МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ

Кваліфікаційна наукова
праця на правах рукопису

МОІСЕЄВ МАКСИМ ГЕННАДІЙОВИЧ

УДК 343.98:004.056:343.35

ДИСЕРТАЦІЯ
ОСНОВИ МЕТОДИКИ РОЗСЛІДУВАННЯ НЕЗАКОННОГО ВТРУЧАННЯ В РОБОТУ АВТОМАТИЗОВАНИХ СИСТЕМ В ОРГАНАХ ТА УСТАНОВАХ СИСТЕМИ ПРАВОСУДДЯ

08 – Право
081 – Право

Подається на здобуття наукового ступеня доктора філософії

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

Науковий керівник: **Зарубей Вікторія Володимирівна,**
кандидат юридичних наук, професор

Київ – 2026

АНОТАЦІЯ

Моісеєв М.Г. Основи методики розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя – *Кваліфікаційна наукова праця на правах рукопису.*

Дисертація на здобуття ступеня доктора філософії за спеціальністю 081 – Право. – Національна академія внутрішніх справ, Київ, 2026.

Дисертаційне дослідження присвячене комплексному аналізу теоретичних і прикладних засад розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя, а також обґрунтуванню сучасних підходів до формування криміналістичної методики виявлення, розкриття та досудового розслідування відповідних кримінальних правопорушень. Робота виконана у контексті трансформації кримінального процесуального законодавства України та активного впровадження цифрових технологій у діяльність судової влади.

Актуальність теми зумовлена інтенсивним розвитком електронного судочинства, широким використанням автоматизованих систем документообігу, електронних реєстрів, цифрових сервісів та інформаційних платформ у діяльності органів правосуддя. Ці процеси суттєво підвищили ефективність, оперативність і прозорість судового провадження, однак одночасно сформували нові ризики, пов’язані з можливістю несанкціонованого втручання у функціонування інформаційних систем. Такі посягання становлять підвищену суспільну небезпеку, оскільки здатні впливати на достовірність процесуальної інформації, порядок розподілу справ, рух судових документів і загалом на авторитет правосуддя.

У дисертації встановлено, що електронне судочинство являє собою складну організаційно-правову та інформаційно-технологічну систему, у межах якої забезпечується створення, обробка, передавання, зберігання та використання процесуально значущих даних.

У роботі доведено, що незаконне втручання в роботу автоматизованих систем у сфері правосуддя має складний, багатоелементний характер і

формується під впливом технічних, організаційних та людських чинників. Такі кримінальні правопорушення, як правило, не є випадковими, а характеризуються попередньою підготовкою, використанням легітимного або службового доступу до систем, а також високим рівнем адаптації до цифрового середовища. Найбільш поширеними формами протиправної поведінки є несанкціоноване втручання в інформаційні ресурси, внесення недостовірних відомостей, використання сторонніх облікових записів, модифікація або видалення електронних даних, а також інші дії, спрямовані на порушення нормального функціонування систем.

Встановлено, що приховування незаконного втручання в роботу автоматизованих систем у сфері правосуддя зазвичай здійснюється шляхом внесення до системи недостовірних або змінених даних, використання чужих облікових записів або спільного використання засобів авторизації, видалення чи модифікації файлів, електронних записів або журналів подій, створення фіктивних службових документів для формального пояснення змін у системі, інсценування технічних збоїв чи помилок програмного забезпечення, а також перекладання відповідальності на інших працівників або сторонніх осіб. Зазначене дає підстави стверджувати, що спосіб учинення відповідного кримінального правопорушення охоплює не лише дії з безпосереднього протиправного впливу на систему, а й комплекс підготовчих і маскувальних заходів, спрямованих на унеможливлення або істотне ускладнення виявлення факту втручання та встановлення винної особи.

Окрему увагу приділено характеристиці слідової картини зазначених кримінальних правопорушень. Встановлено, що вона має переважно цифровий характер і проявляється у вигляді лог-файлів, журналів подій, записів авторизації користувачів, метаданих змін у базах даних, слідів мережевої активності, а також ознак використання спеціалізованого програмного забезпечення або сторонніх технічних засобів. У ряді випадків цифрові сліди доповнюються матеріальними та документальними джерелами інформації, що можуть свідчити про наявність

корупційних зв’язків, неправомірної вигоди або змови між учасниками протиправної діяльності.

