію відповідального виконавця і періодичну перевірку актуальності переданих відомостей. У такому разі міжвідомча взаємодія буде не сукупністю ситуативних запитів, а правомірно організованим механізмом інформаційного забезпечення правоохоронної діяльності.

На нашу думку, повноваження правоохоронних органів щодо інформаційного забезпечення доцільно розвивати на основі суб'єктно-функціонального підходу. Його сутність полягає у тому, що кожний орган повинен мати чітко визначені інформаційні функції: створення даних, первинна перевірка, оновлення, доступ, аналітичне використання, передавання, захист,

контроль і припинення активного використання. При цьому орган-джерело має відповідати за достовірність, повноту й актуальність внесених ним відомостей, орган-користувач – за правомірність доступу та використання, а орган-координатор – за узгодженість міжвідомчого обміну і контроль дотримання встановлених правил.

Суб'єктно-функціональний підхід дозволяє подолати уявлення про інформаційні повноваження як про загальне право органу на доступ до даних. У межах цього підходу кожний суб'єкт має виконувати визначену інформаційну функцію і відповідати за її результат. Орган-джерело створює або первинно вносить дані, тому відповідає за правову підставу, повноту, достовірність, актуальність і правильну класифікацію запису. Орган-користувач отримує доступ до інформації, тому відповідає за службову необхідність, межі використання, недопущення поширення поза встановленою метою та фіксацію запиту. Орган-аналітик перетворює дані на висновок, тому повинен зазначити джерела, метод, рівень достовірності й обмеження результату. Орган-координатор забезпечує узгодження правил, форматів, строків і контролю.

Перевага такого підходу полягає у можливості персоніфікувати відповідальність не лише на рівні окремого працівника, а й на рівні функції органу. Якщо в інформаційному ресурсі міститься помилковий запис, необхідно встановити, хто його вніс, який орган відповідав за перевірку, чи отримував хтось доступ після втрати актуальності, кому відомості передавалися і чи були вони використані у правоохоронньому рішенні. Без такого розподілу відповідальності помилка може тривалий час відтворюватися у різних системах і впливати на права особи. Відповідальність органу-джерела, органу-користувача та органу-координатора дає змогу розірвати цей ланцюг і забезпечити належне виправлення.

Структурно-функціональний підхід, зі свого боку, дозволяє описати не лише суб'єктів, а й зміст інформаційного процесу. Створення, отримання, перевірка, реєстрація, накопичення, систематизація, зберігання, пошук, зіставлення, аналіз, передавання, використання, захист, перегляд актуальності,

виправлення, архівування та припинення активного використання мають розглядатися як послідовні, але взаємопов’язані функції. Кожна з них потребує правової підстави, відповідального суб’єкта, технічної фіксації та можливості контролю. У такому розумінні повноваження правоохоронних органів щодо інформаційного забезпечення утворюють складну систему організованого руху відомостей.

В умовах воєнного стану особливого значення набуває інформаційна взаємодія між правоохоронними органами, органами сектору безпеки і оборони, органами місцевого самоврядування, міжнародними партнерами та спеціалізованими установами. Документування воєнних злочинів, розшук безвісти зниклих осіб, ідентифікація загиблих, фіксація пошкоджень об’єктів, перевірка колаборaційних ризиків, протидія незаконному обігу зброї та забезпечення прикордонного контролю потребують швидкого, але правомірного обміну даними. У таких умовах помилка в інформаційному ресурсі може спричинити не лише управлінський недолік, а й порушення прав людини, втрату доказів, повторну віктимізацію потерпілих або ускладнення міжнародного співробітництва.

Воєнний стан вимагає від правоохоронних органів одночасного дотримання двох вимог, які на практиці можуть перебувати у напруженні: максимально швидкого реагування та збереження правової визначеності. Документування обстрілу, встановлення потерпілих, перевірка особи на блокпості, розшук зниклого, ідентифікація загиблого, фіксація незаконного обігу зброї або перевірка повідомлення про диверсійну загрозу потребують оперативного доступу до інформації. Водночас швидкість не може виправдовувати використання неперевірених, застарілих або неправомірно отриманих даних. Тому інформаційна взаємодія у воєнних умовах має бути побудована на заздалегідь визначених правилах, а не на імпровізованому обміні.

Особливого значення набуває інформація про потерпілих від воєнних злочинів, внутрішньо переміщених осіб, дітей, осіб, які перебували на тимчасово окупованих територіях, свідків, родичів зниклих безвісти, військовослужбовців

та працівників правоохоронних органів. Передання таких відомостей має здійснюватися лише з урахуванням мети, правової підстави, обсягу необхідних даних і можливих ризиків для особи. Неправомірне поширення інформації може спричинити повторну віктимізацію, загрозу безпеці, дискримінацію або ускладнення подальшого розслідування. Тому інформаційне забезпечення в умовах воєнного стану повинно поєднувати оперативність із посиленими гарантіями захисту, що означає потребу в уніфікованих формах міжвідомчих запитів, погоджених класифікаторах подій, осіб, об'єктів і ризиків, єдиних правилах позначення ступеня перевіреності відомостей, автоматизованому журналюванні доступу, визначенні органу-джерела та періодичному перегляді актуальності записів. Такі правила дозволять уникнути ситуації, коли один і той самий факт фіксується у кількох ресурсах з різними реквізитами, різною датою, різним статусом перевірки та різними обмеженнями використання. У воєнних умовах така неузгодженість може мати критичні наслідки для розслідування, розшуку, міжнародного обміну та захисту прав людини.

Отже, характеристика та повноваження правоохоронних органів щодо інформаційного забезпечення правоохоронної діяльності в Україні свідчать про поступове формування багатосуб'єктної системи роботи з інформацією, а її подальший розвиток має бути спрямований на правову визначеність компетенції, уніфікацію правил обміну, відповідальність органу-джерела, службову необхідність доступу, фіксацію кожної інформаційної операції, захист персональних даних і можливість виправлення помилок. Лише за таких умов інформаційне забезпечення правоохоронної діяльності виконуватиме свою основну функцію - створення правомірної, достовірної, актуальної та захищеної основи для виконання правоохоронних завдань.

Подальше удосконалення інформаційних повноважень має передбачати не лише уточнення компетенції окремих органів, а й формування спільних правил для всієї системи правоохоронної діяльності. До таких правил слід віднести обов'язкове зазначення органу-джерела, правової підстави внесення даних, дати останньої перевірки, ступеня достовірності, обмежень щодо використання,

відповідального користувача та підстави запиту. Водночас потрібно передбачити порядок автоматичного повідомлення органу-джерела про виявлену помилку або зміну обставин, яка впливає на актуальність запису. Без такого механізму навіть правильна інформація з часом може втратити актуальність і створити ризик помилкового правоохоронного рішення.

Важливим напрямом є уніфікація класифікаторів. Правоохоронні органи можуть по-різному позначати події, осіб, статуси, види ризиків, категорії зброї, транспортні засоби, об’єкти, джерела інформації або ступінь перевіреності відомостей. Різні класифікатори ускладнюють автоматизований пошук, статистичне узагальнення, кримінальний аналіз і міжнародний обмін. Тому міжвідомча взаємодія потребує спільних довідників і форматів даних, які не скасовують компетенцію окремих органів, але забезпечують однакове розуміння переданої інформації. У цьому полягає відмінність між правомірною інтеграцією інформаційного простору і небезпечним механічним об’єднанням усіх відомчих масивів.

Не менш важливим є закріплення процедур контролю за автоматизованим аналізом. Якщо правоохоронний орган використовує системи, які встановлюють збіги, оцінюють ризики, класифікують повідомлення або пропонують аналітичний висновок, службова особа повинна не формально підтвердити результат, а змістовно перевірити його. Така перевірка має охоплювати джерела даних, актуальність записів, спосіб оброблення, ймовірність помилки, межі допустимого використання та відповідність результату конкретному правоохоронному завданню. Лише після цього автоматизований результат може бути використаний як допоміжна основа рішення. Такий порядок дозволяє поєднати переваги сучасних технологій із принципом персональної відповідальності уповноваженої особи.

У межах характеристики повноважень слід також розмежовувати інформаційні права, інформаційні обов’язки та інформаційну відповідальність. Інформаційне право органу полягає у можливості створювати, отримувати, використовувати, передавати або захищати відомості у межах компетенції.

Інформаційний обов’язок полягає у необхідності своєчасно внести відомості, перевірити їх, оновити, обмежити доступ, захистити ресурс, надати відповідь на правомірний запит або виправити помилку. Інформаційна відповідальність означає настання юридичних чи організаційних наслідків за неправомірний доступ, внесення недостовірних даних, несвоєчасне оновлення, незаконне поширення, втрату або використання інформації поза визначеною метою. Без такого триєдиного підходу повноваження виглядають як можливість доступу, але не як обов’язок забезпечити правомірний інформаційний результат [30].

Законодавче закріплення інформаційних повноважень має враховувати також питання меж розсуду посадової особи. У правоохоронній діяльності працівник часто діє в умовах дефіциту часу, неповноти відомостей і високого рівня ризику. Проте наявність оперативної ситуації не повинна перетворювати доступ до інформації на неконтрольовану дію. Навіть у невідкладних випадках має бути визначено, яка саме інформація потрібна, з якою метою вона запитується, хто приймає рішення про доступ, як фіксується запит і яким чином перевіряється подальше використання. Такий порядок не ускладнює правоохоронну діяльність, а захищає працівника від необґрунтованих претензій і забезпечує належне документування рішення.

Суттєве значення має також співвідношення централізації та відомчої автономії. Надмірна автономія інформаційних ресурсів призводить до дублювання, несумісності, різних правил доступу і невизначеності відповідальності. Надмірна централізація може створити ризик концентрації чутливих даних, розширення доступу без службової потреби та підвищення наслідків можливого витоку. Тому оптимальним є підхід, за якого кожний орган зберігає компетенцію щодо своїх інформаційних ресурсів, але міжвідомча взаємодія здійснюється за єдиними правилами правової підстави, формату, класифікації, журналювання, відповідальності органу-джерела та контролю подальшого використання. Такий підхід забезпечує керованість без поглинання повноважень окремих органів. Практична потреба в такому регулюванні підтверджується тим, що 73,7 % опитаних підтримали ухвалення міжвідомчого

нормативно-правового акта про порядок інформаційної взаємодії правоохоронних органів, а 17,5 % визнали його доцільним після попередньої інвентаризації наявних інформаційних ресурсів (додаток Б).

Перспективним напрямом є запровадження інформаційного паспорта для ключових правоохоронних ресурсів. У такому паспорті мають зазначатися держатель, адміністратор, мета створення, категорії даних, правові підстави внесення, коло користувачів, порядок доступу, строки зберігання, правила оновлення, порядок виправлення помилок, умови передачі іншим органам і засоби контролю. Наявність таких паспортів дозволила б систематизувати відомчі ресурси, виявити дублювання, усунути прогалини у правовому режимі, забезпечити зрозумілість для користувачів і посилити відповідальність за якість даних. Для воєнного стану це має додаткове значення, оскільки дає змогу швидко визначити, який орган володіє потрібною інформацією, хто може її надати і які обмеження мають бути збережені.

На практиці саме інформаційні обов’язки часто залишаються менш деталізованими, ніж права доступу. Закон або підзаконний акт може передбачати право органу отримувати інформацію, однак не завжди визначає строк її актуалізації, обов’язок повідомити інші органи про зміну статусу, порядок позначення неперевіреного повідомлення, правила припинення активного використання або відповідального за виправлення помилки. Унаслідок цього інформація, яка була правомірно отримана на початковому етапі, з часом може стати неактуальною або непридатною для використання, але продовжувати впливати на рішення. Тому удосконалення повноважень має відбуватися через деталізацію не лише прав, а й обов’язків щодо якості, актуальності й захисту даних.

Суб’єктний склад інформаційного забезпечення також потребує чіткого розмежування. Національна поліція України, СБУ, ДБР, БЕБ, НАБУ, органи прокуратури, ДПСУ та інші суб’єкти мають різні завдання, але часто працюють із пов’язаними даними. Один орган може створити первинний запис, другий – використати його для перевірки, третій – сформувати аналітичний висновок,

четвертий – передати інформацію міжнародному партнеру, п’ятий - здійснювати процесуальний контроль. За відсутності правил розмежування відповідальності важко встановити, на якому етапі виникла помилка або порушення. Тому міжвідомчий акт має визначати не лише порядок обміну, а й функціональну відповідальність кожного учасника.

В умовах воєнного стану це питання набуває особливої ваги. Швидкість обміну відомостями про диверсійні ризики, незаконний обіг зброї, осіб, які перебувають у розшуку, потерпілих, свідків, загиблих або зниклих безвісти, не повинна супроводжуватися втратою контролю за даними. Кожний орган повинен розуміти, які відомості він має право отримати, які зобов’язаний надати, які повинен захистити, які має перевірити, а які не може використовувати без додаткового підтвердження. Лише за такого підходу інформаційні повноваження правоохоронних органів будуть спрямовані не на формальне розширення доступу, а на забезпечення законного, своєчасного й обґрунтованого виконання правоохоронних завдань.

Теоретичне значення для розділу 2 має також питання співвідношення інформаційного забезпечення і внутрішнього контролю. У правоохоронній діяльності контроль не повинен здійснюватися лише після виявлення порушення. Він має бути вбудований у саму інформаційну процедуру: під час створення запису, надання доступу, зміни відомостей, передачі іншому органу, формування аналітичного висновку та використання інформації у рішенні. Такий контроль може бути попереднім, поточним і наступним. Попередній контроль полягає у перевірці правової підстави та повноважень користувача. Поточний контроль забезпечує фіксацію дій, обмеження доступу і виявлення нетипових операцій. Наступний контроль дає змогу перевірити законність використання відомостей, виправити помилки і притягнути винних осіб до відповідальності. У сукупності ці види контролю формують гарантійний рівень інформаційного забезпечення.

Практичне значення такого підходу полягає в тому, що інформаційне забезпечення починає виконувати не лише пізнавальну, а й дисциплінуючу

функцію. Працівник, який знає, що кожна дія з даними фіксується, обґрунтовується і може бути перевірена, обережніше ставиться до службової необхідності, захисту персональних даних і меж використання інформації. Орган-джерело, відповідальний за якість запису, зацікавлений у своєчасному оновленні відомостей. Орган-користувач, який отримує інформацію з іншого ресурсу, має враховувати її правовий режим і не може розпоряджатися нею довільно. Орган-координатор, який забезпечує взаємодію, має бачити не лише факт передачі, а й дотримання встановлених правил. У цьому полягає організаційно-правова цінність інформаційного забезпечення для сучасної правоохоронної діяльності.

Підсумовуючи характеристику повноважень правоохоронних органів, слід наголосити на потребі нормативного закріплення єдиного стандарту інформаційного сліду. Такий стандарт має передбачати, що кожна дія з правоохоронною інформацією повинна залишати відомості про користувача, час, правову підставу, мету, джерело даних, обсяг доступу, результат операції та подальше передавання. Інформаційний слід є гарантією законності, оскільки дозволяє встановити, чи відповідав доступ службовій необхідності, чи не було перевищення повноважень, чи не використовувалася інформація поза правоохоронною метою, чи можна виправити або обмежити подальше використання помилкового запису. Для Національної поліції подібний підхід уже відображено у вимозі фіксації дій щодо отримання інформації з визначених інформаційних ресурсів (ст. 27 Закону України «Про Національну поліцію») [90]. На нашу думку, його доцільно поширити на ширше коло правоохоронних інформаційних систем.

Водночас інформаційний слід повинен поєднуватися з режимом захисту службової та іншої інформації з обмеженим доступом. Контроль за діями користувача не означає розкриття змісту оперативної інформації, а повинен забезпечувати можливість перевірки правомірності доступу уповноваженим суб’єктом контролю, зберігаючи при цьому таємницю джерел, методів, оперативних комбінацій, персональних даних і матеріалів кримінального

провадження. Такий баланс особливо важливий для оперативно-розшукової діяльності та контррозвідувальної роботи, документування воєнних злочинів.

Отже, теоретичні засади повноважень правоохоронних органів щодо інформаційного забезпечення мають бути спрямовані на формування правомірного інформаційного середовища, у якому швидкість доступу не суперечить законності, міжвідомча взаємодія не призводить до втрати відповідальності, автоматизований аналіз не підміняє рішення уповноваженої особи, а захист інформації не блокує виконання правоохоронних завдань. У такому середовищі електронна готовність, інструменти інформаційного забезпечення та компетенція правоохоронних органів утворюють єдину теоретичну основу для подальшого розвитку правоохоронної діяльності України в умовах воєнного стану та європейської інтеграції.

Висновки до розділу 2

1. Встановлено, що електронна готовність упровадження сучасних практик інформаційного забезпечення правоохоронної діяльності в Україні має розглядатися як комплексна організаційно-правова характеристика спроможності правоохоронних органів працювати з інформацією у цифровому середовищі. Зміст такої спроможності охоплює нормативну визначеність підстав оброблення даних, організаційну узгодженість діяльності суб’єктів, технічну сумісність інформаційних систем, кадрову підготовку користувачів, аналітичну спроможність, кіберстійкість, захист персональних даних, простежуваність інформаційних операцій і можливість подальшого контролю за правомірністю доступу та використання відомостей.

2. Обґрунтовано, що в умовах воєнного стану електронна готовність набуває значення самостійної умови правоохоронної спроможності держави, оскільки від належної організації цифрової роботи з інформацією залежить документування воєнних злочинів, розшук зниклих безвісти, ідентифікація осіб,

протидія кіберзагрозам, диверсійній діяльності, незаконному обігу зброї та іншим загрозам публічній безпеці. Однак, доведено, що основними проблемами залишаються нерівномірність цифрового розвитку правоохоронних органів, відомча роз'єднаність інформаційних ресурсів, різні правила доступу, дублювання інформаційних масивів, нестача фахівців і недостатня уніфікація критеріїв якості даних. Запропоновано оцінювати електронну готовність правоохоронних органів за критеріями правової визначеності, міжсистемної сумісності, захищеності, кадрової спроможності, актуальності даних, аналітичної придатності, підконтрольності доступу та функціональної стійкості.

3. Наголошено, що інструменти інформаційного забезпечення правоохоронної діяльності в Україні становлять функціонально пов'язану систему засобів, спрямованих на повний цикл роботи з відомостями, зокрема: від визначення інформаційної потреби до правомірного використання інформаційного результату у правоохоронному рішенні. Запропоновано класифікувати такі інструменти на нормативно-правові, організаційні, інформаційно-ресурсні, інформаційно-аналітичні, техніко-технологічні, безпекові та кадрово-методичні.

4. Встановлено, що ЄРДР, ЄІС МВС, ІПНП, АІС ОП, система «іКейс», спеціалізовані інформаційні підсистеми, кримінальний аналіз, OSINT, відеоаналітика, біометрична ідентифікація та засоби штучного інтелекту можуть бути ефективними інструментами правоохоронної діяльності лише за умови наявності правової підстави їх застосування, визначеної мети, розмежування доступу, фіксації інформаційних операцій, перевірки джерел, захисту персональних даних і обов'язкового контролю уповноваженого працівника. Технологічна новизна не є самостійним критерієм ефективності інструменту, якщо результат його застосування не є достовірним, актуальним, захищеним, перевірюваним і придатним для виконання конкретного правоохоронного завдання.

5. З'ясовано, що повноваження правоохоронних органів щодо інформаційного забезпечення правоохоронної діяльності утворюють

багатосуб’єктну систему, у межах якої Національна поліція України, СБУ, ДБР, БЕБ, НАБУ, органи прокуратури, ДПСУ та інші уповноважені органи виступають одночасно джерелами, користувачами, аналітичними обробниками, розпорядниками й суб’єктами захисту інформації. Запропоновано поділяти відповідні повноваження на такі групи: щодо створення і ведення інформаційних систем; одержання інформації; доступу до ресурсів інших суб’єктів; перевірки, аналізу й використання відомостей; передавання інформації; захисту даних і фіксації операцій; контролю законності, актуальності та цільового використання інформації.

6. Обґрунтовано суб’єктно-функціональний підхід до інформаційних повноважень, за яким орган-джерело відповідає за достовірність, повноту й актуальність внесених відомостей, орган-користувач – за правомірність доступу та використання, а орган-координатор – за узгодженість міжвідомчого обміну і дотримання встановлених правил. В умовах воєнного стану такий підхід має забезпечувати не безконтрольне розширення доступу до даних, а правову визначеність, службову необхідність, захист персональних даних, простежуваність кожного запиту та можливість виправлення помилок.

РОЗДІЛ 3. ФОРМИ ТА МЕХАНІЗМИ ЗАХИСТУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У СФЕРІ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ

Захист інформаційних технологій у сфері правоохоронної діяльності становить самостійний напрям організаційно-правового забезпечення функціонування органів правопорядку. Його значення визначається тим, що сучасна правоохоронна діяльність дедалі більшою мірою спирається на електронні реєстри, інформаційно-комунікаційні системи, цифрові документи, засоби електронної ідентифікації, кримінальний аналіз, біометричні технології, відеоаналітику, захищені канали міжвідомчого та міжнародного обміну. За таких умов відомості набувають правоохоронного значення лише тоді, коли їх походження, зміст, режим доступу, цілісність і шлях використання можуть бути перевірені.

Правоохоронна діяльність пов’язана з владним впливом на поведінку особи, реагуванням на правопорушення, документуванням події, обмеженням окремих прав, розшуком осіб, застосуванням заходів примусу, підготовкою процесуальних рішень і міжнародним інформаційним обміном. Тому захист інформаційних технологій у цій сфері має ширший зміст, ніж технічне обслуговування системи або запобігання несанкціонованому доступу. Йдеться про правовий порядок, за якого інформаційна технологія забезпечує достовірність, доступність, цілісність, конфіденційність, підконтрольність і відновлюваність відомостей, що використовуються для виконання правоохоронних завдань.

Воєнний стан істотно посилив вимоги до захисту інформаційних технологій. Правоохоронні органи працюють із цифровими слідами воєнних злочинів, інформацією про зниклих безвісти, біометричними даними, відомостями про переміщення зброї, матеріалами щодо колабораційної та диверсійної діяльності, даними про кіберінциденти, об’єкти критичної інфраструктури й міжнародні запити. За офіційною інформацією CERT-UA, у 2024 р. опрацьовано 4315 кіберінцидентів, що свідчить про значне зростання

навантаження на державний сектор кіберзахисту [130]. ENISA також звертає увагу, що публічна адміністрація належить до найбільш вразливих секторів, а в окремих оглядах частка інцидентів щодо неї становила 38 % [148]. Наведені дані підтверджують потребу розглядати захист інформаційних технологій як умову безперервності правоохоронної діяльності.

Нормативно-правове забезпечення захисту інформаційних технологій визначає правові межі доступу до інформації, її оброблення, зберігання, передавання та використання органами правопорядку. Конституційна основа такого захисту випливає зі ст. 32 Конституції України, якою гарантовано невтручання в особисте і сімейне життя та встановлено обмеження щодо збирання, зберігання, використання і поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом [41]. У ст. 31 Конституції України закріплено гарантію таємниці листування, телефонних розмов, телеграфної та іншої кореспонденції [41]. Водночас за змістом ст. 17 Конституції України забезпечення інформаційної безпеки належить до найважливіших функцій держави [41]. У діяльності органів правопорядку наведені положення формують правову межу, в якій технічна можливість доступу до інформаційного ресурсу підпорядковується закону, службовій меті, компетенції посадової особи та подальшому контролю.