Наведено типовий перелік обставин, що підлягають встановленню в кримінальних провадженнях цієї категорії, а саме: 1) подія кримінального правопорушення, зокрема час, місце, обстановка, спосіб і конкретна форма незаконного втручання в роботу автоматизованої системи, характер змін, що були внесені до інформації чи програмного середовища, а також особливості функціонування органу або установи системи правосуддя, в межах яких відбулося відповідне втручання; 2) обставини, що характеризують автоматизовану систему як об’єкт незаконного впливу, зокрема її функціональне призначення, режим доступу, коло користувачів, порядок адміністрування, наявність засобів захисту інформації, технічні та програмні характеристики, а також види даних, щодо яких було здійснено протиправний вплив; 3) особа, яка вчинила кримінальне правопорушення, форма її вини, мотив, мета, наявність спеціальних знань, службового чи іншого доступу до системи, а також зв’язок такої особи з органом або установою системи правосуддя чи з іншими особами, які могли сприяти вчиненню втручання; 4) наслідки незаконного втручання, зокрема вид і обсяг завданої шкоди, характер порушення нормального функціонування автоматизованої системи, можливе блокування, підроблення, знищення, модифікація, копіювання або витік інформації, а також вплив таких наслідків на здійснення судочинства, документообіг, розподіл справ, доступ до інформації чи реалізацію процесуальних прав учасників проваджень; 5) обставини, які впливають на ступінь тяжкості вчиненого кримінального правопорушення, характеризують особу підозрюваного чи обвинуваченого, обтяжують або пом’якшують покарання, свідчать про наявність групового способу вчинення, повторності, використання службового становища, спеціальних технічних засобів або інших кваліфікуючих ознак, а також виключають кримінальну відповідальність чи є підставою для закриття кримінального провадження; 6) обставини, що підтверджують використання технічних пристроїв, програмних засобів, облікових записів, серверного

обладнання, носіїв інформації або інших засобів як знаряддя чи засобів учинення кримінального правопорушення, а також можливість їх вилучення, арешту, спеціальної конфіскації чи використання для подальшого експертного дослідження; 7) обставини, що свідчать про наявність підстав для застосування до юридичних осіб заходів кримінально-правового характеру, якщо незаконне втручання було вчинене в їх інтересах, від їх імені або уповноваженими особами з використанням їх організаційних, технічних чи фінансових можливостей.

Доведено, що найбільш значущими напрямами взаємодії є взаємодія слідчого з прокурором, оперативними підрозділами, спеціалістами та експертами у сфері комп'ютерної техніки, захисту інформації й телекомунікацій, а також з органами та установами системи правосуддя, суб'єктами технічного адміністрування, операторами електронних комунікацій та іншими особами, які можуть володіти інформацією, необхідною для встановлення обставин кримінального правопорушення.

У дисертації акцентовано увагу на значенні початкового етапу досудового розслідування, де ключову роль відіграють огляд місця події, комп'ютерної техніки, серверного обладнання, автоматизованих робочих місць, мережевої інфраструктури та системних журналів. Наголошено, що своєчасне та якісне проведення таких слідчих (розшукових) дій є критично важливим для збереження динамічних цифрових даних, запобігання їх зміні або втраті, а також для формування первинної доказової бази у провадженні.

Доведено, що обшук у кримінальних провадженнях зазначеної категорії має специфічний пошуково-тактичний характер, оскільки спрямований не лише на виявлення матеріальних об'єктів, а насамперед на ідентифікацію прихованих цифрових носіїв інформації, технічних засобів доступу, службових документів і пристроїв, що можуть містити сліди втручання або використовуватися для його здійснення. Ефективність цієї слідчої (розшукової) дії значною мірою залежить від дотримання вимог раптовості, оперативності, координації дій слідчо-оперативної групи та запобігання дистанційному знищенню електронної інформації.

У роботі встановлено, що допит у провадженнях про незаконне втручання в роботу автоматизованих систем потребує врахування як процесуальних, так і технічних аспектів. Йдеться про необхідність з'ясування особливостей функціонування інформаційних систем, порядку доступу до них, ролі конкретних користувачів, а також механізму вчинення можливих змін у даних. Ефективність допиту визначається правильним формулюванням запитань, урахуванням професійної специфіки допитуваних осіб та подоланням типових захисних версій щодо технічних збоїв або відсутності причетності.