КПК України має особливе значення для захисту інформаційних технологій, оскільки саме через процесуальні норми визначається придатність цифрової інформації для використання у кримінальному провадженні. За змістом ст. 84 КПК України доказами є фактичні дані, отримані у передбаченому Кодексом порядку, а процесуальними джерелами доказів визначено показання, речові докази, документи, висновки експертів [44]. У ст. 99 КПК України документ розкривається як матеріальний об’єкт, що містить зафіксовані за допомогою письмових знаків, звуку, зображення тощо відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження [44]. Отже, захист інформаційної технології прямо впливає на можливість підтвердити походження електронного матеріалу,

цілісність його змісту, спосіб отримання, час фіксації та зв’язок із конкретною процесуальною дією.

Правовий режим електронного документа конкретизовано в Законі України «Про електронні документи та електронний документообіг». Відповідно до ст. 5 цього Закону електронний документ визначено як документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов’язкові реквізити [65]. За змістом ст. 6 електронний підпис може використовуватися для ідентифікації автора електронного документа, а накладанням електронного підпису завершується створення електронного документа [65]. У ст. 7 закріплено положення про оригінал електронного документа [65]. Для органів правопорядку такі норми мають значення з огляду на необхідність встановлення автора, часу створення, незмінності змісту та належності електронного документа до певної процесуальної, оперативної або службової дії.

Спеціальну правову основу захисту інформації в інформаційних системах становить Закон України «Про захист інформації в інформаційно-комунікаційних системах». За змістом ст. 8 цього Закону умови обробки інформації в системі визначаються власником або розпорядником відповідної системи з урахуванням вимог щодо захисту інформації, встановлених законодавством [83]. Відповідно до ст. 9 відповідальність за забезпечення захисту інформації в системі покладається на власника або розпорядника системи, а в разі оброблення державних інформаційних ресурсів чи інформації з обмеженим доступом передбачається створення служби захисту інформації або призначення відповідальних осіб [83]. Наведені приписи мають принципове значення для правоохоронних інформаційних ресурсів, оскільки захист передбачає визначення відповідального суб’єкта, режиму оброблення, порядку контролю та наслідків порушення.

Закон України «Про захист персональних даних» встановлює вимоги до правомірного оброблення відомостей про фізичну особу. За змістом ст. 6 цього Закону мета обробки персональних даних має бути сформульована в законах, інших нормативно-правових актах або документах, що регулюють діяльність

володільця персональних даних [84]. У ст. 8 визначено права суб’єкта персональних даних, а ст. 16 регулює порядок доступу до персональних даних третіх осіб [84]. Для правоохоронної діяльності ці положення означають, що службова потреба в інформації повинна мати належну правову підставу, а обсяг доступу має відповідати меті, компетенції органу та характеру конкретного завдання. Як зазначає О. Марущак, правове забезпечення інформаційної безпеки правоохоронних органів має поєднувати охорону інформаційних ресурсів із гарантіями прав особи [49]. На нашу думку, саме таке поєднання дозволяє розглядати захист інформаційних технологій як правову умову допустимого використання даних у правоохоронних рішеннях.

Безпековий вимір захисту інформаційних технологій розкривається у Законі України «Про основні засади забезпечення кібербезпеки України». За змістом ст. 8 цього Закону національна система кібербезпеки охоплює суб’єктів забезпечення кібербезпеки та взаємопов’язані заходи політичного, науково-технічного, інформаційного, освітнього, організаційного, правового, оперативно-розшукового, розвідувального, контррозвідувального, оборонного, інженерно-технічного, криптографічного і технічного характеру [92]. Для органів правопорядку наведена норма важлива тим, що захист інформаційних технологій пов’язується з участю у загальнодержавному механізмі запобігання, виявлення, припинення та розслідування кіберзагроз. В умовах воєнного стану кібератака на інформаційний ресурс може одночасно вплинути на доступність даних, достовірність електронних доказів, безперервність реагування та безпеку міжвідомчої взаємодії.

У науковому плані захист інформаційних технологій доцільно розглядати як взаємозв’язок правового режиму інформації, організації служби, технічної архітектури, професійної підготовки працівника і контролю за використанням даних. На думку Я. В. Свічкарьової, інформаційна безпека в професійній діяльності правоохоронців має розглядатися через здатність працівника діяти з урахуванням правових і організаційних вимог до інформації [105, с. 64-68]. Як стверджує О. Марущак, правове забезпечення інформаційної безпеки

правоохоронних органів потребує узгодження загального інформаційного законодавства і спеціальних правоохоронних процедур [49]. Наведені позиції дозволяють виходити з того, що захист інформаційних технологій не зводиться до технічної інфраструктури.

Водночас у доктрині існують різні підходи до співвідношення інформаційної безпеки, кібербезпеки і захисту інформаційних технологій. Прихильники широкого підходу пов'язують інформаційну безпеку з охороною інформаційних прав, інформаційного простору, інформаційних ресурсів і діяльності суб'єктів. Представники вузького підходу акцентують увагу на захисті інформаційно-комунікаційних систем від кібератак, шкідливого програмного забезпечення, компрометації облікових записів, атак на доступність і втручання в роботу мереж. На нашу думку, для правоохоронної діяльності більш переконливим є поєднання обох підходів, оскільки неправомірне використання законно отриманих даних може бути таким самим небезпечним, як і зовнішнє втручання в систему.

3.1. Поняття та види форм захисту інформаційних технологій у сфері правоохоронної діяльності

Поняття форм захисту інформаційних технологій у сфері правоохоронної діяльності потребує попереднього розмежування змісту суміжних правових і організаційно-технічних категорій: захисту інформації, інформаційної безпеки, кібербезпеки, технічного захисту інформації, криптографічного захисту, захисту персональних даних, охорони державної таємниці, службового контролю й захисту цифрових доказів. Кожна з названих категорій відображає окремий аспект забезпечення належного режиму роботи з інформацією, однак у діяльності органів правопорядку вони функціонують у взаємозв'язку. Такий взаємозв'язок зумовлений тим, що інформаційні технології використовуються не лише для зберігання або передавання відомостей, а й для запобігання, виявлення,

припинення, документування та розслідування правопорушень, підготовки правоохоронних рішень, міжвідомчої взаємодії та міжнародного обміну інформацією.

У зв'язку з цим форма захисту інформаційних технологій має розглядатися як зовнішній прояв правових, організаційних, режимних, технічних і контрольних засобів, за допомогою яких забезпечується належне функціонування інформаційних ресурсів і систем у правоохоронній діяльності. Її зміст не вичерпується охороною відомостей від незаконного доступу, оскільки охоплює також збереження достовірності, цілісності, доступності, походження, правового режиму та можливості подальшої перевірки інформації, що використовується під час виконання правоохоронних завдань. Саме тому розмежування наведених категорій є необхідною передумовою для визначення видів форм захисту інформаційних технологій та їх значення для законного й обґрунтованого використання даних органами правопорядку.

Загальні правила роботи з інформацією закріплені передусім у базових інформаційних законах. За змістом ст. 1 Закону України «Про інформацію» інформацією визнаються будь-які відомості або дані, що можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [86]. Порядок доступу до інформації, що перебуває у володінні суб'єктів владних повноважень, визначається Законом України «Про доступ до публічної інформації» [64]. Спеціальний правовий режим відомостей, розголошення яких може завдати шкоди національній безпеці України, встановлено Законом України «Про державну таємницю» [63]. Для органів правопорядку наведені акти утворюють загальну нормативну основу, у межах якої кожна інформаційна технологія повинна застосовуватися з урахуванням правового режиму конкретних відомостей, мети їх оброблення, порядку доступу та допустимих меж подальшого використання.

На нашу думку, *під формою захисту інформаційних технологій у правоохоронній діяльності варто розуміти зовнішньо визначений правом, організаційною процедурою, режимним правилом або технічним стандартом*

спосіб забезпечення конфіденційності, цілісності, доступності, достовірності, контрольованості та відновлюваності інформаційних ресурсів, систем, каналів взаємодії, електронних документів і цифрових доказів, що використовуються під час виконання правоохоронних завдань. Запропоноване визначення дозволяє пов'язати захист інформаційної технології з її правовою придатністю для підготовки, перевірки та обґрунтування правоохоронного рішення. Результати анкетування підтверджують комплексний характер захисту: 28,8 % респондентів надали пріоритет правовим і режимним формам, 27,7 % – організаційним і контрольним, 24,4 % – технічним і криптографічним, а 19,1 % – кадровим, аналітико-перевірочним та етичним формам захисту інформаційних технологій (додаток Б).

У свою чергу, І. Є. Іванов, аналізуючи інформаційну безпеку в діяльності Національної поліції України, звертає увагу на необхідність поєднання інформаційно-аналітичної роботи з режимом захисту, відповідальністю працівників і спеціальними правилами доступу [26]. С. В. Сеник у дослідженні адміністративно-правового регулювання обігу інформації з обмеженим доступом у Національній поліції підкреслює значення визначеності суб'єктів, процедур і режимів такої інформації [107]. Наведені позиції засвідчують, що форма захисту повинна мати не лише технічний, а й правовий та організаційний зміст.

Однак, Н. С. Моргун пов'язує інформаційну безпеку в діяльності Національної поліції із захищеністю інформаційних ресурсів, службової інформації та прав людини [53]. А. В. Гарбінська-Руденко розглядає правоохоронні органи як важливих суб'єктів забезпечення інформаційної безпеки держави, зокрема в умовах воєнного стану [14]. Порівняння цих підходів дозволяє підтримати К. І. Белякова, що захист інформаційних технологій у правоохоронній діяльності виконує подвійну функцію: охороняє інформаційну систему органу і водночас захищає правомірність використання даних щодо особи [8, с. 58].

Предметом захисту виступають відомості, інформаційні ресурси, інформаційно-комунікаційні системи, канали електронної взаємодії, службові облікові записи, електронні документи, цифрові докази, журнали доступу, криптографічні ключі, резервні копії, мобільні пристрої й процедури оброблення. За змістом ст. 84 КПК України доказами у кримінальному провадженні є фактичні дані, отримані у передбаченому законом порядку, а процесуальними джерелами доказів визначено показання, речові докази, документи та висновки експертів [44]. У спеціальних настановах щодо роботи з цифровими доказами наголошується на необхідності їх ідентифікації, збирання, отримання, збереження, підтвердження походження, цілісності та можливості подальшої перевірки [153]. Аналогічний підхід простежується у європейських практичних рекомендаціях щодо електронних доказів, де особливе значення надається документуванню поводження з електронними матеріалами, збереженню їх автентичності та придатності для використання у провадженні [132]. Отже, захист інформаційних технологій має охоплювати не лише самі дані, а й умови, за яких вони можуть зберігати юридичне значення.

Правова форма захисту інформаційних технологій полягає у нормативному визначенні правового режиму інформації, підстав доступу, категорій даних, строків зберігання, процедур передавання, обмежень подальшого використання та відповідальності за порушення встановлених правил. Її зміст випливає з конституційних гарантій приватності, таємниці кореспонденції та інформаційної безпеки держави, закріплених у ст. 17, 31 і 32 Конституції України [41]. Загальні засади інформаційних відносин визначено у Законі України «Про інформацію» [86], а вимоги до правомірного оброблення відомостей про особу конкретизовано у Законі України «Про захист персональних даних» [84].

Пріоритетність правової форми зумовлена тим, що кожна дія з інформацією має спиратися на правову підставу, відповідати службовій меті та здійснюватися визначеним суб’єктом у межах його компетенції. Технічна можливість отримати відомості не створює самостійного права на їх

використання. Саме правова форма встановлює, які відомості можуть збиратися, хто має право доступу до них, з якою метою вони обробляються, кому можуть передаватися, як довго зберігаються та які наслідки настають у разі порушення встановленого режиму.

У кримінальному провадженні правова форма захисту інформаційних технологій набуває процесуального значення. За змістом ст. 84 КПК України доказами є фактичні дані, отримані у передбаченому таким нормативно-правовим документом порядку, а процесуальними джерелами доказів визначено показання, речові докази, документи, висновки експертів [44]. У ст. 99 КПК України документ розкривається як матеріальний об’єкт, що містить зафіксовані відомості, які можуть бути використані як доказ факту чи обставин кримінального провадження [44]. Якщо відомості отримано з електронної системи, правове значення мають зміст запису, підстава доступу, час отримання, особа користувача, незмінність інформації після вилучення та можливість перевірити її зв’язок із конкретною процесуальною дією. Правовий статус електронного документа додатково визначається Законом України «Про електронні документи та електронний документообіг», зокрема положеннями ст. 5-7 щодо електронного документа, електронного підпису та оригіналу електронного документа [65].

Організаційна форма захисту інформаційних технологій охоплює розподіл повноважень між держателем інформаційного ресурсу, адміністратором системи, користувачем, органом-джерелом, органом-одержувачем, аналітичним підрозділом, підрозділом внутрішнього контролю та особою, відповідальною за захист інформації. У Положенні про єдину інформаційну систему МВС визначено суб’єктів цієї системи та пріоритетні електронні інформаційні ресурси, що забезпечують діяльність органів системи МВС [75]. Організаційні засади функціонування інформаційного порталу Національної поліції закріплено в Положенні про ІПНП [76].

Зміст організаційної форми полягає у персоніфікації відповідальності за створення, зміну, передавання, перевірку і використання відомостей. Нечіткий

розподіл повноважень між держателем інформаційного ресурсу, адміністратором системи, відповідальним користувачем і посадовою особою, яка приймає правоохоронне рішення, ускладнює встановлення причини помилкового запису, неправомірного доступу або втрати інформації. За таких умов службове реагування стає менш результативним, оскільки неможливо своєчасно визначити, на якому етапі інформаційного процесу виникло порушення.

Під час міжвідомчої взаємодії організаційна форма має забезпечувати узгоджений розподіл відповідальності між органом, який створює або первинно перевіряє інформацію, органом, який адмініструє систему, та органом, який використовує відомості у конкретному провадженні, розшуковому заході, аналітичній роботі або службовій перевірці. У межах ЄІС МВС та ІПНП такий розподіл пов’язаний із різним призначенням окремих підсистем, різним колом користувачів і різними правовими наслідками використання інформації [75]. Саме тому організаційна форма захисту повинна забезпечувати не лише технічне функціонування інформаційного ресурсу, а й керованість дій посадових осіб, контроль доступу, фіксацію операцій та можливість встановлення відповідального суб’єкта [76].

Режимна форма захисту інформаційних технологій виражається у встановленні рівнів доступу, правил маркування інформації, обліку матеріальних і електронних носіїв, копіювання, передавання, архівування, знищення та припинення доступу до відомостей. Її правову основу становлять норми, що визначають порядок роботи з інформацією різного ступеня відкритості. За змістом Закону України «Про державну таємницю» спеціальний режим установлюється щодо відомостей, розголошення яких може завдати шкоди національній безпеці України [63]. Обмеження доступу до публічної інформації допускається відповідно до ст. 6 Закону України «Про доступ до публічної інформації» за умови дотримання встановлених законом критеріїв [64]. У діяльності органів правопорядку режимна форма має враховувати різну правову природу персональних даних, відомостей досудового розслідування,

оперативної інформації, службової інформації, даних про розшук, зброю, перетин державного кордону та об’єкти критичної інфраструктури.

Під час роботи з інформацією з обмеженим доступом режимна форма повинна поєднувати вимоги таємності з можливістю внутрішньої перевірки правомірності дій посадових осіб. С. В. Сеник слушно звертає увагу, що адміністративно-правове регулювання обігу інформації з обмеженим доступом у Національній поліції має бути спрямоване на визначення суб’єктів, режимів і процедур [107]. Наведена позиція є важливою, оскільки режим інформації повинен відображатися не лише у грифі обмеження доступу чи назві інформаційного ресурсу, а й у правах користувачів, правилах копіювання, строках зберігання, порядку передавання, підставах припинення доступу та контролі подальшого використання відомостей.

Технічна форма захисту інформаційних технологій передбачає застосування програмних, апаратних, мережевих та інженерних засобів, за допомогою яких забезпечуються контроль доступу, цілісність, доступність, резервування, сегментація мережі, оновлення програмного забезпечення, захист каналів зв’язку і відновлення роботи систем після інцидентів. Правила забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах визначені постановою Кабінету Міністрів України № 373 [82]. Порядок проведення робіт зі створення комплексної системи захисту інформації деталізовано у нормативному документі системи технічного захисту інформації (НД ТЗІ) 3.7-003-05 [54].

Застосування технічної форми має узгоджуватися з правовим режимом інформації, службовим призначенням ресурсу, колом користувачів і рівнем ризику. Для різних інформаційних систем добираються різні технічні рішення, оскільки ресурс досудового розслідування, розшуковий облік, система відеоаналітики, реєстр зброї або канал міжнародного обміну мають неоднакове функціональне навантаження та різні наслідки порушення конфіденційності, цілісності чи доступності даних.

У діяльності чергових частин, слідчо-оперативних груп і аналітичних підрозділів технічна форма захисту має забезпечувати безперервний доступ до критично необхідних ресурсів із одночасним контролем дій користувача. У період воєнного стану технічна відмова може вплинути на реагування, розшук, евакуацію, фіксацію наслідків обстрілу або документування воєнного злочину. Зміст цієї форми охоплює захищеність, резервування, швидке відновлення роботи системи та перевірку цілісності даних після збою.

Криптографічна форма захисту інформаційних технологій спрямована на забезпечення конфіденційності, автентичності, цілісності та невідмовності електронних повідомлень, документів, журналів доступу й масивів даних, що передаються між уповноваженими суб'єктами. Її нормативну основу становить Закон України «Про електронну ідентифікацію та електронні довірчі послуги», який регулює відносини у сфері електронної ідентифікації, автентифікації та надання електронних довірчих послуг [67]. Європейські підходи до електронної ідентифікації та довірчих послуг закріплені у Регламенті eIDAS, положення якого орієнтують держави на забезпечення довіри до електронної взаємодії, електронних підписів, печаток, часових позначок і засобів ідентифікації [174].

У міжвідомчому обміні криптографічна форма дозволяє підтвердити належність електронного повідомлення конкретному суб'єкту, захистити його зміст від підміни, встановити час вчинення інформаційної дії та зберегти можливість подальшої перевірки. Для органів правопорядку криптографічний захист має бути пов'язаний із службовою метою запиту, правовим режимом інформації та відповідальністю користувача. Електронний підпис, електронна печатка, шифрування, контроль цілісності й фіксація часу виконують не тільки технічну, а й юридичну функцію, оскільки підтверджують походження інформації та сталість її змісту після передавання.

Процедурна форма захисту інформаційних технологій визначає послідовність внесення, перевірки, актуалізації, пошуку, зіставлення, передавання, виправлення, блокування, архівування або видалення відомостей. Загальні правила створення, ведення, взаємодії та адміністрування публічних

електронних реєстрів закріплено у Законі України «Про публічні електронні реєстри» [95]. Порядок формування і ведення Єдиного реєстру досудових розслідувань визначено відповідним Положенням про ЄРДР [74].

Зміст процедурної форми полягає у встановленні перевірюваного зв'язку між первинною інформаційною дією і подальшим правоохоронним рішенням. Саме процедура дає змогу з'ясувати, хто вніс запис, на якій правовій підставі, коли він був перевірений, кому передавався, чи змінювався його зміст і чи зберіг він актуальність на момент використання. Відсутність такої послідовності ускладнює встановлення походження відомостей і створює ризик використання інформації без належної перевірки.

Під час внесення й актуалізації записів процедурна форма запобігає повторному використанню застарілих або помилкових відомостей. Якщо особу знято з розшуку, кримінальне провадження закрито, підозру змінено або біометричний збіг спростовано, пов'язані записи мають бути перевірені в усіх ресурсах, до яких вони були передані. Спеціальне значення електронних процедур у розшуковій діяльності підтверджується Положенням про електронну розшукову справу [77].

Кадрова форма захисту інформаційних технологій пов'язана з добором, навчанням, інструктажем, перевіркою доброчесності та службовою відповідальністю працівників, які мають доступ до захищених інформаційних ресурсів. Я. В. Свічкарьова підкреслює, що інформаційна безпека правоохоронця залежить від його професійної здатності діяти в інформаційному середовищі з урахуванням правових вимог [105, с. 64]. О. В. Таран розглядає інформаційні технології як складову професійної підготовки працівників правоохоронної сфери [113].

Зміст кадрової форми полягає не лише у формальному допуску працівника до інформаційної системи, а й у його здатності правильно визначати правову підставу запиту, межі службової необхідності, порядок копіювання, передавання, збереження та використання відомостей. Недостатня підготовка користувача знижує ефективність навіть належно побудованого технічного

захисту, оскільки порушення режиму інформації часто виникає не через складність системи, а через неправильне розуміння працівником своїх повноважень.

Під час роботи з персональними даними, службовими обліками, цифровими доказами і міжнародними запитами кадрова форма набуває особливої ваги. Працівник повинен розуміти, коли запит є службово обґрунтованим, які відомості можуть бути використані у конкретному провадженні або перевірці, кому вони можуть передаватися, як фіксується помилка та в якому порядку повідомляється про інцидент. Саме тому професійна підготовка має охоплювати не тільки технічні навички користування системою, а й знання правового режиму інформації, правил доступу, відповідальності та меж подальшого використання даних.

Контрольна форма захисту інформаційних технологій полягає у перевірці правомірності доступу, аналізі журналів, проведенні службових розслідувань, аудиті інформаційних систем, а також у прокурорському, судовому, парламентському та іншому передбаченому законом контролі. За змістом ст. 25 Закону України «Про Національну поліцію» поліція здійснює інформаційно-аналітичну діяльність виключно для реалізації своїх повноважень, а кожна дія щодо отримання інформації з інформаційних ресурсів фіксується у спеціальному електронному архіві [90].

Контрольна форма переводить доступ до інформації у юридично перевірюваної дії. Реєстрація подій виконує гарантійну функцію лише за умови реального аналізу його даних: хто звертався до ресурсу, з якою метою, у межах якого завдання, який обсяг інформації отримано та чи використовувалися відомості відповідно до правового режиму.

Контрольна форма виявляється у перевірці нетипових запитів, масового вивантаження даних, повторного доступу без службового зв’язку, використання облікового запису в нетипових умовах або передавання відомостей поза визначеною метою. Формальне збереження журналу доступу саме по собі не гарантує законності. Належний контроль передбачає регулярну перевірку

інформаційних операцій, встановлення відповідального користувача, оцінку службової мети запиту та реагування на кожне порушення встановленого порядку.

Аналітико-перевірочна форма захисту інформаційних технологій спрямована на оцінювання джерела відомостей, ступеня їх підтвердження, актуальності, повноти, наявності суперечностей, ризику помилкового збігу та допустимих меж використання аналітичного результату. У Регламенті ЄС про ШІ особлива увага приділена високоризиковим системам, застосування яких може впливати на права людини [172]. У міжнародних підходах до архітектури нульової довіри наголошується на постійній перевірці користувача, пристрою, запиту та умов доступу до інформаційного ресурсу [162].

Автоматизований збіг, ризиковий профіль або інший результат машинного зіставлення виконує орієнтуючу функцію і потребує подальшої перевірки уповноваженим працівником. Юридично значуще рішення повинно залишатися персоніфікованим, мотивованим і таким, що може бути перевірене за джерелами, логікою аналізу та фактичними даними, які покладені в його основу. Таке розмежування підтримали 80,6 % опитаних, які вважають автоматизований результат орієнтиром для подальшої перевірки, а не остаточною підставою правоохоронного рішення; щодо біометричних технологій і відеоаналітики 69,9 % респондентів вказали на обов’язковість фіксації правової підстави, мети, якості зразка та перевірки результату уповноваженою особою (додаток Б).

Під час кримінального аналізу аналітико-перевірочна форма має забезпечувати розмежування встановленого факту, оперативного повідомлення, аналітичного припущення, статистичної закономірності та результату автоматизованого збігу. Змішування цих категорій створює ризик, за якого первинна помилка або неперевірене припущення надалі сприймаються як достовірне знання. Саме тому результати автоматизованого аналізу повинні супроводжуватися відомостями про джерела, ступінь перевіреності, межі достовірності та службову мету використання [172].

Відновлювальна форма захисту інформаційних технологій охоплює резервне копіювання, дублювання критичних сервісів, аварійне відновлення, збереження журналів, перевірку цілісності даних після інциденту та поновлення встановлених обмежень доступу. У міжнародних рекомендаціях щодо реагування на інциденти інформаційної безпеки та кіберінциденти відновлення розглядається як складова керованого процесу, що включає підготовку, виявлення, аналіз, стримування, усунення наслідків і повернення системи до належного стану [159]. Загальні принципи управління інцидентами інформаційної безпеки також закріплені у стандартах серії ISO/IEC 27035 [152].

В умовах воєнного стану відновлювальна форма набуває особливого значення для забезпечення безперервності розшуку осіб, досудового розслідування, реагування на загрози, фіксації наслідків збройної агресії та документування воєнних злочинів. Порушення роботи інформаційної системи за таких обставин може вплинути не тільки на технічну доступність ресурсу, а й на своєчасність правоохоронного реагування, збереження цифрових доказів та можливість подальшої перевірки прийнятих рішень.

Після кібератаки або технічного збою відновлювальна форма повинна забезпечувати повернення даних разом із їх правовим контекстом. Відновлення бази без журналів доступу, історії змін, прав користувачів, контрольних сум, відомостей про джерело та обмежень подальшого використання не забезпечує повного відновлення інформаційного ресурсу. Належне відновлення має підтверджувати не лише працездатність системи, а й цілісність, походження, актуальність і допустимість подальшого використання відомостей [159].

Міжнародно-кооперaційна форма захисту інформаційних технологій охоплює застосування погоджених каналів зв’язку, форматів даних, процедур запиту, правил передавання, обмежень подальшого використання та визначення відповідальної сторони під час взаємодії з іноземними правоохоронними органами й міжнародними організаціями. Міжнародно-правову основу такого співробітництва становить Конвенція про кіберзлочинність, яка закріплює засади взаємної допомоги, збереження комп’ютерних даних, доступу до

електронних доказів і взаємодії компетентних органів у справах, пов’язаних із кіберзлочинністю [40]. Другий додатковий протокол до цієї Конвенції спрямований на посилення співробітництва щодо розкриття електронних доказів, зокрема шляхом удосконалення процедур безпосередньої взаємодії з постачальниками послуг та компетентними органами інших держав [176].

Передавання відомостей за межі України має супроводжуватися збереженням їх правового режиму, визначеної мети, обмежень подальшого використання, вимог конфіденційності та можливості встановлення органу, відповідального за правомірність надання й подальшого застосування інформації. Такий порядок відповідає принципу еквівалентного захисту інформації, за яким міжнародний обмін не повинен знижувати рівень гарантій, установлених для первинного збирання, перевірки й використання відомостей.

Під час отримання електронних доказів з-за кордону міжнародно-кооперaційна форма має забезпечувати відповідність запиту правовій підставі, службовій меті, обсягу необхідних відомостей і гарантіям захисту особи. Особливого значення набуває чітке визначення виду запитуваної інформації, способу її одержання, строків збереження, умов подальшого передавання та процесуального значення для конкретного провадження. За таких умов міжнародне співробітництво виступає не лише каналом отримання даних, а й правовою процедурою, від належного дотримання якої залежить допустимість, достовірність і перевірюваність електронних доказів.

Етична форма захисту інформаційних технологій полягає у запобіганні дискримінаційному профілюванню, доступу до інформації з мотивів, не пов’язаних зі службовою потребою, необґрунтованому спостереженню, використанню автоматизованого збігу як установленого факту без перевірки та ігноруванню права особи на виправлення помилкових відомостей. Директива (ЄС) 2016/680 встановлює спеціальні гарантії оброблення персональних даних компетентними органами з метою запобігання, розслідування, виявлення або переслідування кримінальних правопорушень [140]. Конвенція 108 Ради Європи закріплює загальні принципи законного автоматизованого оброблення

персональних даних, зокрема добросовісність, визначеність мети, пропорційність, точність і захищеність даних [39].

Етична форма набуває юридичного значення, оскільки порушення балансу між безпековою потребою та правами людини може поставити під сумнів правомірність інформаційної дії, знизити доказову цінність отриманих відомостей і спричинити прийняття необґрунтованого правоохоронного рішення. Застосування інформаційних технологій має залишатися пов'язаним із конкретним правоохоронним завданням, а не з формальною доступністю даних у системі.

Під час використання автоматизованих засобів етична форма має запобігати перетворенню службової зручності на надмірне втручання у приватне життя. Якщо система дає змогу швидко зіставити особу, транспортний засіб, місце перебування або соціальні зв'язки, працівник повинен оцінити законність доступу, пропорційність втручання, службову необхідність запиту та надійність отриманого результату. Автоматизований збіг у такому разі має значення орієнтира для подальшої перевірки, а не самостійної підстави для остаточного правоохоронного рішення [140].

Відзначимо, що поява нових способів оброблення даних, хмарних сервісів, автоматизованої відеоаналітики, біометричних інструментів, мобільного доступу, електронного провадження та транскордонного обміну зумовлює появу нових організаційних і правових режимів. Водночас основні критерії залишаються сталими: правова підстава, службова мета, відповідальний суб'єкт, контроль доступу, захист відомостей, можливість перевірки та поновлення прав особи у разі помилки.

Наукова дискусія щодо форм захисту інформаційних технологій дозволяє виокремити два методологічні підходи. Перший орієнтується на захист системи як технічного середовища, у якому обробляються дані. Другий виходить із захисту правоохоронного рішення, у якому інформаційна технологія є лише одним із елементів. На нашу думку, такі підходи варто поєднати: захист має

охоплювати систему як програмно-технічний об’єкт і весь інформаційний шлях від первинного повідомлення до його використання в правоохоронному рішенні.

С. Г. Петров, досліджуючи повноваження Служби безпеки України як суб’єкта національної системи кібербезпеки, наголошує на значенні координації й правового визначення ролей у цій сфері [59, с. 100]. І. Д. Казанчук розкриває особливості діяльності Національної поліції у сфері забезпечення інформаційної безпеки та підкреслює значення спеціального правового регулювання відповідних повноважень [33, с. 74]. Такі підходи підтверджують потребу класифікувати форми захисту за суб’єктами, об’єктами, процедурою і правовими наслідками.

Таким чином, *форми захисту інформаційних технологій у сфері правоохоронної діяльності становлять систему правових, організаційних, режимних, технічних, криптографічних, процедурних, кадрових, контрольних, аналітико-перевірочних, відновлювальних, міжнародно-кооераційних та етичних способів забезпечення безпечного, правомірного й контрольованого функціонування інформаційних ресурсів, систем і каналів електронної взаємодії*. Їх наукове значення полягає у конкретизації правового режиму поводження з інформаційною технологією: від визначення підстав доступу й кола користувачів до перевірки походження відомостей, захисту цифрових доказів, фіксації інформаційних операцій та відновлення роботи систем після інциденту.

У науковій літературі захист інформаційних технологій переважно розглядається крізь призму інформаційної безпеки [2]. Такий підхід охоплює правовий режим інформації, стан захищеності систем, поведінку користувача, службову дисципліну та довіру до органу правопорядку [28]. Водночас для теоретичного осмислення досліджуваного питання важливо розмежовувати інформаційну безпеку як бажаний стан і форми захисту як юридично, організаційно та технічно визначені способи його досягнення. Стан захищеності характеризує результат належної організації роботи з інформацією, тоді як форма захисту розкриває, за допомогою яких правових приписів, процедур,

режимних правил, технічних засобів і контрольних дій цей результат забезпечується.

Як стверджує Н. С. Моргун, визначення інформаційної безпеки в діяльності Національної поліції України повинно враховувати багаторівневий характер відповідних відносин [53]. Погоджуючись із таким підходом, вважаємо, що багаторівневість не повинна розмивати предмет захисту. Для правоохоронного органу принципове значення має відповідь на питання, який саме об’єкт захищається: персональні дані, службовий реєстр, канал обміну, електронний документ, цифровий доказ, обліковий запис користувача чи аналітичний продукт.

О. А. Марущак наголошує на необхідності правового забезпечення інформаційної безпеки правоохоронних органів [49]. Наведена позиція є важливою для розмежування правових і технічних форм захисту. Правова форма визначає межі допустимої діяльності, а технічна форма забезпечує виконання цих меж у конкретній системі. Тому програмне обмеження доступу повинно відображати не лише внутрішню логіку системи, а й закон, службову компетенцію та цільове призначення інформації.

І. Є. Іванов, аналізуючи діяльність Національної поліції, звертає увагу на актуальність захисту інформації в умовах використання відомчих інформаційних ресурсів [26]. З цього випливає, що форма захисту має бути пов’язана з повсякденною службовою дією: внесенням даних, перевіркою особи, використанням розшукового обліку, створенням аналітичної довідки, передаванням відповіді іншому органу або наданням інформації в межах міжнародного співробітництва.

С. В. Сеник досліджує обіг інформації з обмеженим доступом у діяльності Національної поліції крізь призму адміністративно-правового регулювання [107]. У контексті захисту інформаційних технологій ця позиція дозволяє сформулювати важливе положення: обмеження доступу повинно мати процесуальний і технічний прояв. Якщо правовий режим не відображений у

системних ролях, заборонах копіювання, журналах доступу й контролі передавання, він залишається декларативним.

На думку Д. Калюжного, цифровізація правоохоронної діяльності посилює значення захисту інформаційних прав особи [34]. Такий висновок варто поширити на всі форми захисту інформаційних технологій, позаяк такі мають обслуговувати не лише внутрішню безпеку органу, а й право людини на правомірне, пропорційне й контрольоване використання даних, які стосуються її приватного життя, пересування, зв'язків, майна або процесуального статусу.

У свою чергу П. Д. Біленчук та Л. В. Борисова розглядають інформаційну безпеку як комплексне явище, що виходить за межі технічної охорони відомостей [9]. Така позиція є обґрунтованою, оскільки інформаційна технологія у діяльності органів правопорядку використовується для встановлення факту, особи, маршруту, зв'язку, ризику або іншої юридично значущої обставини, а тому безпосередньо впливає на реалізацію прав і свобод людини.

Отже, доктринальна дискусія підтверджує доцільність розуміння форм захисту інформаційних технологій як системи взаємопов'язаних способів правової, організаційної, режимної, технічної та контрольної охорони інформаційного процесу. За такого підходу захист не зводиться до пароля, шифрування чи формальної заборони доступу, а охоплює весь шлях інформації: її походження, внесення до системи, перевірку, зберігання, передавання, аналітичне опрацювання, використання у правоохоронному рішенні та подальший контроль правомірності такого використання.

3.2. Механізми захисту інформаційних технологій у сфері правоохоронної діяльності

Механізми захисту інформаційних технологій у сфері правоохоронної діяльності характеризують внутрішню послідовність правових, організаційних, технічних і контрольних дій, за допомогою яких забезпечується належний режим

роботи інформаційної системи. Форма показує спосіб організації захисту, а механізм розкриває порядок його дії: від визначення інформаційного активу до реагування на інцидент, відновлення системи, службового контролю та відповідальності.

У загальнотеоретичному значенні, на думку І. В. Арістової, механізм правового забезпечення охоплює норми права, юридичні факти, суб'єктів, процедури, гарантії і засоби відповідальності. У сфері захисту інформаційних технологій такий механізм повинен включати визначення інформаційного активу, оцінку ризиків, правовий режим інформації, розподіл ролей, допуск користувачів, технічний і криптографічний захист, моніторинг, реагування, відновлення, документування і контроль [2, с. 19].

М. В. Гуцалюк звертає увагу, що під час воєнного стану кіберзлочинність набуває особливої суспільної небезпечності через поєднання кримінальних, розвідувальних, диверсійних та інформаційно-психологічних впливів [16]. А. І. Семенченко розглядає кібернетичну безпеку і кібернетичний захист як сферу, що потребує організаційно-правових механізмів державного управління [106]. На підставі цих позицій *механізм захисту інформаційних технологій у правоохоронній діяльності доцільно розуміти як узгоджену систему процедур, засобів і відповідальності, що забезпечує правомірний та контрольований режим роботи інформаційної технології*.

Дискусійним залишається питання про допустимі межі автоматизації захисту інформаційних технологій. За одним підходом, належний рівень захищеності досягається переважно шляхом технічного обмеження доступу, автоматичного виявлення нетипових дій користувача, блокування ризикових операцій і фіксації інформаційних слідів. Інший підхід пов'язує ефективність захисту з чітким правовим режимом інформації, службовою дисципліною, належною підготовкою працівників і персональною відповідальністю за використання відомостей. На нашу думку, автоматизація повинна посилювати контроль за інформаційними операціями, але не замінювати оцінку правових

підстав, службової необхідності та відповідальність уповноваженої особи за прийняте правоохоронне рішення.

Механізм «*ідентифікації інформаційного активу*» передбачає встановлення відомостей, систем, каналів зв'язку, пристроїв, журналів доступу, криптографічних ключів, резервних копій та інших елементів, що мають службове значення для виконання правоохоронних завдань. Його зміст полягає у визначенні держателя інформаційного ресурсу, адміністратора системи, кола користувачів, категорій інформації, рівня критичності ресурсу, правового режиму відомостей і можливих наслідків їх втрати, спотворення, блокування або неправомірного використання. Початковий опис інформаційного активу є необхідною умовою для встановлення належного режиму доступу, резервування, міжвідомчої взаємодії, контролю операцій і персоніфікації відповідальності.

Застосування цього механізму має бути пов'язане з конкретним правоохоронним завданням. Запобігання правопорушенню, розшук особи, фіксація події, досудове розслідування або міжнародний запит потребують різного обсягу інформації, різних строків доступу, різного рівня перевірки й різних гарантій захисту. Тому механізм ідентифікації інформаційного активу повинен забезпечувати узгодження правової підстави, службової потреби, технічної дії та подальшого контролю за використанням відомостей.

У межах механізму «ідентифікація інформаційного активу» доцільно починати з визначення критичності ресурсу для конкретної правоохоронної функції. Інформаційна система, що використовується для реєстрації повідомлень, має інший профіль ризику, ніж ресурс біометричної ідентифікації або система міжнародного обміну. Тому інвентаризація повинна фіксувати не лише технічні параметри, а й правові наслідки втрати, зміни або недоступності відомостей.

Механізм «*оцінки загроз і ризиків*» охоплює аналіз зовнішніх кібератак, фішингу, шкідливого програмного забезпечення, атак на доступність, компрометації облікових записів, фізичного пошкодження інфраструктури,

внутрішніх порушень, помилкового внесення даних і неналежного використання інформаційних ресурсів. У сучасних міжнародних підходах до кібербезпеки управління ризиками розглядається через послідовне визначення активів, захист, виявлення інцидентів, реагування та відновлення належного функціонування систем [161]. У звітах ENISA щодо ландшафту кіберзагроз звертається увага на зростання ризиків для державного сектору, що має особливе значення для органів правопорядку в умовах воєнного стану [146].

Оцінка загроз і ризиків повинна враховувати не лише технічну вразливість системи, а й правові наслідки можливої помилки. Втрата доступу до розшукового обліку, спотворення запису в реєстрі, компрометація службового облікового запису або використання неактуальних відомостей можуть вплинути на своєчасність реагування, законність процесуальної дії, безпеку працівників і захист прав особи. Саме тому результатом оцінки ризиків має бути не загальний опис небезпек, а визначення конкретних заходів захисту, відповідальних суб’єктів, порядку реагування та строків перевірки ефективності таких заходів.

У межах механізму «оцінка загроз і ризиків» повинна враховувати зовнішнього нападника, внутрішнього порушника, технічну помилку, недобросовісного постачальника, службову недбалість і воєнні фактори. Для прифронтових або евакуйованих підрозділів ризики пов’язані також із фізичною втратою обладнання, нестабільним зв’язком і потребою швидкого відновлення доступу до критичних ресурсів. Кожний механізм захисту повинен мати нормативну підставу, визначеного виконавця, технічний спосіб виконання, журнал контролю і наслідки порушення. Оцінювання захисту інформаційної технології має спиратися на здатність системи забезпечити законний, перевірюваний і безпечний рух відомостей.

Механізм «*визначення правового режиму інформації*» пов’язаний із встановленням належності відомостей до відкритої інформації, персональних даних, службової інформації, державної таємниці, таємниці досудового розслідування або оперативної інформації. Правовий режим державної таємниці визначається Законом України «Про державну таємницю», який встановлює

порядок віднесення інформації до таємної, її засекречування, охорони та доступу до неї [63]. Вимоги до правомірного оброблення відомостей про фізичну особу закріплено у Законі України «Про захист персональних даних», зокрема щодо визначення мети оброблення, складу даних, прав суб'єкта персональних даних і підстав доступу до них [84].

Застосування цього механізму має бути пов'язане з конкретним правоохоронним завданням, оскільки запобігання правопорушенню, розшук особи, фіксація події, досудове розслідування або міжнародний запит потребують різного обсягу інформації, строків доступу та рівня перевірки. Визначення правового режиму відомостей дає змогу встановити допустимі межі їх одержання, зберігання, передавання, аналітичного опрацювання і подальшого використання. Помилка на цьому етапі може призвести до незаконного доступу, розголошення інформації з обмеженим доступом, порушення прав особи або втрати доказового значення отриманих даних.

Визначення правового режиму» має супроводжувати кожний етап життєвого циклу даних. Відомості, отримані законно для однієї мети, можуть бути непридатними для іншої мети без додаткової правової підстави. Саме тому у службовій системі має зберігатися позначка про мету оброблення, обмеження використання і строк актуальності.

Механізм «*допуску й авторизації користувача*» передбачає перевірку особи, її службової ролі, рівня доступу, строку повноважень і зв'язку запиту з конкретним правоохоронним завданням. За змістом ст. 25 Закону України «Про Національну поліцію» інформаційно-аналітична діяльність поліції здійснюється виключно для реалізації її повноважень, а кожна дія щодо отримання інформації з інформаційних ресурсів фіксується у спеціальному електронному архіві [90]. Отже, доступ до інформації має розглядатися як юридично значуща службова дія, а не як звичайне технічне підключення користувача до системи.

Допуск і авторизація повинні забезпечувати відповідність між правовою підставою, службовою потребою, обсягом доступу та подальшим контролем. Працівник має отримувати лише той рівень доступу, який необхідний для

виконання визначеного завдання, а зміна посади, завершення службової перевірки, передання провадження або припинення повноважень повинні зумовлювати перегляд чи припинення доступу. Такий механізм зменшує ризики службової цікавості, несанкціонованого копіювання, використання облікового запису поза службовою метою та неконтрольованого поширення відомостей.

У межах механізму, допуск і авторизація мають періодично переглядатися. Переведення працівника на іншу посаду, відсторонення, зміна функціональних обов'язків, завершення службової перевірки або закриття провадження повинні ініціювати перегляд доступу. Надання доступу на невизначений строк створює ризик накопичення надмірних повноважень.

Механізм «*електронної ідентифікації*» забезпечує прив'язку інформаційної дії до конкретного користувача, його електронного підпису, службового облікового запису, засобу автентифікації або іншого ідентифікатора, що дає змогу встановити відповідального суб'єкта. Правові засади електронної ідентифікації, автентифікації та використання електронних довірчих послуг визначено Законом України «Про електронну ідентифікацію та електронні довірчі послуги» [67]. Спільне використання паролів, передавання доступу іншій особі або робота під чужим обліковим записом руйнують персоніфікацію відповідальності та унеможливлюють належну перевірку інформаційної дії.

Електронна ідентифікація має бути персональною, стійкою до передавання іншій особі та пов'язаною з конкретним правоохоронним завданням. Обліковий запис у правоохоронній інформаційній системі є засобом встановлення відповідального користувача, а тому використання багатофакторної автентифікації, службових токенів, електронного підпису, фіксації часу входу й технічних параметрів доступу має пряме правове значення. Завдяки цьому забезпечується відповідність між правовою підставою, службовою потребою, технічною дією та подальшим контролем за використанням відомостей.

Механізм «*розмежування прав користувачів*» полягає у відокремленні прав перегляду, внесення, зміни, експорту, видалення, копіювання, аналітичного опрацювання та передавання відомостей. У спеціальних рекомендаціях щодо

безпеки інформаційних систем значна увага приділяється контролю доступу, аудиту, ідентифікації користувача та встановленню відповідальності за дії в системі [160]. Права користувача мають відповідати його службовим повноваженням, характеру правоохоронного завдання, категорії інформації та допустимому обсягу її використання.

Розмежування доступу потребує поєднання рольового і контекстного підходів. Роль визначає загальну компетенцію працівника, а контекст уточнює зв'язок конкретного запиту з кримінальним провадженням, розшуковим завданням, чергуванням, службовою перевіркою, аналітичною роботою або міжнародним дорученням. Поєднання цих критеріїв зменшує ризик формального доступу без службової потреби та дозволяє надати працівникові саме той обсяг інформації, який необхідний для виконання визначеного завдання.

Механізм «*журналювання операцій*» забезпечує фіксацію користувача, часу, інформаційного ресурсу, змісту запиту, правової підстави, службової мети, результату, обсягу отриманої інформації та подальших дій із нею. Журнал доступу повинен бути захищений від зміни самим користувачем і зберігати дані у формі, придатній для службової перевірки, аудиту або процесуальної оцінки. За змістом ст. 25 Закону України «Про Національну поліцію» фіксація дій щодо отримання інформації є складовою інформаційно-аналітичної діяльності поліції [90]. За результатами анкетування, 37,0 % респондентів визначили журналювання передусім як засіб перевірки законності доступу, 29,6 % – як спосіб персоніфікації дій користувача, а 26,9 % – як інструмент службового контролю, що підтверджує його значення не тільки для технічного адміністрування, а й для юридичної оцінки інформаційної операції (додаток Б).

Журналювання має охоплювати позитивні, негативні й часткові результати запитів. Відсутність знайденого запису, відмова в доступі, спроба перегляду забороненої категорії даних, незавершена операція або повторний запит без очевидного службового зв'язку також мають значення для контролю. Такі записи дозволяють виявити підготовку до неправомірного доступу, помилку в

налаштуваннях прав користувача, технічний збій або інші обставини, що можуть вплинути на законність подальшого використання інформації.

Механізм «*аналізу журналів і службового контролю*» передбачає перевірку нетипових запитів, масового вивантаження даних, доступу без очевидного службового зв'язку, роботи у нетиповий час, спроб обходу обмежень і повторного звернення до відомостей з підвищеним рівнем захисту. На думку І. Є. Іванова, належний контроль за доступом до інформаційних ресурсів поліції має поєднувати відповідальність працівника, фіксацію його дій та перевірку обґрунтованості використання службових даних [26]. Просте накопичення журналів не забезпечує законності, якщо їх зміст не аналізується уповноваженим підрозділом.