Значне місце у дослідженні відведено використанню спеціальних знань у формі судових експертиз і залучення спеціалістів. Обґрунтовано необхідність призначення комп'ютерно-технічних експертиз, експертиз у сфері телекомунікаційних систем, інформаційної безпеки, технічного захисту інформації, а також інших видів досліджень залежно від обставин конкретного провадження. Застосування спеціальних знань дає змогу встановити механізм втручання, джерела доступу до системи, характер змін інформації та зв'язок між технічними діями і конкретною особою.

Узагальнено, що підвищення ефективності розслідування незаконного втручання в роботу автоматизованих систем у сфері правосуддя можливе за умови комплексного вдосконалення організаційних засад взаємодії між слідчими, прокурорами, спеціалістами та експертними установами, а також належного нормативного забезпечення відповідної діяльності. Результати дослідження спрямовані на підвищення якості досудового розслідування, удосконалення криміналістичної практики та забезпечення надійного захисту інформаційної інфраструктури правосуддя.

Ключові слова: автоматизовані системи, електронне судочинство, документи, криміналістична методика, досудове розслідування, кримінальне провадження, цифрові сліди, кіберзлочинність, обшук, огляд, допит, спеціальні знання, судова експертиза.

ANNOTATION

Moisieiev M.H. Fundamentals of the Methodology for Investigating Unauthorized Interference with Automated Systems in Bodies and Institutions of the Justice System – *Qualifying Scientific Work as a Manuscript*.

Dissertation for the Degree of Doctor of Philosophy in Specialty 081 – Law. – National Academy of Internal Affairs, Kyiv, 2026.

The dissertation research is devoted to a comprehensive analysis of the theoretical and applied foundations for investigating unlawful interference with the operation of automated systems within bodies and institutions of the justice system, as well as to substantiating contemporary approaches to the development of a forensic methodology for the detection, disclosure, and pre-trial investigation of the relevant criminal offenses. The study was conducted in the context of the transformation of the criminal procedural legislation of Ukraine and the active implementation of digital technologies in the functioning of the judiciary.

The relevance of the topic is determined by the intensive development of e-justice, the widespread use of automated document management systems, electronic registers, digital services, and information platforms in the activities of judicial authorities. These processes have significantly increased the efficiency, promptness, and transparency of judicial proceedings; however, at the same time, they have created new risks associated with the possibility of unauthorized interference with the functioning of information systems. Such encroachments pose an increased public danger, as they may affect the reliability of procedural information, case allocation procedures, judicial document circulation, and ultimately the authority and integrity of the justice system.

The dissertation establishes that e-justice constitutes a complex organizational, legal, and information-technological system within which the creation, processing, transmission, storage, and use of procedurally significant data are ensured.

The study demonstrates that unlawful interference with the operation of automated systems in the sphere of justice possesses a complex and multi-component nature formed under the influence of technical, organizational, and human factors. As a rule, such criminal offenses are not random in nature but are characterized by prior

preparation, the use of legitimate or official access to systems, and a high degree of adaptation to the digital environment. The most common forms of unlawful conduct include unauthorized interference with information resources, insertion of false information, use of third-party user accounts, modification or deletion of electronic data, as well as other actions aimed at disrupting the normal functioning of systems.

It has been established that concealment of unlawful interference with the operation of automated systems in the justice sector is usually carried out through the insertion of false or altered data into the system, the use of other persons' accounts or shared authentication tools, deletion or modification of files, electronic records, or event logs, creation of fictitious official documents to formally justify changes within the system, simulation of technical failures or software malfunctions, and shifting responsibility to other employees or third parties. This provides grounds to conclude that the method of committing such criminal offenses encompasses not only direct unlawful influence on the system but also a set of preparatory and concealment measures aimed at preventing or significantly complicating the detection of interference and identification of the offender.

Particular attention is devoted to the characteristics of the trace pattern of these criminal offenses. It has been established that such a pattern predominantly has a digital nature and manifests itself in the form of log files, event logs, user authentication records, metadata regarding database modifications, traces of network activity, and indicators of the use of specialized software or external technical devices. In certain cases, digital traces are supplemented by material and documentary sources of information that may indicate the existence of corrupt connections, undue advantages, or collusion among participants in unlawful activities.

A typical list of circumstances subject to establishment in criminal proceedings of this category is provided, namely: (1) the event of the criminal offense, including the time, place, circumstances, method, and specific form of unlawful interference with the operation of an automated system, the nature of modifications made to information or software environments, and peculiarities of the functioning of the justice body or institution within which such interference occurred; (2) circumstances characterizing

the automated system as an object of unlawful influence, including its functional purpose, access regime, circle of users, administration procedures, information security measures, technical and software characteristics, as well as the categories of data subjected to unlawful impact; (3) the identity of the offender, the form of guilt, motive and purpose, possession of specialized knowledge, official or other access to the system, and connections with judicial institutions or other persons who may have facilitated the commission of interference; (4) consequences of unlawful interference, including the type and extent of damage caused, disruption of the normal functioning of the automated system, possible blocking, forgery, destruction, modification, copying, or leakage of information, and the impact of such consequences on judicial proceedings, document circulation, case allocation, access to information, or the exercise of procedural rights of participants in proceedings; (5) circumstances affecting the gravity of the criminal offense, characterizing the suspect or accused person, aggravating or mitigating punishment, indicating commission by a group, repeated offending, abuse of official position, use of special technical means or other qualifying features, as well as circumstances excluding criminal liability or constituting grounds for termination of criminal proceedings; (6) circumstances confirming the use of technical devices, software tools, user accounts, server equipment, data carriers, or other means as instruments of committing the offense, as well as the possibility of their seizure, attachment, special confiscation, or use for further forensic examination; (7) circumstances indicating grounds for the application of criminal law measures to legal entities where unlawful interference was committed in their interests, on their behalf, or by authorized persons using their organizational, technical, or financial capabilities.

It has been proven that the most significant areas of interaction involve cooperation between investigators and prosecutors, operational units, specialists and experts in computer technologies, information security and telecommunications, as well as judicial institutions, technical administrators, electronic communications operators, and other persons possessing information necessary for establishing the circumstances of the criminal offense.

The dissertation emphasizes the importance of the initial stage of pre-trial investigation, where a key role is played by the inspection of the scene, computer equipment, server hardware, automated workstations, network infrastructure, and system logs. It is stressed that timely and proper conduct of such investigative (search) actions is critically important for preserving volatile digital data, preventing their alteration or loss, and forming the initial evidentiary basis in criminal proceedings.

It has been established that searches in criminal proceedings of this category possess a specific search-and-tactical nature, as they are aimed not only at identifying material objects but primarily at locating hidden digital storage media, technical means of access, official documentation, and devices that may contain traces of interference or be used for its commission. The effectiveness of this investigative action largely depends on compliance with the requirements of surprise, promptness, coordination of investigative-operational groups, and prevention of remote destruction of electronic information.

The study establishes that interrogation in proceedings concerning unlawful interference with automated systems requires consideration of both procedural and technical aspects. This concerns the need to clarify the peculiarities of information system functioning, access procedures, the role of specific users, and the mechanism of possible data modifications. The effectiveness of interrogation is determined by the proper formulation of questions, consideration of the professional specifics of interviewed persons, and overcoming typical defensive versions related to technical malfunctions or denial of involvement.

Considerable attention in the research is devoted to the use of specialized knowledge in the form of forensic examinations and involvement of specialists. The necessity of appointing computer-technical examinations, examinations in the field of telecommunications systems, information security, technical information protection, and other types of forensic studies depending on the circumstances of a specific proceeding is substantiated. The use of specialized knowledge makes it possible to establish the mechanism of interference, the source of system access, the nature of

modifications of information, and the connection between technical actions and a particular individual.

It is generalized that increasing the effectiveness of investigations into unlawful interference with the operation of automated systems in the field of justice is possible provided there is comprehensive improvement of organizational principles of interaction between investigators, prosecutors, specialists, and expert institutions, as well as proper regulatory support for such activities. The results of the research are aimed at improving the quality of pre-trial investigations, enhancing forensic practice, and ensuring reliable protection of the information infrastructure of justice.