Аналіз журналів має поєднувати автоматизоване виявлення нетипових операцій зі службовою оцінкою їх змісту. Інформаційна система може позначити підозрілу активність, однак відповідальний працівник повинен встановити, чи була вона пов'язана з реальним службовим завданням, надзвичайною подією, технічною помилкою, неправильним налаштуванням доступу або ознаками дисциплінарного чи іншого правопорушення. Саме така перевірка дозволяє пов'язати технічний запис у журналі з правовою підставою, службовою потребою, обсягом отриманої інформації та наслідками її використання.

Механізм «*створення та підтримання комплексної системи захисту інформації*» охоплює обстеження середовища функціонування інформаційної системи, визначення загроз, розроблення технічного завдання, впровадження організаційних і технічних заходів, випробування та підтвердження відповідності встановленим вимогам. Порядок проведення робіт зі створення комплексної системи захисту інформації визначено у нормативному документі системи технічного захисту інформації (НД ТЗІ) 3.7-003-05 [54]. Оцінювання стану захищеності державних інформаційних ресурсів регулюється наказом Адміністрації Держспецзв'язку № 660 [80].

Комплексна система захисту інформації має розглядатися як постійний процес підтримання належного рівня захищеності, а не як одноразове технічне

оформлення інформаційної системи. Її заходи потребують перегляду після зміни програмного забезпечення, підключення нового реєстру, розширення кола користувачів, зміни каналу зв'язку, виявлення нової вразливості або появи нового класу загроз. Для органів правопорядку це має особливе значення, оскільки інформаційні системи безпосередньо забезпечують реагування, розшук, досудове розслідування, аналітичну роботу та міжвідомчу взаємодію.

Механізм «*криптографічного захисту*» забезпечує захищене передавання і зберігання даних, автентичність електронних повідомлень, цілісність електронних документів та захист інформації від непомітної зміни. Під час міжвідомчого обміну криптографічний захист має поєднуватися з правовою оцінкою запиту, оскільки захищений канал підтверджує безпечність передавання, а правомірність доступу визначається законом, компетенцією суб'єкта та службовою метою [34].

Криптографічний захист потребує належного управління ключами, сертифікатами, носіями та строками їх чинності. Компрометація ключа, несвоєчасне відкликання сертифіката, передавання носія іншій особі або відсутність його обліку ставлять під сумнів довіру до електронного повідомлення. У службовому інформаційному обміні це впливає на можливість підтвердити походження, цілісність і незмінність відомостей, які надалі можуть використовуватися під час прийняття правоохоронного рішення.

Механізм *«захисту електронних документів»* охоплює електронний підпис, позначку часу, контроль цілісності, реєстрацію документа, маршрут погодження, збереження версій і можливість відтворення його змісту. Правовий статус електронного документа визначено Законом України «Про електронні документи та електронний документообіг» [65]. У кримінальному провадженні електронний документ має зберігати відомості про автора, час створення або підписання, зміст, реквізити та незмінність після вчинення відповідної процесуальної чи службової дії.

Захист електронних документів повинен забезпечувати збереження їх версій і можливість встановити, який саме документ використовувався під час

прийняття рішення. Проєкт процесуального документа, погоджений документ, підписаний документ і документ, переданий іншому органу, мають різне службове й правове значення. Відсутність історії змін або неможливість відтворити попередню версію ускладнює перевірку змісту рішення, встановлення відповідального виконавця та оцінку законності подальшого використання інформації.

Механізм «*збереження цифрових доказів*» охоплює ідентифікацію, збирання, отримання, копіювання, обчислення контрольних сум, опис умов вилучення, фіксацію технічного середовища, зберігання та передавання електронних матеріалів. У спеціальних настановах щодо поводження з цифровими доказами акцентовано увагу на їх ідентифікації, збиранні, отриманні та збереженні у спосіб, що дозволяє підтвердити цілісність і походження відповідних даних [153]. У європейських практичних рекомендаціях щодо електронних доказів також підкреслюється значення ланцюга збереження, документування кожної дії та можливості подальшої перевірки електронного матеріалу [132].

Збереження цифрових доказів має бути пов’язане з конкретним правоохоронним завданням і процесуальною метою їх використання. Для електронного листування, відеозапису, файлу журналу, образу носія, мобільного пристрою або даних із хмарного сервісу необхідно фіксувати спосіб отримання, формат, метадані, контрольну суму, умови зберігання та осіб, які мали доступ. Така фіксація забезпечує зв’язок між правовою підставою отримання інформації, технічною дією, джерелом походження даних і можливістю їх подальшого використання у кримінальному провадженні.

Механізм «*резервного копіювання і відновлення*» охоплює резервування основних даних, метаданих, журналів доступу, налаштувань прав користувачів, криптографічних ключів, контрольних сум і відомостей про версії. Відновлена система повинна зберігати правовий зв’язок між записом, джерелом, користувачем і попередніми інформаційними операціями. Втрата журналів,

метаданих або історії змін після відновлення може поставити під сумнів достовірність і перевірюваність подальшого використання інформації.

Резервне копіювання має охоплювати також правові метадані. Якщо резервна копія містить основний запис без відомостей про джерело, дату створення, користувача, режим доступу, підставу внесення і журнал змін, відновлена інформація залишається технічно доступною, проте її використання у правоохоронній діяльності ускладнюється з погляду перевірки походження, актуальності та правомірності застосування. У період воєнного стану такий механізм набуває особливого значення для безперервності розшуку, досудового розслідування, фіксації наслідків збройної агресії та збереження цифрових доказів.

Механізм «*реагування на інциденти*» передбачає підготовку, виявлення, повідомлення, оцінювання, локалізацію, усунення причини, відновлення роботи системи та врахування отриманого досвіду. У міжнародних рекомендаціях реагування на інциденти розглядається як керований процес кібербезпеки, що включає послідовні дії з підготовки, аналізу, стримування, усунення наслідків і відновлення [159]. Стандарти управління інцидентами інформаційної безпеки також виходять із необхідності заздалегідь визначених процедур, ролей, порядку повідомлення та документування дій [152].

Реагування на інцидент повинно включати правову оцінку події. Кібератака, компрометація облікового запису, несанкціоноване копіювання, втрата носія або спотворення запису можуть мати ознаки технічної події, дисциплінарного проступку, адміністративного правопорушення або кримінального правопорушення. КК України передбачає відповідальність за кримінальні правопорушення у сфері використання електронно-обчислювальних машин, систем, комп’ютерних мереж і мереж електрозв’язку [43]. Тому реагування має забезпечувати не тільки відновлення працездатності системи, а й фіксацію обставин інциденту, збереження слідів, визначення відповідальних осіб і прийняття процесуального або службового рішення.

Механізм «*управління змінами*» полягає в оцінюванні впливу оновлення програмного забезпечення, підключення нового інформаційного ресурсу, запровадження API, хмарного сервісу або мобільного доступу на режим безпеки, оброблення персональних даних, ведення журналів, розмежування прав користувачів і збереження правового значення інформації. Правові засади надання та використання хмарних послуг визначено Законом України «Про хмарні послуги» [100]. Для органів правопорядку використання таких сервісів має супроводжуватися збереженням державного контролю над службовою інформацією, визначенням місця її оброблення, порядку доступу, резервування, шифрування та відповідальності постачальника послуги.

Управління змінами повинно враховувати сумісність із суміжними інформаційними ресурсами та правові наслідки оновлення. Нове поле в реєстрі, зміна класифікатора, інший формат відповіді або підключення нового каналу обміну можуть спричинити неправильне тлумачення відомостей іншими органами. Тому зміни мають погоджуватися технічним адміністратором, держателем інформації та посадовою особою, відповідальною за її правовий режим. Такий порядок забезпечує зв’язок між технічною зміною, службовою потребою, правовою підставою та подальшим контролем за використанням даних.

Механізм «*контролю автоматизованого аналізу*» передбачає змістовну перевірку результату машинного зіставлення, ризикового профілю, біометричного збігу або автоматизованого сповіщення уповноваженим працівником. У Регламенті ЄС про ШІ особливу увагу приділено високоризиковим системам, застосування яких може впливати на права людини [172]. Автоматизований результат доцільно використовувати як орієнтир для подальшої перевірки, а його врахування у рішенні, що зачіпає права особи, потребує оцінки джерел, якості даних, меж достовірності та службової необхідності.

Контроль автоматизованого аналізу має передбачати фіксацію використаних джерел, ознак, врахованих системою, рівня збігу, обмежень

результату та особи, яка здійснила його перевірку. Машинний висновок без такого пояснення створює ризик сприйняття технічного результату як установленого юридичного факту. Належний контроль дозволяє встановити, чи відповідав автоматизований аналіз правовій підставі, службовій меті, обсягу необхідних даних і допустимим межам подальшого використання інформації.

Механізм «*навчання користувачів*» охоплює підготовку працівників щодо правового режиму інформації, захисту персональних даних, поводження з електронними доказами, використання службових облікових записів, роботи з відкритими джерелами, реагування на інциденти та меж подальшого використання даних. О. В. Таран наголошує на значенні інформаційних технологій у професійній підготовці працівників правоохоронної сфери [113]. Я. В. Свічкарьова пов’язує інформаційну безпеку з професійною компетентністю правоохоронця та його здатністю діяти в інформаційному середовищі з урахуванням правових вимог [105, с. 64-68].

Навчання користувачів має бути періодичним і ситуаційно орієнтованим. Окремі навчальні модулі доцільно спрямовувати на роботу з персональними даними, цифровими доказами, відкритими джерелами, міжнародними запитами, службовими обліковими записами, помилковими записами в реєстрах, втратою пристрою, підозрілим електронним повідомленням і діями під час кібератаки. Така підготовка забезпечує відповідність між повноваженнями працівника, службовою потребою, технічною дією та відповідальністю за використання інформації.

Окремого аналізу потребує захист інформаційних технологій, що використовуються для роботи з відкритими джерелами. Відкритість джерела не змінює правової природи подальшого використання відомостей правоохоронним органом. Якщо інформація з відкритої мережі використовується для орієнтування, достатньою може бути аналітична позначка про її неперевірений характер. Якщо вона має значення для документування правопорушення, необхідними є збереження первинного посилання, часу доступу, технічних ознак файлу, контексту публікації, способу збереження і результатів перевірки.

Особливої обережності потребує робота з фото-, відео- та аудіоматеріалами, отриманими з відкритих джерел у період воєнного стану. Такі матеріали можуть підтверджувати факт обстрілу, місце перебування підрозділів, пошкодження об’єкта, переміщення особи або використання зброї, однак вони можуть бути змонтовані, вирвані з контексту, повторно опубліковані з іншою датою або створені для інформаційного впливу. Тому механізм перевірки має включати встановлення першоджерела, геолокації, часу створення, метаданих, співставлення з іншими відомостями і належне процесуальне оформлення.

М. В. Гуцалюк слушно пов’язує протидію кіберзлочинності під час воєнного стану з необхідністю швидкого реагування на технічні атаки та одночасного документування їх кримінально-правових ознак [16]. З цього випливає, що технічне усунення інциденту не завершує механізм захисту. Правоохоронний орган повинен встановити, чи є ознаки кримінального правопорушення, які дані були змінені або викрадені, кого необхідно повідомити, чи вплинув інцидент на інші системи, чи потрібно обмежити подальше використання певних записів.

Д. Калюжний звертає увагу на проблему захисту інформаційних прав особи в умовах цифровізації правоохоронної діяльності [34]. Наведена позиція важлива для розуміння механізмів захисту, оскільки вони забезпечують збереження інформації в інтересах органу та запобігання неправомірному втручанню в права людини. У разі помилкової ідентифікації, застарілого запису, неправомірного доступу або поширення даних механізм захисту повинен передбачати спосіб виправлення помилки і відновлення правового стану особи.

Отже, *механізми захисту інформаційних технологій у сфері правоохоронної діяльності слід систематизувати за їх функціональним призначенням на превентивні, поточні, моніторингові, реагувальні, відновлювальні, контрольні, механізми службової відповідальності, процесуально-доказові, міжвідомчі та міжнародні*. Узгоджене застосування таких механізмів забезпечує технічну працездатність інформаційних систем, правомірність доступу, захищеність відомостей, перевірюваність інформаційних

операцій і належний рух даних від джерела походження до правоохоронного рішення.

Воєнний стан істотно змінює навантаження на систему захисту інформаційних технологій. У звичайних умовах основна увага зосереджується на стабільному функціонуванні реєстрів, розмежуванні доступу, збереженні цілісності даних і контролі за діями користувачів. У період збройної агресії додаткового значення набувають швидке відновлення доступу до інформаційних ресурсів, захист мобільних пристроїв, резервування каналів зв'язку, переміщення або дублювання серверної інфраструктури, перевірка цілісності даних після кібератак, збереження цифрових доказів воєнних злочинів та підтримання безперервності міжвідомчої взаємодії.

Особливий режим захисту потрібен для інформації про осіб, зниклих безвісти за особливих обставин. Такі відомості поєднують гуманітарне, розшукове, криміналістичне, процесуальне значення і водночас належать до інформації, пов'язаної з персональними даними. Вони можуть охоплювати біометричні дані, ДНК-профілі, фотозображення, опис особливих прикмет, дані родичів, місце останнього перебування, повідомлення військових або цивільних осіб. Помилка в такому масиві здатна спричинити тяжкі моральні, соціальні й процесуальні наслідки, тому порядок роботи з ним має передбачати перевірку джерела, позначення ступеня достовірності, обмеження кола користувачів і фіксацію кожної дії з інформацією.

Захист даних про зброю, боєприпаси та вибухові речовини має забезпечувати актуальність записів, контроль доступу, швидкий пошук, своєчасне оновлення статусу об'єкта і фіксацію всіх інформаційних операцій. Єдиний реєстр зброї функціонує в межах єдиної інформаційної системи МВС [79]. Для органів правопорядку принципове значення має своєчасне відображення відомостей про втрату, вилучення, переміщення, знищення або зміну статусу зброї у суміжних ресурсах, які використовуються під час реагування, розшуку, перевірки осіб і розслідування кримінальних правопорушень.

Інформація про об’єкти критичної інфраструктури потребує поєднання фізичного, кібернетичного, режимного та організаційного захисту. Закон України «Про критичну інфраструктуру» визначає правові та організаційні засади створення і функціонування національної системи захисту критичної інфраструктури [88]. Відомості про такі об’єкти повинні бути доступними для своєчасного реагування уповноважених органів, планування охорони, евакуації та відновлення, але їх поширення має здійснюватися з урахуванням ризиків для обороноздатності, громадської безпеки й безперервності життєво важливих послуг.

Матеріали щодо колаборaційної діяльності, диверсійних загроз і допомоги державі-агресору потребують чіткого розмежування фактичних даних, оперативних повідомлень, показань, відомостей із відкритих джерел, результатів аналітичного зіставлення та припущень. Помилкове позначення особи або некритичне використання неперевіреного повідомлення може вплинути на репутацію, свободу пересування, процесуальний статус і безпеку людини. Тому такі відомості мають містити позначку про джерело, час отримання, ступінь перевіреності, межі використання та відповідального працівника.

Мобільний доступ до інформаційних ресурсів має особливе значення для підрозділів, які працюють на місці події, у прифронтових районах, під час обстрілів, евакуації, розшукових заходів або масових надзвичайних ситуацій. Мобільний пристрій повинен мати шифрування, багатофакторну автентифікацію, віддалене блокування, обмеження копіювання, журналювання, захищений канал зв’язку та визначений порядок дій у разі втрати або компрометації. За відсутності таких умов мобільність перетворюється на джерело витоку службової інформації та втрати контролю за її подальшим використанням.

Використання хмарних сервісів у діяльності органів правопорядку потребує встановлення місця зберігання даних, режиму адміністрування, доступу постачальника, порядку резервування, аудиту, шифрування, видалення та повернення інформації після завершення договору. Закон України «Про

хмарні послуги» створює загальні правові умови використання таких послуг [100]. Для службової інформації визначальним має бути збереження державного контролю над даними, можливість перевірити дії адміністратора, підтвердити цілісність інформації та забезпечити її повернення або знищення у передбаченому порядку.

Біометричні технології потребують підвищених гарантій захисту, оскільки біометричний шаблон, фотозображення, відбитки пальців або генетичні дані дають змогу ідентифікувати особу з високим рівнем точності. Помилковий збіг, низька якість зразка, незаконне повторне використання або передавання таких даних поза визначеною метою можуть мати істотні правові наслідки. Кожна біометрична операція має містити правову підставу, мету, джерело отримання, характеристику якості зразка, результат перевірки, відомості про користувача та посадову особу, яка прийняла рішення про використання результату.

Відеоаналітика вимагає врахування технічних і правових ризиків розпізнавання облич, номерних знаків, маршрутів руху або поведінкових ознак. Автоматизований збіг повинен запускати подальшу перевірку уповноваженим працівником. Для законності правоохоронного рішення важливо зафіксувати результат системи, вихідні дані, час і місце отримання зображення, рівень збігу, додаткові відомості, що підтвердили або спростували результат, а також особу, яка здійснила остаточну оцінку.

Міжнародні цифрові докази потребують збереження походження, цілісності та процесуального значення після транскордонного передавання. У практичних матеріалах Управління ООН з наркотиків і злочинності щодо запитів електронних доказів за кордоном звертається увага на точність запиту, визначення постачальника послуг, категорії даних і належного правового каналу отримання інформації [181]. Для України такі вимоги мають особливе значення під час документування кіберзлочинів, воєнних злочинів і транснаціональних правопорушень, коли помилка у каналі отримання або описі даних може ускладнити їх подальше використання.

3.3. Шляхи запровадження та уніфікації електронної взаємодії правоохоронних органів у питаннях інформаційного забезпечення та використання інформаційних технологій

Запровадження та уніфікація електронної взаємодії правоохоронних органів є необхідним напрямом удосконалення захисту інформаційних технологій. У міжвідомчому обміні найбільш виразно проявляються ризики втрати правового режиму даних, дублювання відомостей, неузгодженості класифікаторів, невизначеності відповідального суб'єкта, помилкового тлумачення запису та неконтрольованого подальшого використання інформації.

З урахуванням усього вищевикладеного у попередніх підрозділах, на нашу думку, під *електронною взаємодією правоохоронних органів варто розуміти нормативно визначений, організаційно погоджений і технічно захищений порядок руху відомостей між суб'єктами правоохоронної діяльності, що забезпечує збереження джерела походження, правової підстави, мети, режиму доступу, ступеня перевіреності, строку актуальності, обмежень використання, журналів операцій і відповідальної сторони*. Наведене дозволяє поєднати швидкість обміну з правовою визначеністю.

У постанові Кабінету Міністрів України № 606 «Деякі питання електронної взаємодії електронних інформаційних ресурсів» визначені питання електронної взаємодії електронних інформаційних ресурсів [21]. У свою чергу, у постанові Кабінету Міністрів України № 357 «Деякі питання організації електронної взаємодії державних електронних інформаційних ресурсів» деталізовано організацію електронної взаємодії державних електронних інформаційних ресурсів [22]. Державне підприємство «ДІЯ» характеризує систему «Трембіта» як засіб електронної взаємодії державних електронних інформаційних ресурсів [20]. Офіційні матеріали Trembita розкривають її призначення як інфраструктури обміну між державними ресурсами [179].

Загальна інфраструктура електронної взаємодії органів правопорядку потребує спеціальних гарантій. ЄРДР, ЄІС МВС, ІПНП, АІС ОП, «іКейс»,

Єдиний реєстр зброї, електронні розшукові обліки, прикордонні ресурси, антикорупційні й економічні аналітичні системи створювалися для різних завдань і різними суб’єктами. Положення про ЄІС МВС визначає загальні засади цієї системи [75]. Положення про ІПНП деталізує функціонування інформаційного порталу Національної поліції [76]. Положення про ЄРДР регулює порядок формування і ведення реєстру досудових розслідувань [74].

Я. В. Ступник, аналізуючи координацію діяльності правоохоронних органів в умовах воєнного стану, слушно звертає увагу на необхідність погодженості дій різних суб’єктів у кризових умовах [111]. У сфері електронної взаємодії така погодженість має виражатися у передачі відомостей із визначеним правовим режимом, метою використання, строком актуальності, рівнем перевіреності та обмеженнями подальшого поширення. За відсутності таких ознак інформаційний обмін втрачає належну керованість, а отримані дані можуть бути використані поза межами первинної мети або без урахування їх фактичної достовірності.

У теоретичному плані уніфікація електронної взаємодії правоохоронних органів може розглядатися у межах двох підходів. Перший пов’язаний із централізованим зосередженням максимальної кількості відомостей в одному інформаційному ресурсі. Його перевагою є швидкість пошуку та спрощення технічного доступу, однак така модель посилює ризики надмірної концентрації даних, дублювання помилок і втрати відповідальності органу, який первинно створив або перевірив інформацію [104, с. 89-90]. Другий підхід ґрунтується на сумісності розподілених систем, у межах яких кожен орган зберігає відповідальність за сформований ним інформаційний масив, а обмін здійснюється за єдиними правовими, організаційними й технічними правилами [42, с. 72]. На нашу думку, для України більш обґрунтованою є саме розподілена модель уніфікованої електронної взаємодії, оскільки дозволяє поєднати міжвідомчу доступність відомостей, відповідальність органу-джерела, захист прав людини та належний контроль за подальшим використанням інформації.

Запровадження такої моделі потребує системного врегулювання кількох взаємопов’язаних напрямів. Насамперед необхідним є ухвалення міжвідомчого нормативно-правового акта, який визначатиме суб’єктів електронної взаємодії, види інформації, підстави і цілі обміну, порядок формування запиту, мінімальні реквізити відповіді, строки опрацювання, підстави відмови, рівні доступу, технічні формати, правила журналювання, відповідальність органу-джерела й органу-користувача, порядок виправлення помилок та реагування на інциденти. Такий акт має встановити мінімальний стандарт інформаційного обміну між органами правопорядку, за якого кожна інформаційна дія буде пов’язана з правовою підставою, службовою потребою та відповідальним суб’єктом.

Наступним елементом має стати інвентаризація інформаційних ресурсів, що використовуються для запобігання, виявлення, припинення і розслідування правопорушень. Вона повинна охоплювати держателів, адміністраторів, категорії даних, правові підстави створення ресурсів, режими доступу, канали обміну, строки зберігання, наявність журналів, установлені обмеження подальшого використання та порядок виправлення помилок. Така інвентаризація дозволить виявити дублювання даних, несумісні класифікатори, застарілі канали обміну, невизначених адміністраторів і ресурси, щодо яких не встановлено належного режиму доступу.

Важливим напрямом є уніфікація класифікаторів, довідників і форматів даних. Одна й та сама подія, особа, транспортний засіб, зброя, документ, місце, ризик або процесуальний статус мають позначатися так, щоб різні системи могли коректно зіставляти відомості без втрати їх правового змісту. Для розшуку особи, обліку зброї, реєстрації кримінального правопорушення, фіксації кіберінциденту або аналізу фінансової операції значення має не тільки назва поля в реєстрі, а його нормативне наповнення, зв’язок із джерелом інформації та допустимі межі використання.