Keywords: automated systems, e-justice, documents, forensic methodology, pre-trial investigation, criminal proceedings, digital traces, cybercrime, search, inspection, interrogation, specialized knowledge, forensic examination.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

у яких опубліковано основні наукові результати дисертації:

1. Моісеєв М. Г. Основні засади електронного судочинства у праві Європейського союзу та незалежній Україні: порівняльний аспект. *Публічне право*. 2022. № 4 (48). С. 167–174. DOI: https://doi.org/10.32782/2306-9082/2022-48-19

2. Моісеєв М. Г., Зарубей В. В. Криміналістична характеристика особи злочинця, що незаконно втручається в роботу автоматизованих систем в органах та установах системи правосуддя. *Knowledge, Education, Law, Management*. 2024 № 8 (68). С. 122–132. DOI: https://doi.org/10.51647/kelm.2024.8.17

3. Моісеєв М. Г. Криміналістична характеристика незаконного втручання в роботу автоматизованих систем в органах правосуддя. *Юридичний вісник*. № 3, 2023. С. 265–277. DOI: https://doi.org/10.32782/yuv.v3.2023.33

4. Зарубей В. В., Моісеєв М. Г. Тактика проведення огляду під час розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя. *Право.UA*. № 1. 2026. С. 274–278. DOI: https://doi.org/10.71404/LAW.UA.2026.1.36

5. Моісеєв М. Г. Обшук під час розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя. *Наукові інновації та передові технології.* № 4(56) 2026. С. 3331–3343. DOI: https://doi.org/10.52058/2786-5274-2026-4(56)-3331-3343

які засвідчують апробацію матеріалів дисертації:

6. Моісеєв М. Г. Основні засади електронного судочинства в праві Європейського союзу. *Кримінальне судочинство: права людини під час дії надзвичайного або воєнного стану* : міжнар. наук.-практ. конф. (Київ, 18 листоп. 2022 р.). Київ : Нац. акад. внутр. справ, 2022. С. 215–218. URL : https://elar.navs.edu.ua/server/api/core/bitstreams/0c56ce37-2df4-48cb-b8d8-1d5fe007a70a/content

7. Моісеєв М. Г. Можливості застосування міжнародного досвіду щодо удосконалення електронного судочинства в Україні при запровадженні воєнного стану. *Кримінальне процесуальне право на сучасному етапі розвитку України* : матеріали круглого столу, присвяч. 40-річчю кафедри кримінального процесу (Київ, 27 жовт. 2023 р.). Київ : Нац. акад. внутр. справ, 2023. С. 282–286. URL : https://elar.navs.edu.ua/server/api/core/bitstreams/ece9dd4d-8e55-4ed1-bfae-ebb66a98894e/content#page=283&zoom=100,72,481

8. Моісеєв М. Г. Електронне судочинство в умовах воєнного стану. *Кримінальне судочинство: сучасний стан та перспективи розвитку* : міжвідом. наук.-практ. конф. (Київ, 28 квіт. 2023 р.). Київ : Нац. акад. внутр. справ, 2023. С. 174–177. URL : https://elar.navs.edu.ua/server/api/core/bitstreams/72b10f52-7185-4e4c-b36f-943b408c5f7b/content

9. Моісеєв М. Г. Особа правопорушника як елемент криміналістичної характеристики незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя. *Кримінологія і війна: екзистенційні виклики для України* : міжвідом. наук.-практ. круглого столу (Київ, 6 листоп. 2025 р.). Київ : Нац. акад. внутр. справ, 2025. С. 272–274.

ЗМІСТ

ВСТУП

Обґрунтування вибору теми дослідження. Захист особи, суспільства та держави від кримінальних правопорушень, забезпечення відновлення порушених прав, належне функціонування механізму правосуддя та гарантування доступу до нього є одним із пріоритетних напрямів державної політики у сфері національної безпеки й правопорядку. Реалізація цих завдань безпосередньо пов’язана з ефективністю діяльності органів та установ системи правосуддя, стабільністю функціонування їх інформаційної складової, надійністю автоматизованих систем, у межах яких здійснюється електронний документообіг, розподіл справ, збереження процесуальної інформації, облік і передавання даних.

Упровадження автоматизованих систем в органах та установах системи правосуддя суттєво вплинуло на підвищення ефективності судового адміністрування, прискорення обміну інформацією, прозорість процедур, доступність судових сервісів та загалом на цифровий розвиток правосуддя. Водночас електронне судочинство, функціонування автоматизованих систем документообігу, інтеграція баз даних, застосування електронного підпису, віддаленого доступу та мережевих сервісів об’єктивно зумовили появу нових криміналістично значущих загроз. Однією з таких загроз є незаконне втручання в роботу автоматизованих систем органів та установ системи правосуддя, яке посягає не лише на інформаційну безпеку, а й на нормальне функціонування правосуддя, принципи законності, достовірність електронного документообігу та довіру суспільства до судової влади.