Окремого закріплення потребують правові метадані. Кожна інформаційна одиниця має супроводжуватися відомостями про джерело, дату створення або отримання, правову підставу, мету, категорію інформації, режим доступу,

ступінь перевіреності, строк актуальності, обмеження подальшого використання та відповідального суб’єкта. Якщо дані передаються іншому органу, разом із ними має передаватися і правовий контекст їх використання. Такий порядок запобігає ситуації, коли відомості зберігають технічну доступність, але втрачають зрозуміле походження, мету та межі застосування.

Відповідальність органу-джерела повинна полягати в обов’язку підтримувати актуальність створених або первинно перевірених відомостей і своєчасно повідомляти про їх уточнення, виправлення, скасування або втрату актуальності всіх суб’єктів, яким такі дані були передані. Якщо розшук припинено, біометричний збіг спростовано, запис виправлено або процесуальний статус особи змінено, відповідна інформація має бути доведена до суміжних ресурсів і користувачів, які могли використати попередній запис.

Водночас орган-користувач має нести обов’язок використовувати отримані відомості тільки в межах мети запиту, визначеного провадження, службової перевірки, розшукового завдання або аналітичної роботи. Отримання інформації від іншого органу не повинно перетворюватися на підставу для її необмеженого копіювання, передавання третім суб’єктам або використання в іншому контексті без нової правової підстави. Саме тому доступ за службовою необхідністю має визначатися через поєднання посадової функції, конкретного завдання, категорії інформації та строку її використання.

Журналювання запитів доцільно розглядати як міжвідомчий стандарт електронної взаємодії. Якщо один орган отримує дані з ресурсу іншого органу, журнал має фіксувати користувача, час, правову підставу, мету, категорію даних, результат запиту, обсяг отриманої інформації, обмеження використання та подальші операції. Такий журнал повинен бути доступним для перевірки як держателем ресурсу, так і органом, який використав відповідні відомості.

Уніфікований порядок виправлення помилок має будуватися за логікою інформаційного відкликання. Помилковий або сумнівний запис повинен блокуватися чи позначатися до завершення перевірки, а виправлення має доводитися до всіх органів, які вже отримали відповідні відомості або створили

на їх підставі аналітичні продукти. Похідні аналітичні матеріали повинні містити позначку про зміну первинних даних, оскільки інакше помилка продовжуватиме впливати на подальші правоохоронні рішення.

Кіберзахист електронної взаємодії має охоплювати захист каналів обміну, автентичність повідомлень, контроль цілісності, управління ключами, протидію атакам на доступність, перевірку постачальників і порядок реагування на інциденти. Атака на один ресурс може вплинути на достовірність даних, які вже використані іншим органом, тому реагування на інцидент повинно включати перевірку цілісності переданих відомостей і тимчасове обмеження використання сумнівних записів.

Передавання цифрових доказів між органами потребує збереження контрольної суми, метаданих, опису способу отримання, відомостей про відповідального працівника та процесуального контексту. Передавання файлу без цих ознак знижує можливість подальшої перевірки його походження, цілісності й допустимості. Аналогічні вимоги мають застосовуватися до аналітичних продуктів: аналітична довідка, ризиковий профіль, схема зв’язків або результат автоматизованого зіставлення повинні містити дані про джерела, ступінь перевіреності, припущення аналітика, межі достовірності та обмеження використання.

Територіальна стійкість електронної взаємодії набуває особливого значення в умовах воєнного стану. Переміщення підрозділів, евакуація, зміна підслідності, тимчасове порушення зв’язку або передання матеріалів іншому органу не повинні призводити до втрати історії доступу, версій документів, обмежень використання та відомостей про невирішені інциденти. Для цього потрібні резервні канали, захищений віддалений доступ, відновлення журналів, контроль за мобільними пристроями та чіткий порядок передання інформаційних матеріалів між підрозділами.

Автоматизовані сповіщення і ризикові профілі також потребують окремих правил перевірки. Спрацювання системи щодо особи, транспортного засобу, документа, зброї або маршруту має бути підставою для службової перевірки

уповноваженим працівником. Воно не повинно самостійно визначати факт правопорушення, вину особи або необхідність застосування примусового заходу. У рішенні має бути зафіксовано, хто перевірив спрацювання, які додаткові відомості враховано і чому результат системи був прийнятий або відхилений.

Міжнародний вимір уніфікації електронної взаємодії пов'язаний із принципом еквівалентного захисту. Передавання інформації іншій державі або міжнародній організації має супроводжуватися збереженням правових обмежень, які діяли під час її первинного збирання. Директива (ЄС) 2023/977 встановлює правила обміну інформацією між правоохоронними органами держав-членів ЄС і поєднує оперативність обміну з процедурною визначеністю запиту [142]. Директива (ЄС) 2016/680 визначає спеціальні гарантії оброблення персональних даних компетентними органами з правоохоронною метою [140]. Для України врахування цих положень важливе у процесі європейської інтеграції, розслідування транснаціональних правопорушень, документування воєнних злочинів і налагодження сталого обміну інформацією з міжнародними партнерами.

Уніфікація електронної взаємодії органів правопорядку має враховувати досвід Естонії щодо розподіленого обміну даними [143]. Цінність такого досвіду полягає в організації обміну між інформаційними системами без багаторазового копіювання одного й того самого масиву. Для України відповідна модель може бути корисною за умови збереження спеціального правового режиму правоохоронної інформації, персональних даних, цифрових доказів і відомостей з обмеженим доступом.

У період воєнного стану електронна взаємодія повинна забезпечувати стійкість управління правоохоронними інформаційними ресурсами. Підрозділ, який переміщується, працює в умовах пошкодженої інфраструктури або тимчасового обмеження зв'язку, має отримувати контрольований доступ до необхідних відомостей. Водночас система повинна зберігати журнали доступу,

версії документів, обмеження подальшого використання, відомості про відповідального користувача та дані про невирішені інциденти.

Науково обґрунтованим є підхід, за якого електронна взаємодія органів правопорядку формується на трьох взаємопов'язаних рівнях. Перший рівень становить правова визначеність, що охоплює підстави, мету, суб'єктів, категорії даних і гарантії захисту. Другий рівень утворює організаційна узгодженість, яка передбачає визначення відповідальних осіб, маршрутів обміну, порядку контролю, виправлення помилок і реагування на інциденти. Третій рівень становить технічна сумісність, пов'язана з єдиними форматами, класифікаторами, захищеними каналами, журналюванням, резервуванням і перевіркою цілісності даних.

Отже, запровадження та уніфікація електронної взаємодії органів правопорядку в питаннях інформаційного забезпечення та використання інформаційних технологій має здійснюватися через закріплення єдиного правового порядку руху відомостей. Його зміст повинен охоплювати інвентаризацію ресурсів, уніфікацію класифікаторів, правові метадані, відповідальність органу-джерела, доступ за службовою необхідністю, журналювання, контроль якості, виправлення помилок, реагування на інциденти, захист цифрових доказів і перевірку правомірності інформаційних операцій.

Відтак, міжвідомчий нормативно-правовий акт про порядок електронної інформаційної взаємодії органів правопорядку доцільно прийняти і побудувати за логікою повного циклу роботи з відомостями. У його загальних положеннях мають бути визначені мета акта, коло суб'єктів, види електронної взаємодії, категорії інформації та основні засади обміну: законність, цільове призначення, службова необхідність, пропорційність, достовірність, актуальність, захищеність, простежуваність і відповідальність. Пріоритетність такого напряму підтверджується результатами анкетування, за якими 32,3 % респондентів назвали уніфікацію міжвідомчої електронної взаємодії першочерговим напрямом реформування, 29,3 % – підвищення якості, актуальності та

перевірюваності даних, 20,8 % – кіберзахист і відновлюваність систем, а 17,6 % – підготовку користувачів та розвиток аналітичної спроможності (додаток Б).

Окремого нормативного закріплення потребує статус суб'єктів електронної взаємодії. Доцільно розмежувати орган-джерело, орган-користувач, держателя інформаційного ресурсу, адміністратора системи, відповідального за захист інформації, аналітичний підрозділ, підрозділ внутрішнього контролю та уповноваженого працівника, який використовує відомості у правоохоронному рішенні. Такий розподіл дозволить встановити відповідального суб'єкта на кожному етапі руху інформації та запобігти втраті відповідальності у складних міжвідомчих процесах.

Норми щодо інформаційних ресурсів мають визначати порядок їх інвентаризації, правовий режим, категорії даних, технічні формати, класифікатори, строки зберігання, правила актуалізації і порядок тимчасового обмеження використання. У Законі України «Про публічні електронні реєстри» закріплено загальні засади створення, ведення, взаємодії та адміністрування електронних реєстрів [95]. Водночас інформаційні ресурси органів правопорядку потребують спеціальних гарантій через характер відомостей, які в них обробляються, та можливі наслідки їх використання для прав людини, досудового розслідування, розшуку і публічної безпеки.

Порядок формування запиту має передбачати мінімальні обов'язкові реквізити: суб'єкт запиту, правова підстава, службова мета, категорія інформації, обсяг потрібних відомостей, строк використання, рівень терміновості, обмеження подальшого передавання та посилання на конкретне правоохоронне завдання. Такий порядок дозволить органу-джерелу оцінити допустимість передавання і надати саме той обсяг інформації, який необхідний для виконання визначеної службової мети.

Відомості, що передаються у відповідь на запит, повинні супроводжуватися правовими метаданими. До них доцільно віднести джерело, дату формування, ступінь перевіреності, режим доступу, строк актуальності, обмеження використання та відповідального суб'єкта. Якщо передається

аналітичний продукт, необхідно зазначати використані джерела, метод аналізу, припущення аналітика, рівень підтвердження та межі достовірності висновку.

Підстави відмови або обмеження передавання інформації мають бути чіткими й передбачуваними. До них можуть належати відсутність компетенції, невизначена мета запиту, надмірний обсяг запитуваних відомостей, загроза розкриття державної таємниці, ризик порушення прав людини, відсутність правової підстави або технічна неможливість безпечного передавання. Відмова повинна бути мотивованою і, за можливості, стосуватися тієї частини відомостей, передавання якої є недопустимим.

Журналювання електронної взаємодії має встановлювати єдиний мінімальний склад інформаційного сліду. До нього слід включати дані про користувача, час, ресурс, запит, правову підставу, мету, результат, обсяг доступу, подальше передавання, виправлення, блокування або видалення відомостей. Журналювання повинно бути доступним для контролю, але захищеним від зміни користувачем, дії якого фіксуються.

Порядок виправлення помилок має передбачати позначення сумнівного запису, тимчасове обмеження його використання, перевірку органом-джерелом, повідомлення органів-користувачів і коригування похідних аналітичних продуктів. У разі помилкової ідентифікації, спростування збігу або втрати актуальності запису виправлення повинно мати такий самий міжвідомчий масштаб, як і попереднє поширення відповідних відомостей.

Реагування на інциденти в системі електронної взаємодії має охоплювати повідомлення, локалізацію, обмеження доступу, перевірку цілісності переданих даних, відновлення обміну, службову перевірку і правову кваліфікацію події. Кіберінцидент в одному органі може впливати на правомірність використання відомостей іншими органами, тому міжвідомчий порядок реагування повинен поширюватися на всю систему інформаційної взаємодії.

Міжнародний обмін доцільно врегулювати з урахуванням принципу еквівалентного захисту. Передавання інформації іноземному органу або міжнародній організації повинно супроводжуватися визначенням мети, обсягу,

правового режиму, обмежень подальшого використання і відповідальної сторони. Директива (ЄС) 2023/977 може слугувати орієнтиром щодо поєднання оперативності інформаційного обміну з процедурною визначеністю запиту [142].

Підготовка користувачів міжвідомчих інформаційних ресурсів має бути обов'язковою умовою надання доступу. Вона повинна охоплювати правовий режим даних, службову необхідність, захист персональних даних, роботу з цифровими доказами, використання відкритих джерел, журналювання, порядок повідомлення про помилку або інцидент і відповідальність за неправомірне використання відомостей.

Контроль за електронною взаємодією має передбачати види перевірок, періодичність аудиту, підстави службового розслідування, порядок аналізу журналів, права контролюючих суб'єктів і межі розкриття інформації під час контрольних заходів. Захист службової інформації не повинен перешкоджати перевірці законності доступу, а здійснення контролю має відбуватися з дотриманням таємниці досудового розслідування, оперативної роботи та інших установлених законом обмежень.

Уніфікація електронної взаємодії органів правопорядку має починатися з визначення мінімального стандарту якості даних. Такий стандарт повинен охоплювати точність, повноту, актуальність, наявність джерела, правову підставу, ступінь перевіреності та режим подальшого використання відомостей. Якщо один орган передає іншому неповні, застарілі або належним чином не перевірені дані, технічна швидкість обміну втрачає правоохоронне значення. Тому якість інформації має бути предметом постійного службового контролю протягом усього періоду її використання.

Важливим елементом уніфікації є розмежування первинних даних та аналітичного результату. Первинний запис відображає повідомлення, документ, подію, особу, предмет або дію, тоді як аналітичний результат формується внаслідок зіставлення, групування, оцінювання чи прогнозування. Змішування цих рівнів створює ризик використання аналітичного припущення як установленого факту, що може вплинути на затримання особи, проведення

обшуку, оголошення в розшук, визначення процесуального статусу або прийняття іншого правоохоронного рішення.

Єдиний підхід до службової мети запиту має стати самостійною умовою належної електронної взаємодії. Формулювання мети на зразок «для службового використання» не дає змоги оцінити пропорційність доступу й необхідність отримання конкретного обсягу відомостей. Належною слід вважати таку мету, яка прямо пов’язує запитувані дані з конкретним завданням: перевіркою повідомлення, розшуком особи, встановленням власника зброї, документуванням кіберінциденту, забезпеченням безпеки критичної інфраструктури або виконанням міжнародного доручення.

Окремого нормативного врегулювання потребує електронна взаємодія під час масових подій, надзвичайних ситуацій і воєнних загроз. За таких обставин швидкість доступу до відомостей має особливе значення, однак спрощений доступ повинен бути тимчасовим, мотивованим і зафіксованим у системі. Після завершення невідкладної ситуації необхідною є перевірка обґрунтованості запитів, обсягу отриманих даних і подальшого використання інформації.

Під час воєнного стану особливої ваги набуває обмін інформацією між суб’єктами сектору безпеки і оборони, а відтак уніфікований порядок електронної взаємодії має передбачати спеціальний режим екстреного доступу. Його застосування можливе під час терористичної загрози, диверсії, масованого обстрілу, втечі небезпечної особи, захоплення заручників, кібератаки на критичну інфраструктуру або необхідності негайної ідентифікації загиблих. Екстрений доступ повинен супроводжуватися фіксацією підстави, строку, користувача, обсягу даних і подальшою перевіркою керівником або підрозділом контролю, щоб виняткова процедура не перетворювалася на постійну практику.

Сумісність інформаційних систем не може обмежуватися технічними форматами. Узгодження потребують правові категорії, класифікатори, правила актуалізації, строки зберігання, режими доступу та підходи до аналітичних продуктів. Якщо одна система позначає особу як розшукувану, інша – як таку, що перевіряється, а третя – як особу з ризиковим профілем, працівник повинен

бачити правову різницю між цими статусами та допустимі межі використання кожного з них.

Обов’язковою складовою уніфікованого порядку має бути збереження історії змін. Правоохоронне рішення часто ґрунтується на даних, що змінювалися у часі, тому важливо встановити, який саме запис існував на момент запиту, хто його змінив, на якій підставі та чи були повідомлені користувачі, які раніше отримали відповідні відомості. Відсутність історії змін унеможливлює повну перевірку інформаційного шляху до прийнятого рішення.

Міжвідомчий обмін має враховувати право особи на виправлення недостовірної інформації. Закон України «Про захист персональних даних» передбачає права суб’єкта персональних даних щодо відомостей про себе [84]. Реалізація цього права може мати спеціальні межі, пов’язані з досудовим розслідуванням або оперативно-розшуковою діяльністю, однак можливість виправлення помилки повинна бути нормативно передбачена. За відсутності такого порядку помилковий запис може тривалий час впливати на рішення різних органів.

Для електронної взаємодії важливо визначити співвідношення службового контролю й незалежного нагляду. Внутрішній контроль дозволяє швидко реагувати на порушення, проте здійснюється в межах органу, який сам використовує інформацію. Незалежний нагляд має значення для оцінки системних ризиків, захисту прав людини та перевірки практики доступу до відомостей з підвищеним рівнем захисту. Його організація повинна забезпечувати перевірку законності без розкриття таємниці досудового розслідування, оперативної роботи чи іншої інформації з обмеженим доступом.

Уніфікована електронна взаємодія повинна передбачати спеціальні правила роботи з відомостями про дітей, потерпілих, свідків, заявників, викривачів, внутрішньо переміщених осіб, військовослужбовців та інших осіб, інформація про яких потребує підвищеного захисту. У таких випадках службова необхідність доступу має оцінюватися особливо ретельно, а подальше поширення даних повинно обмежуватися мінімально необхідним обсягом.

Під час обміну інформацією про фінансові операції, корупційні ризики або економічні правопорушення принципове значення має розмежування фактичних даних і ризикових індикаторів. У межах електронної взаємодії аналітичний ризик має використовуватися як підстава для подальшої перевірки, а не як заміна встановленого факту. В антикорупційних розслідуваннях електронна взаємодія має забезпечувати конфіденційність джерел, захист даних про викривачів, контроль доступу до матеріалів і збереження електронних доказів.

Електронна взаємодія потребує періодичного перегляду доступів. Працівники, які тривалий час не працюють із певним ресурсом, змінили посаду або завершили виконання конкретного завдання, повинні втрачати відповідні права доступу. Такий перегляд доцільно здійснювати автоматично за визначеними правилами з подальшим підтвердженням відповідальним керівником, що зменшує ризик накопичення надмірних повноважень.

Уніфікований порядок має передбачати оцінювання ефективності електронної взаємодії. До відповідних показників можуть належати середній час відповіді на запит, частка відмов через неналежне обґрунтування, кількість виявлених помилкових записів, випадки нецільового доступу, інциденти під час передавання даних і строки виправлення помилок. Такі показники повинні ґрунтуватися на реальних журналах, службовій статистиці та результатах контролю, а не на декларативних звітах.

Особливої уваги потребує захист взаємодії з міжнародними партнерами у справах про воєнні злочини та кіберзлочини. Передавання цифрових матеріалів має забезпечувати збереження походження, цілісності, правового режиму, обмежень використання та можливості подальшого застосування в іноземній юрисдикції або міжнародній установі. Помилка у фіксації чи передаванні таких матеріалів може вплинути на їх доказову силу та перспективу використання у відповідному провадженні.

У підсумку уніфікацію електронної взаємодії органів правопорядку слід розглядати як тривалий організаційно-правовий процес, спрямований на створення порядку, за якого відомості рухаються швидко, захищено, з

визначеною метою, збереженням джерела, правового режиму, журналів, відповідальної сторони та можливості виправлення. Такий порядок відповідає сучасним потребам правоохоронної діяльності в умовах воєнного стану та європейської інтеграції.

Уніфікована електронна взаємодія має враховувати різницю між доступом до даних і їх використанням. Доступ означає технічну та правову можливість отримати відомості з певного ресурсу. Використання передбачає включення цих відомостей до перевірки, аналітичного висновку, службової доповіді, матеріалів провадження або правоохоронного рішення. Тому журналювання повинно фіксувати факт отримання інформації та подальші дії з нею, якщо вони впливають на права особи або перебіг виконання правоохоронного завдання.

Повторне використання відомостей потребує окремої правової оцінки. Інформація, отримана для перевірки одного повідомлення, може мати значення для іншого провадження, розшукового заходу або аналітичного дослідження, однак службова доцільність не повинна підміняти правову підставу. Уніфікований порядок має визначати, коли повторне використання є допустимим, хто його погоджує, як воно фіксується та які обмеження зберігаються.

Порядок роботи з помилковими автоматизованими сповіщеннями також має бути врегульований. Якщо система повідомила про збіг щодо особи, документа, транспортного засобу або зброї, а подальша перевірка спростувала цей збіг, інформація про спростування має бути збережена і доведена до пов’язаних ресурсів. Така процедура запобігає повторному виникненню тієї самої помилки в іншому органі або в іншій інформаційній системі.

Під час створення міжвідомчих інформаційних ресурсів необхідно закріпити правило мінімізації даних. Орган повинен отримувати лише той обсяг відомостей, який є достатнім для виконання конкретного правоохоронного завдання. Надмірне передавання повних масивів персональних, біометричних або оперативних даних збільшує ризик витоку, ускладнює контроль і створює передумови для використання інформації поза первинною метою. Принцип

мінімізації узгоджується з європейським підходом до оброблення персональних даних компетентними органами [140]. Обережність у роботі з такими масивами підтверджується результатами опитування: 37,8 % респондентів віднесли біометричні й генетичні дані до найбільш чутливої категорії правоохоронної інформації, 26,8 % – оперативну інформацію та відомості про джерела її походження, а 24,7 % – матеріали досудового розслідування (додаток Б).

Уніфікація електронної взаємодії має враховувати подальше наближення національного законодавства до права Європейського Союзу. Директива NIS2 посилює вимоги до кіберстійкості важливих і критичних суб'єктів [141]. Регламент ЄС про кібербезпеку визначає роль ENISA та європейські підходи до сертифікації кібербезпеки [170]. Для України ці акти мають значення як орієнтири розвитку правового режиму захисту інформаційних технологій, електронної взаємодії та кіберстійкості органів, що виконують правоохоронні завдання.

Узгодження електронної взаємодії має забезпечувати перевірюваність інформаційного сліду. Якщо працівник отримав відомості, використав їх для аналітичної довідки, а надалі така довідка стала підставою для процесуальної або організаційної дії, система повинна дозволяти відтворити послідовність цих операцій. Значення має можливість встановити зв'язок між запитом, отриманою відповіддю, подальшим аналізом і рішенням конкретної посадової особи.

Уніфікований порядок електронної взаємодії повинен містити правила припинення активного використання інформації. Відомості, які втратили актуальність, були спростовані, виправлені або стали непридатними для первинної мети, мають отримувати спеціальну позначку. Така позначка не завжди означає знищення інформації, оскільки окремі дані можуть мати значення для контролю, історії змін або підтвердження факту помилки. Водночас вона повинна обмежувати подальше використання таких відомостей у нових правоохоронних рішеннях.

Для забезпечення реальної уніфікації доцільно встановити єдині правила тестування міжвідомчого обміну перед підключенням нового ресурсу, яке

дозволить перевіряти коректність класифікаторів, повноту правових метаданих, роботу журналів, обмеження доступу, порядок відмови, повідомлення про помилку та збереження обмежень подальшого використання. Без попередньої перевірки навіть належно захищений ресурс може створити ризики через неправильне тлумачення даних іншою системою.

Висновки до розділу 3

1. Обґрунтовано, що форми захисту інформаційних технологій у сфері правоохоронної діяльності слід розглядати як систему зовнішньо визначених правом, організаційними процедурами, режимними правилами, технічними стандартами та службовим контролем способів забезпечення конфіденційності, цілісності, доступності, достовірності, правомірності, контрольованості й відновлюваності інформаційних ресурсів, інформаційно-комунікаційних систем, каналів електронної взаємодії, електронних документів, цифрових доказів, журналів доступу, криптографічних ключів і пов’язаних з ними процедур.

2. Запропоновано класифікувати форми захисту інформаційних технологій у сфері правоохоронної діяльності на правові, організаційні, режимні, технічні, криптографічні, процедурні, кадрові, контрольні, аналітико-перевірочні, відновлювальні, міжнародно-кооперaційні та етичні. Доведено, що їх значення для правоохоронної діяльності полягає у забезпеченні належного режиму поводження з відомостями та правової придатності інформаційної технології для запобігання, виявлення, припинення, документування і розслідування правопорушень. Умови воєнного стану посилюють значення форм, пов’язаних із безперервністю роботи інформаційних систем, збереженням цифрових доказів, захистом персональних і біометричних даних, охороною інформації з обмеженим доступом, відновленням після інцидентів та недопущенням використання спотворених, застарілих або неперевірених відомостей у правоохоронних рішеннях.

3. Встановлено, що механізми захисту інформаційних технологій у сфері правоохоронної діяльності становлять узгоджену послідовність правових, організаційних, технічних, криптографічних, кадрових, аналітико-перевірочних, контрольних, відновлювальних дій, дій реагування та застосування службової відповідальності, за допомогою яких забезпечується належний режим функціонування інформаційних систем і правомірне використання відомостей у правоохоронних рішеннях. До ключових механізмів віднесено ідентифікацію інформаційного активу, оцінку загроз і ризиків, визначення правового режиму інформації, допуск і авторизацію користувача, електронну ідентифікацію, розмежування прав доступу, журналювання операцій, аналіз журналів, створення та підтримання комплексної системи захисту інформації, криптографічний захист, захист електронних документів, збереження цифрових доказів, резервне копіювання, реагування на інциденти, управління змінами, контроль автоматизованого аналізу, навчання користувачів і притягнення винних осіб до відповідальності.

4. Наголошено, що результативність механізмів захисту інформаційних технологій у сфері правоохоронної діяльності залежить від узгодженості між правовою підставою доступу, службовою метою, режимом інформації, діями користувача, технічною можливістю, фіксацією операцій, службовим контролем, відновленням порушеного стану та персоніфікованою відповідальністю. Автоматизовані засоби захисту мають посилювати контроль за інформаційними операціями, проте юридично значуще правоохоронне рішення повинно залишатися мотивованим, персоніфікованим і перевірюваним.

5. Доведено, що запровадження та уніфікація електронної взаємодії правоохоронних органів у питаннях інформаційного забезпечення та використання інформаційних технологій мають здійснюватися через формування нормативно визначеного, організаційно погодженого і технічно захищеного порядку руху відомостей між суб’єктами правоохоронної діяльності. Пріоритетними напрямами такого розвитку визначено ухвалення міжвідомчого нормативно-правового акта про порядок електронної інформаційної взаємодії

правоохоронних органів; інвентаризацію інформаційних ресурсів і каналів обміну; уніфікацію класифікаторів, довідників і форматів; запровадження правових метаданих; закріплення відповідальності органу-джерела за достовірність, повноту й актуальність відомостей; встановлення відповідальності органу-користувача за правомірність доступу, межі використання та подальше передавання даних; доступ за службовою необхідністю; автоматизоване журналювання кожного запиту; єдині правила виправлення помилок; поєднання електронної взаємодії з кіберзахистом; уніфікацію підходів до цифрових доказів; правила створення аналітичних продуктів; територіальну стійкість обміну в умовах воєнного стану; контроль автоматизованих сповіщень і ризикових профілів. Електронна взаємодія повинна забезпечувати швидкість обміну, правову визначеність, збереження режиму інформації, перевірюваність кожної інформаційної операції та поновлення прав особи у разі помилки або неправомірного використання даних.

ВИСНОВКИ

У **дисертації** теоретично узагальнено та розв'язано комплексну науково-прикладну задачу щодо інформаційного забезпечення правоохоронної діяльності з урахуванням умов воєнного стану. До основних сформульованих концептуальних наукових положень, висновків і рекомендацій належать такі:

1. Обґрунтовано, що ефективність інформаційного забезпечення правоохоронної діяльності має оцінюватися не за обсягом накопичених даних, а за якістю їх правового режиму, достовірністю, актуальністю, простежуваністю використання у правоохоронному рішенні та наявністю механізмів персоніфікованої відповідальності за неправомірне або необґрунтоване використання інформації. Запропоновано періодизацію розвитку інформаційного забезпечення правоохоронної діяльності з виокремленням таких етапів: протореєстраційний (від найдавніших часів до сер. XIV ст.), документально-обліковий (сер. XIV ст. – перша пол. XIX ст.), криміналістично-ідентифікаційний (друга половина XIX ст. – 1917 р.), централізовано-картотечний (1917 р. – сер. 1950-х рр.), . автоматизовано-обчислювальний (сер. 1950-х – 1991 р.), національно-інформаційний (1991 р. – 2010 р.) та інтеграційно-цифровий (2011 р. і дотепер). У межах останнього виокремлено воєнно-інтеграційний підетап (з 2022 р.), для якого характерні документування воєнних злочинів, розшук зниклих безвісти, ідентифікація загиблих, протидія диверсійній діяльності й кіберзагрозам, опрацювання значних масивів цифрових і біометричних даних та посилення міжнародного інформаційного обміну.

2. Встановлено, що міжнародно-правові стандарти інформаційного забезпечення правоохоронної діяльності ґрунтуються на поєднанні двох взаємопов'язаних вимог: оперативного обміну інформацією між компетентними органами та правомірного, цільового й контрольованого використання даних із дотриманням принципів законності, пропорційності, якості й актуальності відомостей, доступу за службовою необхідністю, простежуваності інформаційних операцій, незалежного нагляду та подальшої перевірки

правомірності кожного запиту. Для України наукову й практичну цінність становить запровадження сталої системи міжвідомчої інформаційної взаємодії, у якій кожний орган відповідає за достовірність, повноту й актуальність внесених ним відомостей, а доступ до даних здійснюється за визначеними повноваженнями, службовою потребою та з обов'язковою фіксацією інформаційного сліду. Реалізація такого підходу потребує ухвалення міжвідомчого нормативно-правового акта щодо порядку інформаційної взаємодії правоохоронних органів, уніфікації класифікаторів і форматів даних, створення постійного контактного осередку міжнародного інформаційного обміну, запровадження регулярної перевірки якості й актуальності інформації, а також закріплення обов'язкового контролю уповноваженого працівника за результатами автоматизованого аналізу. Такий підхід дасть змогу поєднати оперативність інформаційного обміну з правовою визначеністю, захистом прав людини та доказовою придатністю інформації у правоохоронній діяльності.

3. Обґрунтовано, що електронна готовність правоохоронних органів України є комплексною організаційно-правовою характеристикою їх здатності працювати з інформацією у цифровому середовищі, а її зміст охоплює взаємопов'язані складові: *нормативна* визначає правові підстави створення інформаційного ресурсу, категорії відомостей, що можуть до нього вноситися, коло користувачів, порядок доступу, строки зберігання та гарантії захисту; *організаційна* охоплює розподіл відповідальності між суб'єктами, маршрути руху інформації, порядок міжвідомчої взаємодії, внутрішній контроль і реагування на помилки в інформаційних ресурсах; *технічна* включає програмні, телекомунікаційні, криптографічні та інші засоби, необхідні для безперервності, сумісності й захищеності роботи інформаційних систем; *кадрова* пов'язана із професійною здатністю працівників працювати з цифровими інструментами без порушення правового режиму інформації, службової дисципліни та прав людини; *аналітична* забезпечує перехід від окремого запису чи повідомлення до обґрунтованого висновку, оцінки ризику або інформаційної підстави для прийняття рішення; *безпекова* спрямована на захист інформаційних ресурсів від

витоку, спотворення, втрати, несанкціонованого доступу, неправомірного копіювання та використання поза визначеною правоохоронною метою.

В умовах воєнного стану належний рівень електронної готовності є самостійною умовою правоохоронної спроможності держави, оскільки забезпечує документування воєнних злочинів, розшук зниклих безвісти, ідентифікацію осіб, протидію кіберзагрозам, диверсійній діяльності, незаконному обігу зброї, оперативне реагування та збереження доказової або аналітичної придатності інформації.

4. Встановлено, що інструменти інформаційного забезпечення правоохоронної діяльності становлять функціонально пов’язану систему *нормативно-правових* засобів, які визначають підстави, межі, процедури й відповідальність за роботу з інформацією; *організаційних* засобів, що забезпечують розподіл компетенції, порядок взаємодії, маршрутизацію запитів і контроль виконання; *інформаційно-ресурсних* засобів, які охоплюють реєстри, банки, бази даних, обліки, електронні документи й архіви; *інформаційно-аналітичних* засобів, спрямованих на перетворення даних на аналітичний результат; *техніко-технологічних* засобів, до яких належать програмне забезпечення, мережі, засоби ідентифікації, геоінформаційні системи, відеоаналітика, системи розпізнавання та автоматизованої обробки; *безпекових* засобів, що забезпечують захист інформації та інформаційних систем; *кадрово-методичних* засобів, пов’язаних із професійною підготовкою користувачів інформаційних ресурсів. У сукупності такі засоби забезпечують повний цикл роботи з відомостями.

Результативність інформаційного забезпечення правоохоронної діяльності визначається правомірністю застосування, якістю й актуальністю даних, визначеністю мети, розмежуванням доступу, фіксацією операцій, перевіркою джерел, захистом інформації та обов’язковою оцінкою уповноваженим працівником результатів автоматизованого аналізу. Тому ЄРДР, ЄІС МВС, ІПНП, АІС ОП, «іКейс», спеціалізовані підсистеми, кримінальний аналіз, відкриті джерела, відеоаналітика, біометрична ідентифікація та штучний

інтелект можуть бути належними інструментами лише за умови збереження правового зв’язку між джерелом інформації, способом її оброблення та правоохоронним рішенням.

5. Доведено, що інформаційні повноваження правоохоронних органів України утворюють багатосуб’єктну систему створення, одержання, перевірки, аналізу, передавання, використання і захисту відомостей, необхідних для виконання правоохоронних завдань. Подальший розвиток цієї системи повинен ґрунтуватися на суб’єктно-функціональному підході, за яким орган-джерело відповідає за достовірність, повноту й актуальність внесених даних, орган-користувач – за правомірність доступу та межі використання, орган-аналітик – за обґрунтованість висновку, а орган-координатор – за узгодженість міжвідомчої інформаційної взаємодії. Запропоновано *прийняти міжвідомчий нормативно-правовий акт щодо порядку інформаційної взаємодії правоохоронних органів*, передбачити уніфікацію класифікаторів і форматів даних, фіксацію кожного запиту, регулярну перевірку актуальності записів, захист персональних даних і можливість виправлення помилок.

6. Констатовано, що форми захисту інформаційних технологій у сфері правоохоронної діяльності становлять цілісну систему правових, організаційних, режимних, технічних, криптографічних, процедурних, кадрових, контрольних, аналітико-перевірочних, відновлювальних, міжнародно-кооераційних та етичних способів забезпечення належного режиму роботи з інформаційними ресурсами, системами, електронними документами, цифровими доказами і каналами обміну. Призначення таких форм полягає у забезпеченні конфіденційності, цілісності, доступності, достовірності, правомірності, контрольованості та відновлюваності відомостей, що використовуються для виконання правоохоронних завдань. У період воєнного стану особливого значення набувають захист цифрових доказів, персональних і біометричних даних, інформації з обмеженим доступом, журналів доступу, резервних копій, мобільного доступу та каналів міжвідомчого і міжнародного обміну.

7. Встановлено, що механізми захисту інформаційних технологій у правоохоронній діяльності охоплюють ідентифікацію інформаційного активу, оцінку ризиків, визначення правового режиму інформації, допуск і авторизацію користувача, електронну ідентифікацію, розмежування прав доступу, журналювання, аналіз журналів, створення та підтримання КСЗІ, криптографічний захист, захист електронних документів і цифрових доказів, резервне копіювання, реагування на інциденти, управління змінами, контроль автоматизованого аналізу, навчання користувачів і застосування відповідальності. Доведено, що ці механізми мають забезпечувати стійкий зв'язок між правовою підставою доступу, службовою метою, технічною дією, інформаційним слідом, контролем і персоніфікованою відповідальністю. Автоматизований захист, журналювання та аналітичні інструменти повинні підтримувати правоохоронне рішення, але не замінювати правову оцінку, службову перевірку і відповідальність уповноваженої особи.

8. Науково доведено, що уніфікація електронної взаємодії правоохоронних органів має здійснюватися через закріплення єдиного правового порядку руху інформації між сумісними інформаційними ресурсами. Запропоновано ухвалити міжвідомчий нормативно-правовий акт про порядок електронної інформаційної взаємодії правоохоронних органів, у якому передбачити уніфікацію класифікаторів і форматів, правові метадані, відповідальність органу-джерела й органу-користувача, доступ за службовою необхідністю, журналювання кожного запиту, правила виправлення помилок, захист цифрових доказів, реагування на кіберінциденти та контроль результатів автоматизованого аналізу. Такий порядок має забезпечити швидкий і захищений обмін відомостями, збереження їх правового режиму, перевірюваність походження, можливість відновлення інформаційного сліду та належне використання даних у правоохоронних рішеннях.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Антологія розшуку : у 14 т. / відп. ред. Ю. І. Римаренко, В. І. Кушерець. Київ : Знання України, 2005. Т. 1 : Документи та матеріали з кримінального розшуку (1397–1918 рр.). 596 с.

2. Арістова І. В. Національний механізм реалізації цілей сталого розвитку в умовах інформаційного суспільства в Україні: роль юридичного механізму та його складових. *Сучасна парадигма публічного та приватного права в умовах сталого розвитку:* монографія. Riga, Latvia: Baltija Publishing, 2023. Vol. 1. P. 1-31.

3. Банах С. Інформаційне забезпечення діяльності правоохоронних органів: історико-правовий аналіз. *Актуальні проблеми правознавства*. 2019. Вип. 2. С. 11–16.

4. Батрак К. М. Інформаційне забезпечення правоохоронної діяльності в умовах воєнного стану. *Юридичний науковий електронний журнал.* 2024. № 9. С. 200–203.

5. Батрак К. М. Проблеми та перспективи розвитку інформаційного забезпечення діяльності правоохоронних органів України. *Інтернаука*. 2025. Вип. №6. DOI: https://doi.org/10.25313/2520-2057-2025-6-11101

6. Батрак К. М., Юрах В. М. Термінологічні аспекти поняття «інформаційне забезпечення» та класифікація інформації в прокурорській діяльності. *Future of science: innovations and perspectives:* Proceedings of the 3rd International scientific and practical conference. SSPG Publish. Stockholm, Sweden. 2025. Pp. 348–352.

7. Батрак К. М. Міжнародно-правові засади інформаційного забезпечення правоохоронної діяльності в Україні. *Українська поліцеїстика: теорія, законодавство, практика*. 2026. № 1 (17). С. 132–137.

8. Бєляков К. І. Інформатизація в Україні: проблеми організаційного-правового та наукового забезпечення: монографія. Київ: КВІЦ, 2008. 576 с.

9. Біленчук П. Д., Борисова Л. В., Некрасов В. А. Інформаційна безпека людини, суспільства, держави : монографія. Київ, 2018. URL: https://repositsc.nuczu.edu.ua/handle/123456789/8484.

10. Благута Р. І., Мовчан А. В. Новітні технології у розслідуванні злочинів: сучасний стан і проблеми використання : монографія. Львів : ЛьвДУВС, 2020. 256 с.

11. Бондаренко О. С., Литвиненко Т. О. Історичний розвиток правоохоронних органів: досвід США, Сполученого Королівства та України. *Молодий вчений*. 2018. № 10 (62). С. 216–222.

12. Боняк В. О. Становлення та розвиток правоохоронних органів України: історико-правовий аспект. *Правоохоронна функція держави: теоретико-методологічні та історико-правові підходи дослідження* : матеріали міжкафедрального круглого столу (Харків, 23 жовт. 2012 р.). Харків : ХНУВС, 2012. С. 53–56.

13. Використання інструментів та методів OSINT для отримання пошукової інформації : практ. порадник / Зоренко Д. С., Лех Р. В., Кулик Д. О., Червяков О. І. Х.: ІПЮК для СБУ, 2023. 36 с.

14. Гарбінська-Руденко А. В. Забезпечення інформаційної безпеки правоохоронними органами України. *International Review of Law and Public Administration*. 2025. Вип. 3(20). С. 28–36.

15. Гончарук О. М. Кримінальний аналіз у системі правоохоронних органів України. *Law. State. Technology*. 2023. № 4. С. 3–9.

16. Гуцалюк М. В. Особливості протидії кіберзлочинності під час воєнного стану. *Інформація і право*. 2023. № 3 (46). С. 108–117.

17. Давидов Р. М. Принципи інформаційно-аналітичного забезпечення ОВС України. *Публічне право*. 2016. № 2. С. 203–209.

18. Демчук Т. І. Інформаційно-аналітичні та організаційні методи правоохоронної діяльності. *Науковий вісник Ужгородського національного університету*. Серія: Право. 2025. Вип. 90. Ч. 5. С. 430–436.

19. Департамент інформаційно-аналітичного забезпечення. *Міністерство внутрішніх справ України*. URL: https://mvs.gov.ua/.

20. Державне підприємство «ДІЯ». Система електронної взаємодії державних електронних інформаційних ресурсів «Трембіта». URL: https://se.diia.gov.ua/.

21. Деякі питання електронної взаємодії електронних інформаційних ресурсів : постанова Кабінету Міністрів України від 8 верес. 2016 р. № 606. URL: https://zakon.rada.gov.ua/laws/show/606-2016-%D0%BF.

22. Деякі питання організації електронної взаємодії державних електронних інформаційних ресурсів : постанова Кабінету Міністрів України від 10 трав. 2018 р. № 357. URL: https://zakon.rada.gov.ua/laws/show/357-2018-%D0%BF.

23. Дорошенко Д. І. Нарис історії України : у 2 т. Київ : Глобус, 1991. Т. 1. 238 с.

24. Дуфенюк О. М. Невирішені проблеми та нові виклики використання цифрових технологій у кримінальному провадженні. *Аналітично-порівняльне правознавство*. 2025. № 2. С. 993–1000.

25. Заросило В. О. Порівняльний аналіз адміністративної діяльності міліції України та поліції зарубіжних країн (Сполученого Королівства, США, Канади та Франції) : дис. ... канд. юрид. наук : 12.00.07. Київ, 2002. 250 с.

26. Іванов І. Є. Актуальні питання інформаційної безпеки у діяльності Національної поліції України. *Наукові записки Науково-методичного центру*. 2021. URL: https://journal-nam.com.ua/index.php/journal/article/download/152/146.

27. Ільченко О. В., Корощенко К. Р. Правоохоронні органи як суб’єкти забезпечення кібербезпеки в інформаційному просторі України. *Аналітично-порівняльне правознавство*. 2022. № 1. С. 163–167.

28. Інформаційна безпека України : глосарій / заг. ред. Р. А. Калюжний. Київ : Текст, 2004. 136 с.

29. Інформаційне забезпечення професійної діяльності : навч. посіб. / І. В. Краснобрижий, С. О. Прокопов, Е. В. Рижков. Дніпро : ДДУВС, 2018. 218 с.

30. Інформаційне право України: навч. посіб. / М. В. Ковалів, С. С. Єсімов, О. Г. Ярема. Львів: Львів. держ. ун-т внутр. справ, 2022. 416 с.

31. Інформаційні технології : підручник / І. В. Краснобрижий, С. О. Прокопов, В. Б. Вишня, Е. В. Рижков, К. Ю. Ісмайлов. Дніпро : ДДУВС, 2021. 492 с.

32. Ісмайлов К. Ю. Теоретико-правові підходи до проблем інформаційно-аналітичної діяльності Національної поліції України на сучасному етапі державотворення. *European Reforms Bulletin*. 2019. № 2. С. 109–115.

33. Казанчук І. Д. Особливості правового регулювання діяльності Національної поліції України у сфері забезпечення інформаційної безпеки. *Право і безпека*. 2020. № 1. С. 74-80.

34. Калюжний Д. Захист інформаційних прав особи в умовах цифровізації правоохоронної діяльності. *Науковий вісник Ужгородського національного університету*. Серія: Право. 2025. Вип. 90. Т. 3. С. 214–219.

35. Катеринчук І. П. Правові засади інформаційного забезпечення діяльності правоохоронних органів України : автореф. дис. ... д-ра юрид. наук : 12.00.07. Київ, 2015. 41 с.

36. Квітка С. А. Державне управління формуванням партнерських відносин між владою та бізнесом в умовах соціальних перетворень: монографія. Дніпро : Грані, 2017. 268 с.

37. Коваль Р. А. Інформаційно-аналітичне забезпечення діяльності органів влади : автореф. дис. ... канд. наук з держ. упр. : 25.00.02. Запоріжжя, 2008. 20 с.

38. Колодяжний М. Г. Досвід Великої Британії у використанні громадськості щодо запобігання злочинності. *Форум права*. 2013. № 3. С. 317–323.

39. Конвенція про захист осіб у зв’язку з автоматизованою обробкою персональних даних від 28 січ. 1981 р. URL: https://zakon.rada.gov.ua/laws/show/994_326.

40. Конвенція про кіберзлочинність : міжнародний документ від 23 листоп. 2001 р. URL: https://zakon.rada.gov.ua/laws/show/994_575.

41. Конституція України: Закон від 28 черв. 1996 р. № 254к/96-ВР. URL: http://zakon.rada.gov.ua/laws/show/254к/96-вр.

42. Користін О. Є., Свиридюк Н. П. Оцінювання гібридних загроз та спроможностей протидії їм при формуванні стратегічних комунікацій. *Науковий вісник Ужгородського Національного Університету. Серія: Право*. 2023. Вип. 77. Ч. 2. С. 66–74.

43. Кримінальний кодекс України : Закон України від 05 квіт. 2001 р. № 2341-III. URL: http://zakon3.rada.gov.ua/laws/show/2341-14.

44. Кримінальний процесуальний кодекс України : Закон України від 13 квіт. 2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text.

45. Кудінов В. А., Пакриш О. Є. Інформаційно-аналітичне забезпечення правоохоронної діяльності : навч.-практ. посіб. Київ : Нац. акад. внутр. справ, 2025. 116 с.

46. Кудінов В. А., Яровий К. В. Інформаційне забезпечення правоохоронної діяльності : навч.-практ. посіб. Київ : Нац. акад. внутр. справ, 2024. 120 с.

47. Маковій В. П., Усата Г. О. Інформаційно-аналітична підтримка діяльності поліції як складова інформаційної безпеки держави. *Південноукраїнський правничий часопис*. 2023. № 1. С. 62–66.

48. Маковій В. П., Усата Г. О. Інформаційно-аналітична підтримка діяльності поліції як складова частина системи заходів із забезпечення інформаційної безпеки держави. *Морська безпека та оборона*. 2023. № 1. С. 62–68.

49. Марущак О. А. Правове забезпечення інформаційної безпеки правоохоронних органів. *Актуальні проблеми правознавства*. 2020. № 1. URL: https://aplsp.stu.cn.ua/article/view/228547.

50. Матвієць О. А. Повноваження Бюро економічної безпеки України як елемент його адміністративно-правового статусу. *Науковий вісник*

Ужгородського національного університету. Серія ПРАВО. 2026. Вип. 93. Ч. 3. С. 204–212.

51. Мовчан А. В. Історичні аспекти створення обліково-реєстраційних підрозділів в органах внутрішніх справ. *Право і безпека*. 2009. № 1. С. 53–58.

52. Мовчан А. В. Теоретичні засади інформаційно-аналітичного забезпечення оперативно-розшукової діяльності. *Науковий вісник Національної академії внутрішніх справ*. 2011. № 2. С. 182–193.

53. Моргун Н. С. Щодо визначення поняття інформаційної безпеки у діяльності Національної поліції України. *Аналітично-порівняльне правознавство*. 2024. № 5. URL: https://journal-app.uzhnu.edu.ua/article/view/311033.

54. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. URL: https://tzi.ua/nd_tz_3.7-003_-2005.html.

55. Негодченко О. В. Зміст адміністративно-правових способів і засобів забезпечення обігу інформації підрозділами інформаційно-аналітичного забезпечення та оперативного реагування органів Національної поліції України. *Підприємництво, господарство і право*. 2017. № 3. С. 149-154.

56. Олійничук Р. П. Аналітична діяльність поліції в умовах воєнного стану. *Наукові записки*. Серія: Право. 2025. № 18. URL: https://pravo.cusu.edu.ua/index.php/pravo/article/view/650.

57. Основи кримінального аналізу : підручник / А. М. Бабенко, О. М. Заєць, В. А. Некрасов, К. Ю. Ісмайлов, Д. О. Пефтієв та ін. ; за заг. ред. О. Є. Користіна. Київ, 2020. 296 с.

58. Пеньков С. В. Аналіз організації інформаційно-аналітичного забезпечення діяльності Національної поліції України. *Вісник Харківського національного університету внутрішніх справ*. 2017. № 3 (78). С. 66-73.

59. Петров С. Г. Повноваження СБ України як суб’єкта національної системи кібербезпеки. *Інформація і право*. 2019. № 2(29). С. 100-106.

60. Про Бюро економічної безпеки України : Закон України від 28 січ. 2021 р. № 1150-IX. URL: https://zakon.rada.gov.ua/laws/show/1150-20.

61. Про Державне бюро розслідувань : Закон України від 12 листоп. 2015 р. № 794-VIII. URL: https://zakon.rada.gov.ua/laws/show/794-19.

62. Про Державну прикордонну службу України : Закон України від 3 квіт. 2003 р. № 661-IV. URL: https://zakon.rada.gov.ua/laws/show/661-15.

63. Про державну таємницю : Закон України від 21 січ. 1994 р. № 3855-XII. URL: https://zakon.rada.gov.ua/laws/show/3855-12.

64. Про доступ до публічної інформації : Закон України від 13 січ. 2011 р. № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17.

65. Про електронні документи та електронний документообіг : Закон України від 22 трав. 2003 р. №851-IV. URL: https://zakon.rada.gov.ua/laws/show/851-15.

66. Про електронні комунікації : Закон України від 16 груд. 2020 р. № 1089-IX. URL: https://zakon.rada.gov.ua/laws/show/1089-20.

67. Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 5 жовт. 2017 р. № 2155-VIII. URL: https://zakon.rada.gov.ua/laws/show/2155-19.

68. Про затвердження Інструкції з формування та ведення інформаційної підсистеми «Гарпун» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України» : наказ Міністерства внутрішніх справ України від 13 черв. 2018 р. № 497. URL: https://zakon.rada.gov.ua/laws/show/z0787-18.

69. Про затвердження Інструкції з формування та ведення інформаційної підсистеми «Єдиний облік» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України» : наказ Міністерства внутрішніх справ України від 14 черв. 2019 р. № 508. URL: https://zakon.rada.gov.ua/laws/show/z0739-19.

70. Про затвердження Інструкції з формування та ведення інформаційної підсистеми «СЛІД» інформаційно-комунікаційної системи «Інформаційний

портал Національної поліції України» : наказ Міністерства внутрішніх справ України від 16 берез. 2020 р. № 257. URL: https://zakon.rada.gov.ua/laws/show/z0319-20.

71. Про затвердження Інструкції з формування та ведення інформаційної підсистеми «Custody Records» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України» : наказ Міністерства внутрішніх справ України від 24 трав. 2022 р. № 311. URL: https://zakon.rada.gov.ua/laws/show/z0629-22.

72. Про затвердження Інструкції про порядок використання правоохоронними органами України інформаційної системи Міжнародної організації кримінальної поліції – Інтерпол : наказ МВС України, Офісу Генерального прокурора, НАБУ, СБУ, ДБР, Міністерства фінансів України, Міністерства юстиції України від 17 серп. 2020 р. № 613/380/93/228/414/510/2801/5. URL: https://zakon.rada.gov.ua/laws/show/z0849-20.

73. Про затвердження Положення про автоматизовану інформаційну систему оперативного призначення єдиної інформаційної системи МВС : наказ Міністерства внутрішніх справ України від 20 жовт. 2017 р. № 870. URL: https://zakon.rada.gov.ua/laws/show/z1433-17.

74. Про затвердження Положення про Єдиний реєстр досудових розслідувань, порядок його формування та ведення : наказ Офісу Генерального прокурора від 30 черв. 2020 р. № 298. URL: https://zakon.rada.gov.ua/laws/show/v0298905-20.

75. Про затвердження Положення про єдину інформаційну систему Міністерства внутрішніх справ та переліку пріоритетних електронних інформаційних ресурсів її суб'єктів : постанова Кабінету Міністрів України від 14 листоп. 2018 р. № 1024. URL: https://zakon.rada.gov.ua/laws/show/1024-2018-%D0%BF.

76. Про затвердження Положення про інформаційно-комунікаційну систему «Інформаційний портал Національної поліції України» : наказ

Міністерства внутрішніх справ України від 3 серп. 2017 р. № 676. URL: https://zakon.rada.gov.ua/laws/show/z1059-17.

77. Про затвердження Положення про інформаційну підсистему «Електронна розшукова справа» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України» : наказ Міністерства внутрішніх справ України від 5 лип. 2023 р. № 548. URL: https://zakon.rada.gov.ua/laws/show/z1504-23.

78. Про затвердження Положення про Національний реєстр електронних інформаційних ресурсів : постанова Кабінету Міністрів України від 17 берез. 2004 р. № 326. URL: https://zakon.rada.gov.ua/laws/show/326-2004-%D0%BF.

79. Про затвердження Положення про функціональну підсистему «Єдиний реєстр зброї» єдиної інформаційної системи Міністерства внутрішніх справ : наказ Міністерства внутрішніх справ України від 10 січ. 2022 р. № 2. URL: https://zakon.rada.gov.ua/laws/show/z0090-22.

80. Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах : наказ Адміністрації Держспецзв'язку від 2 груд. 2014 р. № 660. URL: https://zakon.rada.gov.ua/laws/show/z0090-15.

81. Про затвердження Порядку фіксації біометричних даних іноземців та осіб без громадянства під час здійснення прикордонного контролю в пунктах пропуску через державний кордон та у контрольних пунктах в'їзду-виїзду : наказ Міністерства внутрішніх справ України від 24 квіт. 2019 р. № 311. URL: https://zakon.rada.gov.ua/laws/show/z0496-19.

82. Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах : постанова Кабінету Міністрів України від 29 берез. 2006 р. № 373. URL: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF.

83. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 5 лип. 1994 р. № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.

84. Про захист персональних даних : Закон України від 1 черв. 2010 р. № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17.

85. Про інформаційно-телекомунікаційну систему досудового розслідування «іКейс» : наказ Національного антикорупційного бюро України, Офісу Генерального прокурора, Ради суддів України, Вищого антикорупційного суду від 15 груд. 2021 р. № 175/390/57/72. URL: https://zakon.rada.gov.ua/laws/show/v0390886-21.

86. Про інформацію : Закон України від 2 жовт. 1992 р. № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12.

87. Про Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023–2027 роки : Указ Президента України від 11 трав. 2023 р. № 273/2023. URL: https://zakon.rada.gov.ua/laws/show/273/2023.

88. Про критичну інфраструктуру : Закон України від 16 листоп. 2021 р. № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20.

89. Про Національне антикорупційне бюро України : Закон України від 14 жовт. 2014 р. № 1698-VII. URL: https://zakon.rada.gov.ua/laws/show/1698-18.

90. Про Національну поліцію : Закон України від 2 лип. 2015 р. № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19.

91. Про оперативно-розшукову діяльність : Закон України від 18 лют. 1992 р. № 2135-XII. URL: https://zakon.rada.gov.ua/laws/show/2135-12.

92. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовт. 2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19.

93. Про Положення про технічний захист інформації в Україні : Указ Президента України від 27 верес. 1999 р. № 1229/99. URL: https://zakon.rada.gov.ua/laws/show/1229/99.

94. Про прокуратуру : Закон України від 14 жовт. 2014 р. № 1697-VII. URL: https://zakon.rada.gov.ua/laws/show/1697-18.

95. Про публічні електронні реєстри : Закон України від 18 листоп. 2021 р. № 1907-IX. URL: https://zakon.rada.gov.ua/laws/show/1907-20.

96. Про рішення Ради національної безпеки і оборони України від 14 трав. 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26 серп. 2021 р. № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013.

97. Про рішення Ради національної безпеки і оборони України від 15 жовт. 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 28 груд. 2021 р. № 685/2021. URL: https://www.president.gov.ua/documents/6852021-41069.

98. Про систему екстреної допомоги населенню за єдиним телефонним номером 112 : Закон України від 13 берез. 2012 р. № 4499-VI. URL: https://zakon.rada.gov.ua/laws/show/4499-17.

99. Про Службу безпеки України : Закон України від 25 березня 1992 р. № 2229-XII. URL: https://zakon.rada.gov.ua/laws/show/2229-12.

100. Про хмарні послуги : Закон України від 17 лют. 2022 р. № 2075-IX. URL: https://zakon.rada.gov.ua/laws/show/2075-20.

101. Проблеми застосування інформаційних технологій правоохоронними структурами : зб. матеріалів наук.-практ. конф. Львів : ЛьвДУВС, 2018. 281 с. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/2378/1/21_12_2018.pdf.

102. Публічна служба : системна парадигма : кол. монографія / К. О. Ващенко, С. М. Серьогін, Є. І. Бородін та ін. ; за заг. ред. С. М. Серьогіна. Дніпро : ДРІДУ НАДУ, 2017. 256 с.

103. Рижков Е. В. Social networks as interested objects of law-enforcement bodies. *Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs*. 2018. Special Issue. № 2. С. 224-228.

104. Ряполов А. П. Нормативно-правові основи інформаційної безпеки України в умовах гібридної агресії. *Науковий вісник Ужгородського Національного Університету. Серія: Право*. 2025. Вип. 89. Ч. 3. С. 87–91.

105. Свічкарьова Я. В. Сутність інформаційної безпеки в професійній діяльності правоохоронців. *Наукові записки*. Серія: Право. 2023. № 15. С. 64-68.

106. Семенченко А. І. Організаційно-правові механізми державного управління забезпеченням кібернетичної безпеки та кібернетичного захисту України : монографія. Київ, 2020. URL: https://nasplib.isofts.kiev.ua/bitstreams/83ffc73c-b931-41f5-9e9f-a0fd5f32c241/download.

107. Сеник С. В. Адміністративно-правове регулювання діяльності Національної поліції України у сфері обігу інформації з обмеженим доступом : дис. ... канд. юрид. наук : 12.00.07. Львів, 2020. 240 с.

108. Сиза Н. Суди і кримінальне судочинство України в добу Гетьманщини. Київ : Українська видавнича спілка, 2000. 120 с.

109. Статути Великого князівства Литовського : у 3 т. / за ред. С. В. Ківалова, П. П. Музиченка, А. Р. Панькова. Одеса : Юридична література, 2002. Т. 3, кн. 1 : Статут Великого князівства Литовського 1588 року. 672 с.

110. Столітній А. В. Єдиний реєстр досудових розслідувань як частина інформаційної системи кримінального провадження. *Аналітично-порівняльне правознавство*. 2025. № 1. С. 179–186.

111. Ступник Я. В. Координація діяльності правоохоронних органів в умовах воєнного стану. *Науковий вісник Ужгородського національного університету*. Серія: Право. 2026. Вип. 93. Ч. 5. С. 200–206.

112. Судова влада України. *Офіційний веб портал*. URL: https://court.gov.ua/.

113. Таран О. В. Інформаційні технології в правоохоронній діяльності : навч. посіб. Київ : Нац. акад. внутр. справ, 2021. URL: https://elar.navs.edu.ua/bitstreams/28ffc35c-c1e5-4583-8e16-2954c8bdd641/download.

114. Теремецький В. І., Цвірюк Д. В. Застосування зарубіжного досвіду правового захисту персональних даних в Україні. *Часопис Академії адвокатури України*. 2014. № 2 (23). Т. 7. С. 73–82.

115. Терехов В. Питання інформаційно-аналітичних досліджень у сфері правоохоронної діяльності. *Актуальні проблеми правознавства*. 2021. Вип. 3 (27). С. 103–109.

116. Трофименко Є. В. Інформаційно-аналітичне забезпечення Національної поліції України. *Питання сучасної науки і права* : матеріали XII Всеукр. наук.-практ. конф. здобувачів вищої освіти. Суми : Ельдорадо, 2021. С. 247–248.

117. Угода між Україною та Європейським поліцейським офісом про оперативне та стратегічне співробітництво від 14 груд. 2016 р. URL: https://zakon.rada.gov.ua/laws/show/984_001-16.

118. Управління органами Національної поліції України : підручник / за заг. ред. В. В. Сокуренка. Харків : Стильна типографія, 2017. 580 с.

119. Федотов Д. В. Адміністративно-правовий механізм забезпечення інформаційної безпеки в Національній поліції України : дис. ... д-ра філос. : 081. Київ, 2024. 240 с.

120. Федотов Д. В. Поняття адміністративно-правового механізму забезпечення інформаційної безпеки в Національній поліції України. *KELM*. 2023. № 7. С. 386–390.

121. Федчак І. А. Основи кримінального аналізу : навч. посіб. Львів : Львів. держ. ун-т внутр. справ, 2021. 288 с.

122. Фролова О. Г. Проблеми правового регулювання інформаційно-методичного управління в органах внутрішніх справ. *Проблеми правознавства та правоохоронної діяльності*. 2002. № 1. С. 53–62.

123. Хамула П. Особливості становлення та розвитку правоохоронних органів на території України: історичний аспект. *Віче*. 2015. № 4. С. 28–31.

124. Чукут С. А., Полярна В. Л. Основні напрями та пріоритети надання електронних послуг у країнах Європейського Союзу: на прикладі Данії. *Державне управління: удосконалення та розвиток*. 2016. № 10. URL: http://www.dy.nayka.com.ua/?op=1&z=1015.

125. Шепітько В. Ю., Авдєєва Г. К. Інновації в діяльності органів кримінальної юстиції. *Криміналістика і судова експертиза*. 2014. Вип. 59. С. 3-11.

126. Янковська О. Г. До питання ефективності системи інформаційного забезпечення у розкритті та розслідуванні злочинів. *Правова інформатика*. 2010. № 2 (26). С. 78–81.

127. Access to Information Act, R.S.C., 1985, c. A-1. *Justice Laws Website*. URL: https://laws-lois.justice.gc.ca/eng/acts/A-1/.

128. Bundesministerium des Innern. Official website. URL: https://www.bmi.bund.de/.

129. Bundespolizei. Official website. URL: https://www.bundespolizei.de/.

130. CERT-UA. CERT-UA у 2024 році опрацювала 4315 кіберінцидентів. *Державна служба спеціального зв'язку та захисту інформації України*. 2025. URL: https://cip.gov.ua/en/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv.

131. College of Policing. National Decision Model. URL: https://www.college.police.uk/app/national-decision-model/national-decision-model.

132. Council of Europe. Electronic Evidence Guide: A basic guide for police officers, prosecutors and judges. *Strasbourg : Council of Europe*, 2020. URL: https://rm.coe.int/electronic-evidence-guide/1680a0512f.

133. Council of Europe. Practical Guide on the Use of Personal Data in the Police Sector. *Strasbourg : Council of Europe*, 2018. 42 p. URL: https://rm.coe.int/t-pd-201-01-practical-guide-on-the-use-of-personal-data-in-the-police-/16807927d5.

134. Danish Police. Official website. URL: https://politi.dk/en/.

135. Decision No 1719/1999/EC of the European Parliament and of the Council of 12 July 1999 on guidelines for trans-European networks for the electronic interchange of data between administrations. *Official Journal of the European Communities*. 1999. L 203. P. 1–8.

136. Decision No 1720/1999/EC of the European Parliament and of the Council of 12 July 1999 adopting measures to ensure interoperability of and access to trans-

European networks for the electronic interchange of data between administrations. *Official Journal of the European Communities*. 1999. L 203. P. 9–13.

137. Dialogue Police: Experiences, Observations and Opportunities. Stockholm : *Swedish National Police Board*, 2010. 48 p. URL: https://polisen.se/.

138. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Communities*. 1995. L 281. P. 31–50.

139. Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector. *Official Journal of the European Communities*. 1998. L 24. P. 1–8.

140. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities. Official Journal of the European Union. 2016. L 119. P. 89–131. URL: https://eur-lex.europa.eu/eli/dir/2016/680/oj.

141. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022. *Official Journal of the European Union*. 2022. L 333. P. 80-152. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj.

142. Directive (EU) 2023/977 of the European Parliament and of the Council of 10 May 2023 on the exchange of information between the law enforcement authorities of Member States. *Official Journal of the European Union*. 2023. L 134. P. 1–24. URL: https://eur-lex.europa.eu/eli/dir/2023/977/oj.

143. e-Governance Academy. Making Data Run, Not People. Tallinn, 2021. URL: https://ega.ee/wp-content/uploads/2021/08/Broshure_EGOV4Ukraine_EN_F-1.pdf.

144. ENISA. 2024 Report on the State of the Cybersecurity in the Union. Athens : *European Union Agency for Cybersecurity*, 2024. URL: https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union.

145. ENISA. Best Practices for Cyber Crisis Management. Athens : *European Union Agency for Cybersecurity*, 2024. URL: https://www.enisa.europa.eu/publications/best-practices-for-cyber-crisis-management.

146. ENISA. ENISA Threat Landscape 2024. *Athens : European Union Agency for Cybersecurity*, 2024. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

147. ENISA. Good Practice Guide for Incident Management. *Heraklion* : *European Network and Information Security Agency*, 2010. URL: https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management.

148. ENISA. Public administration increasingly targeted by DDoS attacks. *European Union Agency for Cybersecurity*. 2025. URL: https://www.enisa.europa.eu/news/public-administration-increasingly-targeted-by-ddos-attacks.

149. INTERPOL's Rules on the Processing of Data. *Lyon : ICPO-INTERPOL*, 2025. URL: https://www.interpol.int/en/content/download/5694/file/26%20E%20RulesProcessingData_RPD.pdf.

150. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. URL: https://www.iso.org/standard/27001.

151. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection – Information security controls. URL: https://www.iso.org/standard/75652.html.

152. ISO/IEC 27035-1:2023. Information technology – Information security incident management – Part 1: Principles and process. URL: https://www.iso.org/standard/78973.html.

153. ISO/IEC 27037:2012. Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. URL: https://www.iso.org/standard/44381.html.

154. Metropolitan Police Service. Official website. URL: https://www.met.police.uk/.

155. More than 3,000 law enforcement authorities now connected to Europol. Europol. 12 April 2024. URL: https://www.europol.europa.eu/media-press/newsroom/news/more-3-000-law-enforcement-authorities-now-connected-to-europol.

156. Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990. URL: https://www.ontario.ca/laws/statute/90m56.

157. National Crime Information Center. Federal Bureau of Investigation. URL: https://www.fbi.gov/services/cjis/ncic.

158. National Data Exchange (N-DEx). Federal Bureau of Investigation. URL: https://www.fbi.gov/services/cjis/ndex.

159. NIST. Incident Response Recommendations and Considerations for *Cybersecurity Risk Management*. Special Publication 800-61, Revision 3. *Gaithersburg : National Institute of Standards and Technology*, 2025. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf.

160. NIST. Security and Privacy Controls for Information Systems and Organizations. Special Publication 800-53, Revision 5. *Gaithersburg : National Institute of Standards and Technology*, 2020. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

161. NIST. The NIST Cybersecurity Framework (CSF) 2.0. *Gaithersburg : National Institute of Standards and Technology,* 2024. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

162. NIST. Zero Trust Architecture. Special Publication 800-207. *Gaithersburg : National Institute of Standards and Technology*, 2020. URL: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=930420.

163. Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5. *Justice Laws Website*. URL: https://laws-lois.justice.gc.ca/eng/acts/P-8.6/.

164. Polismyndigheten. Official website. URL: https://polisen.se/.

165. Privacy Act, R.S.C., 1985, c. P-21. *Justice Laws Website*. URL: https://laws-lois.justice.gc.ca/eng/acts/P-21/.

166. Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data : CETS No. 223. *Strasbourg : Council of Europe*, 2018. URL: https://rm.coe.int/16808ac918.

167. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Union*. 2016. L 119. P. 1–88. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

168. Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System in the field of border checks. *Official Journal of the European Union*. 2018. L 312. P. 14–55.

169. Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System in the field of police cooperation and judicial cooperation in criminal matters. *Official Journal of the European Union*. 2018. L 312. P. 56–106.

170. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019. *Official Journal of the European Union*. 2019. L 151. P. 15-69. URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj.

171. Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. Official Journal of the European Union. 2024. L 1183. URL: https://eur-lex.europa.eu/eli/reg/2024/1183/oj.

172. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence. *Official*

Journal of the European Union. 2024. L 1689. URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj.

173. Regulation (EU) 2024/982 of the European Parliament and of the Council of 13 March 2024 on the automated search and exchange of data for police cooperation. *Official Journal of the European Union*. 2024. L 982. URL: https://eur-lex.europa.eu/eli/reg/2024/982/oj.

174. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014. *Official Journal of the European Union*. 2014. L 257. P. 73-114. URL: https://eur-lex.europa.eu/eli/reg/2014/910/oj.

175. Roberts A. Two Challenges in Administration of the Access to Information Act. The Public Service and Transparency. 2006. Vol. 2. P. 115–162.

176. Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. *Strasbourg : Council of Europe*, 2022. URL: https://www.coe.int/en/web/cybercrime/second-additional-protocol.

177. Secure Information Exchange Network Application (SIENA). *Europo*l. URL: https://www.europol.europa.eu/how-we-work/services-support/siena.

178. The Swedish Police: An Introduction. *Stockholm : Swedish National Police Board*, 2011. 108 p.

179. Trembita. Electronic interaction system of state electronic information resources. URL: https://trembita.gov.ua/en/about.

180. United Nations. Department of Economic and Social Affairs. E-Government Survey. URL: https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/180-Ukrain

181. UNODC. Practical Guide for Requesting Electronic Evidence Across Borders. *Vienna : United Nations Office on Drugs and Crime*, 2019. URL: https://www.unodc.org.

182. X-tee: Data Exchange Layer. Information System Authority of Estonia. URL: https://www.ria.ee/en/state-information-system/x-tee.

ДОДАТКИ

Додаток А

Акти впровадження

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ДОНЕЦЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

ЗАТВЕРДЖУЮ
Перший проректор
кандидат юридичних наук, професор,
полковник поліції
Олена ВОЛОБУЄВА
«05» 10 2026 року

АКТ
впровадження результатів дисертаційного дослідження в науково-дослідну діяльність Донецького державного університету внутрішніх справ

1. Комісія у складі:
Голова комісії:

Наталя ПАСІЧНИК, начальник відділу організації наукової діяльності, доктор історичних наук, професор;

Члени комісії:

1. Юлія ДАНИЛЕВСЬКА, завідувач відділення аспірантури (ад'юнктури) і докторантури, кандидат юридичних наук, старший науковий співробітник;
2. Тетяна ПОНОМАРЬОВА, завідувач науково-дослідної лабораторії з проблем запобігання кримінальним правопорушенням Навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції імені Е.О. Дідоренка Донецького державного університету внутрішніх справ, доктор юридичних наук, старший дослідник;
3. Ганна БУГА, завідувач кафедри адміністративного права та процесу Навчально-наукового інституту права та соціального менеджменту, доктор юридичних наук, доцент;

2. Комісія встановила:
Результати дисертаційного дослідження Батрака Костянтина Миколайовича на тему: «Інформаційне забезпечення правоохоронної діяльності в Україні» за спеціальністю 262 Правоохоронна діяльність (галузь знань 26

Цивільна безпека / К Безпека та оборона, спеціальність К9 Правоохоронна діяльність) використовуються в науково-дослідній діяльності Донецького державного університету внутрішніх справ під час проведення загальнотеоретичних і галузевих досліджень, спрямованих на розвиток науки правоохоронної діяльності, інформаційного права та інформаційної безпеки в умовах воєнного стану і європейської інтеграції.

У науково-дослідній роботі Донецького державного університету внутрішніх справ використовуються положення щодо:

- запропонованої у дисертаційному дослідженні періодизації розвитку інформаційного забезпечення правоохоронної діяльності в Україні (протореєстраційний, документально-обліковий, криміналістично-ідентифікаційний, централізовано-картотечний, автоматизовано-обчислювальний, національно-інформаційний та інтеграційно-цифровий етапи, у межах останнього – воєнно-інтеграційний підетап);

- авторського визначення поняття «інформаційне забезпечення правоохоронної діяльності» як нормативно врегульованої, організаційно узгодженої й технічно підтримуваної діяльності уповноважених суб'єктів щодо визначення інформаційних потреб, одержання, перевірки, реєстрації, накопичення, систематизації, зберігання, пошуку, зіставлення, аналізу, передавання, використання та захисту відомостей, необхідних для своєчасного, законного й обґрунтованого виконання правоохоронних завдань;

- структурно-функціонального підходу до використання інформації у правоохоронній діяльності, за яким відомості набувають правоохоронного значення за умови проходження повного циклу: визначення інформаційної потреби, встановлення правової підстави одержання, джерела походження і ступеня перевіреності, розмежування доступу, аналітичного опрацювання, фіксації операцій, захисту даних та персоніфікації відповідальності органу-джерела, органу-користувача, органу-аналітика й органу-координатора;

- поняття електронної готовності впровадження сучасних практик інформаційного забезпечення правоохоронної діяльності як стану нормативної, організаційної, кадрової, технічної, аналітичної та безпекової спроможності уповноважених суб'єктів використовувати інформаційні ресурси, інформаційно-комунікаційні системи й цифрові інструменти;

- систематизації інструментів інформаційного забезпечення (нормативно-правові, організаційні, інформаційно-ресурсні, інформаційно-аналітичні, техніко-технологічні, безпекові та кадрово-методичні), форм і механізмів захисту інформаційних технологій у правоохоронній діяльності, а також шляхів уніфікації електронної взаємодії правоохоронних органів, зокрема щодо ухвалення міжвідомчого нормативно-правового акта про порядок електронної інформаційної взаємодії, запровадження правових метаданих, доступу за службовою необхідністю та контролю результатів автоматизованого аналізу;

- результатів анкетування 155 працівників Національної поліції України та 210 працівників закладів вищої освіти системи МВС України (разом 365 респондентів), що підтверджують практичну значущість інформаційного забезпечення, часткову електронну готовність органів, потребу в міжвідомчому

акті про інформаційну взаємодію та обов'язкову перевірку результатів автоматизованого аналізу уповноваженим працівником, включених до наукових матеріалів університету як емпірична база подальших досліджень.

Голова комісії:
_____ **Наталя ПАСІЧНИК**

Члени комісії:
_____ **Юлія ДАНИЛЕВСЬКА**
_____ **Тетяна ПОНОМАРЬОВА**
_____ **Ганна БУГА**

ЗАРЕЄСТРОВАНО
в журналі обліку актів впровадження результатів наукових досліджень в науково-дослідну діяльність
Донецького державного університету внутрішніх справ
«05» 10 2026 р.
Науковий співробітник ВОНР
_____ Терцова І.В.
(підпис, прізвище)

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ДОНЕЦЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

ЗАТВЕРДЖУЮ
Перший проректор
кандидат юридичних наук, професор,
полковник поліції
_____ **Олена ВОЛОБУЄВА**
«27» 10 2026 року

АКТ
впровадження результатів дисертаційного дослідження
в освітній процес Донецького державного університету внутрішніх справ

Комісія у складі:

Голова комісії: Артур ВОЛОБОЄВ, начальник відділу організації освітнього процесу, доктор філософії з права.

Члени комісії:

1. Ольга МЕРДОВА, гарант освітньо-професійної програми «Правоохоронна діяльність (поліцейські)» першого (бакалаврського) рівня вищої освіти за спеціальністю К9 Правоохоронна діяльність галузі знань К Безпека та оборона, кандидат юридичних наук, професор;
2. Ольга ЛИТВИНЕНКО, гарант освітньо-професійної програми «Право (поліцейські)» першого (бакалаврського) рівня вищої освіти за спеціальністю D8 «Право» галузі знань D «Бізнес, адміністрування та право», доктор філософії з права, доцент.
3. Ганна КОНАРЄВА, гарант освітньо-професійної програми «Правоохоронна діяльність» першого (бакалаврського) рівня вищої освіти за спеціальністю К9 Правоохоронна діяльність галузі знань К Безпека та оборона, кандидат юридичних наук;

4. Ольга БОНДАРЕНКО, гарант освітньо-професійної програми «Право» першого (бакалаврського) рівня вищої освіти за спеціальністю D8 «Право» галузі знань D «Бізнес, адміністрування та право, кандидат юридичних наук, доцент.

Комісія встановила:

Результати дисертаційного дослідження Батрака Костянтина Миколайовича на тему: «Інформаційне забезпечення правоохоронної діяльності в Україні» за спеціальністю 262 Правоохоронна діяльність (галузь знань 26 Цивільна безпека / К Безпека та оборона, спеціальність К9 Правоохоронна діяльність) використовуються в освітньому процесі Донецького державного університету внутрішніх справ при викладанні навчальних дисциплін актуальних освітніх програм, розміщених на офіційному сайті університету (https://dnuvs.ukr.education/osvitni-programy), зокрема: ОПП «Правоохоронна діяльність» та ОПП «Правоохоронна діяльність (поліцейські)» першого (бакалаврського) рівня вищої освіти за спеціальністю К9 Правоохоронна діяльність галузі знань К Безпека та оборона; ОПП «Правоохоронна діяльність» другого (магістерського) рівня вищої освіти за спеціальністю К9 Правоохоронна діяльність (зокрема дисципліни «Інформаційно-аналітичне забезпечення правоохоронної діяльності», «Кримінальний аналіз», «Кібербезпека та інформаційно-аналітичне забезпечення правоохоронної діяльності»); ОНП «Правоохоронна діяльність» третього (освітньо-наукового) рівня вищої освіти за спеціальністю К9 / 262 Правоохоронна діяльність, а також при підготовці лекцій, робочих програм і навчально-методичних матеріалів із зазначених дисциплін.

Зокрема в частині:

- представлення генези інформаційного забезпечення правоохоронної діяльності в Україні, міжнародно-правових стандартів і зарубіжного досвіду електронної взаємодії правоохоронних органів, а також сучасного стану інформаційного забезпечення в умовах воєнного стану, цифрової трансформації та європейської інтеграції;
- розкриття змісту інформаційного забезпечення правоохоронної діяльності, поняття електронної готовності правоохоронних органів, інструментів інформаційного забезпечення, повноважень правоохоронних органів щодо створення, одержання, перевірки, аналізу, передавання, використання і захисту відомостей;
- викладення теоретичних основ захисту інформаційних технологій у правоохоронній діяльності, понять і видів форм захисту, механізмів захисту та пріоритетів їх оптимізації;

- визначення шляхів уніфікації електронної взаємодії правоохоронних органів, запровадження правових метаданих, доступу за службовою необхідністю, журналювання запитів, контролю автоматизованого аналізу та збереження цифрових доказів в умовах воєнного стану.

Голова комісії:
_____ Артур ВОЛОБОЄВ

Завідувач науково-дослідної лабораторії з проблем запобігання кримінальним правопорушенням навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції імені Е.О. Дідоренка Донецького державного університету внутрішніх справ, доктор юридичних наук, старший дослідник

_____ Тетяна ПОНОМАРЬОВА

Члени комісії:
_____ Ольга МЕРДОВА
_____ Ольга ЛИТВИНЕНКО
_____ Ганна КОНАРЄВА
_____ Ольга БОНДАРЕНКО

ЗАРЕЄСТРОВАНО
в журналі обліку актів впровадження результатів наукових досліджень в освітній процес
Донецького державного університету внутрішніх справ
«07» жовтня 2026 р.
Науковий співробітник ВОНР Пасічник Н.О.
(підпис, прізвище)

Додаток Б

ЗВЕДЕНІ ДАНІ
опитування 155 працівників Національної поліції України та 210 працівників закладів вищої освіти системи МВС України

Питання та варіанти відповідей	НПУ (155), %	ЗВО системи МВС (210), %	Усього (365), %
1. Як Ви оцінюєте значення інформаційного забезпечення для виконання правоохоронних завдань?			
а) має визначальне значення для своєчасного й обґрунтованого рішення	68,4	61,9	64,7
б) є важливим, але залежить від інших організаційних умов	24,5	30,5	28,0
в) має переважно допоміжне значення	5,2	5,7	5,5
г) важко відповісти	1,9	1,9	1,8
2. Який складник інформаційного забезпечення, на Вашу думку, є найбільш проблемним?			
а) нормативна визначеність порядку доступу й обміну	24,5	34,3	30,1
б) технічна сумісність інформаційних систем	31,0	22,4	26,1
в) якість, актуальність і повнота внесених даних	33,5	28,6	30,7
г) підготовка користувачів інформаційних систем	11,0	14,7	13,1
3. Який підхід до розуміння інформаційного забезпечення є найбільш переконливим?			
а) управлінський, як умова підготовки рішення	18,7	20,0	19,4
б) діяльнісний, як послідовність роботи з відомостями	29,0	24,8	26,6
в) системний, як поєднання правових, організаційних і технічних складників	47,1	50,9	49,3

г) важко відповісти	5,2	4,3	4,7
4. Що найчастіше знижує придатність інформації для використання у правоохоронному рішенні?			
а) відсутність відомостей про джерело походження	26,5	28,1	27,4
б) несвоєчасне оновлення або скасування запису	34,2	27,6	30,4
в) різні формати й класифікатори в інформаційних системах	25,8	25,7	25,7
г) надмірне копіювання відомостей між підрозділами	13,5	18,6	16,5
5. Який історичний етап найбільше вплинув на сучасний стан інформаційного забезпечення правоохоронної діяльності?			
а) формування централізованих відомчих обліків	18,1	15,7	16,7
б) комп’ютеризація правоохоронних баз даних	23,9	18,1	20,6
в) розвиток міжвідомчого інформаційного обміну	31,0	30,5	30,7
г) інтеграційно-цифровий та воєнно-інтеграційний етап	27,0	35,7	32,0
6. Наскільки національне регулювання інформаційного забезпечення відповідає міжнародним стандартам?			
а) переважно відповідає	18,7	16,7	17,5
б) відповідає частково і потребує системного узгодження	62,6	66,2	64,7
в) має істотні прогалини у сфері контролю й відповідальності	15,5	13,8	14,5
г) важко відповісти	3,2	3,3	3,3
7. Яка гарантія є найважливішою під час міжнародного обміну правоохоронною інформацією?			
а) швидкість передавання запиту й відповіді	18,7	11,0	14,3
б) збереження правового режиму та мети	39,4	45,7	43,0

використання даних			
в) відповідальність органу-джерела за якість інформації	25,8	27,1	26,5
г) незалежний контроль за правомірністю обміну	16,1	16,2	16,2
8. Яка зарубіжна модель електронної взаємодії є найбільш корисною для України?			
а) централізовані національні обліки за зразком США	18,1	13,8	15,6
б) федеральна координація зі збереженням компетенції органів за зразком Німеччини	20,6	22,9	21,9
в) розподілений захищений обмін за зразком Естонії	38,7	40,0	39,4
г) поєднання моделей з урахуванням українських умов	22,6	23,3	23,1
9. Як Ви оцінюєте електронну готовність правоохоронних органів України?			
а) достатня для більшості правоохоронних завдань	17,4	14,3	15,6
б) часткова, з істотними відмінностями між органами й підрозділами	59,4	61,0	60,3
в) недостатня через технічні, кадрові та нормативні проблеми	20,0	21,9	21,1
г) важко відповісти	3,2	2,8	3,0
10. Який критерій електронної готовності слід посилювати першочергово?			
а) нормативний	20,6	28,1	24,9
б) технічний	31,0	22,4	26,1
в) кадровий та методичний	25,8	27,6	26,8
г) безпековий і відновлювальний	22,6	21,9	22,2
11. Які інструменти інформаційного забезпечення мають найбільше практичне значення?			
а) електронні реєстри, бази даних та обліки	39,4	32,4	35,4
б) інформаційно-аналітичні інструменти і	28,4	31,9	30,4

кримінальний аналіз			
в) захищені канали міжвідомчої взаємодії	19,4	21,4	20,6
г) кадрово-методичні інструменти навчання користувачів	12,8	14,3	13,6
12. Який недолік відомчих інформаційних ресурсів є найбільш відчутним?			
а) дублювання одних і тих самих відомостей	19,4	20,5	20,0
б) несумісність форматів та класифікаторів	30,3	27,6	28,7
в) різні правила доступу та обміну	27,7	31,4	29,8
г) недостатнє оновлення записів	22,6	20,5	21,5
13. Який принцип роботи з правоохоронною інформацією слід визнати базовим?			
а) законність одержання та використання	30,3	33,8	32,3
б) службова необхідність доступу	22,6	21,0	21,7
в) достовірність, актуальність і повнота даних	30,3	27,6	28,7
г) простежуваність кожної інформаційної операції	16,8	17,6	17,3
14. Чи потрібне обов'язкове зазначення правових метаданих для кожного важливого запису?			
а) так, для всіх правоохоронних інформаційних ресурсів	57,4	64,8	61,7
б) так, але лише для відомостей з обмеженим доступом	28,4	23,8	25,8
в) ні, достатньо загальних реквізитів системи	8,4	5,2	6,6
г) важко відповісти	5,8	6,2	5,9
15. Чи доцільно ухвалити міжвідомчий нормативно-правовий акт про порядок електронної інформаційної взаємодії правоохоронних органів?			
а) так, це необхідна умова узгодження обміну	70,3	76,2	73,7
б) так, але лише після інвентаризації наявних ресурсів	20,0	15,7	17,5
в) ні, достатньо чинних відомчих актів	5,8	4,3	4,9

г) важко відповісти	3,9	3,8	3,9
16. Хто повинен нести первинну відповідальність за достовірність і актуальність переданих відомостей?			
а) орган-джерело	60,6	63,8	62,4
б) орган-користувач	12,3	8,6	10,2
в) адміністратор інформаційної системи	16,8	14,3	15,4
г) відповідальність має бути спільною залежно від операції	10,3	13,3	12,0
17. Як слід визначати доступ до інформаційних ресурсів?			
а) за посадою працівника	12,3	8,6	10,2
б) за належністю до конкретного органу	7,7	5,7	6,5
в) за службовою необхідністю і конкретним завданням	68,4	73,3	71,2
г) за рішенням безпосереднього керівника без додаткової фіксації	11,6	12,4	12,1
18. Яке значення має журналювання доступу до інформаційних ресурсів?			
а) забезпечує персоніфікацію дій користувача	31,6	28,1	29,6
б) створює підстави для службового контролю	27,1	26,7	26,9
в) дає можливість перевірити законність використання даних	34,2	39,0	37,0
г) має переважно технічне значення	7,1	6,2	6,5
19. Як слід використовувати результати автоматизованого аналізу або біометричного збігу?			
а) як остаточну підставу для рішення	3,2	1,9	2,5
б) як орієнтир, що потребує перевірки уповноваженим працівником	78,1	82,4	80,6
в) лише як статистичний матеріал	10,3	8,1	9,0
г) важко відповісти	8,4	7,6	7,9
20. Яким має бути використання відкритих джерел інформації у правоохоронній діяльності?			

а) вільним, оскільки джерела є відкритими	7,1	5,7	6,3
б) допустимим лише із зазначенням джерела, часу доступу та ступеня перевірки	61,3	66,2	64,1
в) допустимим переважно для орієнтування	23,9	20,5	21,9
г) недоцільним через ризик недостовірності	7,7	7,6	7,7
21. Яка категорія даних потребує найбільш обережного режиму оброблення?			
а) біометричні та генетичні дані	36,1	39,0	37,8
б) відомості досудового розслідування	25,2	24,3	24,7
в) оперативна інформація та дані про джерела	28,4	25,7	26,8
г) статистичні й узагальнені дані	10,3	11,0	10,7
22. Які форми захисту інформаційних технологій мають пріоритетне значення?			
а) правові й режимні	25,2	31,4	28,8
б) технічні та криптографічні	27,7	21,9	24,4
в) організаційні й контрольні	28,4	27,1	27,7
г) кадрові, аналітико-перевірочні та етичні	18,7	19,6	19,1
23. Який механізм захисту інформаційних технологій потребує першочергового посилення?			
а) оцінка загроз і ризиків	18,7	20,5	19,7
б) розмежування прав доступу й електронна ідентифікація	29,0	27,1	27,9
в) аналіз журналів і службовий контроль	26,5	24,8	25,5
г) резервне копіювання та відновлення після інцидентів	25,8	27,6	26,9
24. Яка загроза в умовах воєнного стану є найбільш небезпечною для інформаційних технологій правоохоронних органів?			
а) кібератаки на інформаційні системи та канали зв’язку	34,8	31,9	33,1
б) втрата або пошкодження обладнання й носіїв	18,1	15,2	16,4
в) несанкціонований доступ або витік службової інформації	31,6	35,2	33,7

г) використання застарілих або спотворених даних	15,5	17,7	16,8
25. Що має бути обов'язковим під час резервного відновлення інформаційних систем?			
а) відновлення лише основних записів	5,2	3,8	4,4
б) відновлення записів разом із журналами, метаданими та правами доступу	72,9	76,7	75,1
в) відновлення тільки після завершення службової перевірки	12,3	10,0	11,0
г) важко відповісти	9,6	9,5	9,5
26. Що є головною умовою збереження цифрових доказів?			
а) швидке копіювання файлів	11,0	8,1	9,3
б) фіксація джерела, способу отримання, контрольної суми та ланцюга збереження	68,4	74,3	71,8
в) передавання матеріалів до іншого органу	7,7	5,7	6,5
г) використання лише паперової копії електронного документа	12,9	11,9	12,4
27. Яке значення має криптографічний захист у міжвідомчій взаємодії?			
а) підтверджує походження й цілісність електронного повідомлення	44,5	43,8	44,1
б) забезпечує конфіденційність передавання	29,0	26,7	27,7
в) замінює правову оцінку запиту	3,9	2,4	3,0
г) має значення лише для державної таємниці	22,6	27,1	25,2
28. Як має оцінюватися застосування відеоаналітики та біометричних технологій?			
а) за технічною точністю системи	14,8	10,5	12,3
б) за наявністю правової підстави, мети, якості зразка і перевірки результату	66,5	72,4	69,9
в) за кількістю отриманих збігів	7,7	5,2	6,3
г) за рішенням адміністратора системи	11,0	11,9	11,5
29. Який напрям підготовки користувачів інформаційних систем є найважливішим?			

а) технічні навички роботи з інтерфейсом	18,1	14,3	15,9
б) правовий режим даних і службова необхідність доступу	37,4	42,9	40,6
в) реагування на кіберінциденти та втрату пристрою	22,6	20,9	21,6
г) робота з цифровими доказами та відкритими джерелами	21,9	21,9	21,9
30. Який напрям реформування інформаційного забезпечення правоохоронної діяльності є першочерговим?			
а) уніфікація міжвідомчої електронної взаємодії	31,0	33,3	32,3
б) підвищення якості, актуальності та перевірюваності даних	30,3	28,6	29,3
в) посилення кіберзахисту й відновлюваності систем	21,9	20,0	20,8
г) системна підготовка користувачів і розвиток аналітичних підрозділів	16,8	18,1	17,6

Додаток В

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

в яких опубліковані основні наукові результати дисертації:

1. Батрак К. М. Інформаційне забезпечення правоохоронної діяльності в умовах воєнного стану. *Юридичний науковий електронний журнал.* 2024. № 9. С. 200–203.

DOI: https://doi.org/10.32782/2524-0374/2024-9/44

2. Ковальова О. В., Батрак К. М. Міжнародно-правові засади інформаційного забезпечення правоохоронної діяльності в Україні. *Українська поліцеїстика: теорія, законодавство, практика*. 2026. № 1 (17). С. 132–137. (Особистий внесок здобувача: досліджено європейський досвід правового регулювання інформаційних відносин та механізми адаптації стандартів ЄС (GDPR, директиви щодо персональних даних і транс'європейських мереж) до інформаційного забезпечення правоохоронної діяльності в Україні).

DOI: https://doi.org/10.32782/2709-9261-2026-1-17-22

3. Батрак К. М. Інструменти інформаційного забезпечення правоохоронної діяльності в Україні. *Вісник кримінологічної асоціації України*. 2025. № 3(36). С. 668–679.

DOI: https://doi.org/10.32631/vca.2025.3.58

які засвідчують апробацію матеріалів дисертації:

4. Батрак К. М., Юрах В. М. Термінологічні аспекти поняття «інформаційне забезпечення» та класифікація інформації в прокурорській діяльності. *Future of science: innovations and perspectives:* Proceedings of the 3rd International scientific and practical conference. SSPG Publish. Stockholm, Sweden. 2025. Pp. 348–352.

DOI: https://sci-conf.com.ua/wp-content/uploads/2025/01/FUTURE-OF-SCIENCE-INNOVATIONS-AND-PERSPECTIVES-26-28.01.25.pdf

5. Ковальова О. В., Батрак К. М. Організація правоохоронної діяльності в європейських державах: кращі практики. *European congress of scientific discovery:* Proceedings of the 2nd International scientific and practical conference. Barca Academy Publishing. Madrid, Spain. 2025. Pp. 344–349.

DOI: https://sci-conf.com.ua/wp-content/uploads/2025/02/EUROPEAN-CONGRESS-OF-SCIENTIFIC-DISCOVERY-3-5.02.25.pdf

6. Батрак К. М. Європейські стандарти інформаційного забезпечення правоохоронної діяльності. *Актуальні проблеми юридичної науки та практики у воєнний період*: міжнар. наук.-практ. конф. (Львів, 10 жовт. 2025 р.). Львів. Торунь : Liha-Pres, 2025. С. 177–181.

DOI: https://doi.org/10.36059/978-966-397-550-4-52

які додатково відображають наукові результати дисертації:

7. Батрак К. М. Проблеми та перспективи розвитку інформаційного забезпечення діяльності правоохоронних органів України. *Інтернаука*. 2025. Вип. №6. С. 131–136.

DOI: https://doi.org/10.25313/2520-2057-2025-6-11101