Згідно зі статистичною інформацією Офісу Генерального прокурора, до Єдиного реєстру досудових розслідувань упродовж 2020–2026 років внесено відомості про кримінальні правопорушення, передбачені ст. 376-1 КК України: у 2020 році – 30 кримінальних проваджень (повідомлень про підозру – 0), у 2021 році – 32 (2 підозри), у 2022 році – 46 (0 підозр), у 2023 році – 65 (19 підозр), у 2024 році – 42 (9 підозр), у 2025 році – 35 (3 підозри), а за чотири місяці 2026 року – 17 (1 підозра) [38].

Щодо результативності завершення досудового розслідування, у вигляді направлення обвинувальних актів до суду, встановлено такі показники: у 2020 році – 0 кримінальних проваджень (0 %), у 2021 році – 2 (6,2 %), у 2022 році – 0 (0 %), у 2023 році – 19 (29,2 %), у 2024 році – 9 (21,4 %), у 2025 році – 3 (8,5 %), у 2026 році – 1 (2,8 %).

Розрахунок середнього показника за досліджуваний період свідчить, що середній рівень направлення кримінальних проваджень до суду становить близько 9,7 %, що є вкрай низьким індикатором ефективності завершення досудового розслідування зазначеної категорії кримінальних правопорушень.

Отримані результати свідчать про наявність системної проблеми у діяльності органів досудового розслідування щодо забезпечення належної процесуальної результативності у провадженнях про кримінальні правопорушення, передбачені ст. 376-1 КК України.

Поряд із цим, необхідно додати, що в умовах інтенсивної цифровізації державного управління, а також на тлі воєнного стану, коли значна кількість управлінських і процесуальних процедур переноситься в електронне середовище, кримінальні правопорушення, пов’язані з незаконним втручанням у роботу автоматизованих систем, набувають підвищеної суспільної небезпеки. Їх специфіка полягає в тому, що такі посягання нерідко мають прихований характер, вчиняються із використанням легітимних облікових записів, технічних засобів маскування, змін у конфігурації програмного забезпечення або маніпулювання електронними даними.

У свою чергу, це істотно ускладнює своєчасне виявлення факту втручання, встановлення його механізму, локалізації цифрових слідів, визначення кола причетних осіб та доказування причинно-наслідкового зв’язку між конкретними діями і наслідками для функціонування системи правосуддя. До числа типових проблем, що виникають під час розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя, слід віднести: складність виявлення самого факту несанкціонованого впливу на систему; труднощі у відмежуванні злочинного втручання від технічних збоїв,

помилок адміністрування або неправомірних, але формально авторизованих дій користувачів; швидкоплинність і вразливість цифрових слідів; необхідність залучення спеціальних знань у сфері комп'ютерної техніки, телекомунікацій, захисту інформації та електронного документообігу; складність визначення меж відповідальності між службовими особами, адміністраторами систем, технічними працівниками й зовнішніми суб'єктами втручання. Аналіз слідчої та судової практики свідчить, що у процесі розслідування таких кримінальних правопорушень нерідко допускаються тактичні, організаційні та процесуальні помилки, пов'язані з несвоєчасним оглядом технічних засобів, неправильним вилученням цифрових носіїв, неповною фіксацією електронної обстановки, помилками у формулюванні питань до експертів, недооцінкою значення мережевих журналів, резервних копій і метаданих. Усе це негативно позначається на результативності розслідування та подальшій перспективі судового розгляду. На противагу цьому особи, які вчиняють такі кримінальні правопорушення, зазвичай, добре орієнтуються у функціонуванні відповідних автоматизованих систем, порядку доступу до них та механізмах авторизації. За таких умов розроблення сучасної методики розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя є об'єктивно необхідним і має не лише теоретичне, а й прикладне значення.

Теоретичне підґрунтя дисертації становлять наукові праці вітчизняних учених-криміналістів: Ю. П. Аленіна, А. О. Антощука, В. Д. Басая, І. В. Басистої, В. П. Бахіна, В. Д. Берназа, Г. П. Власової, В. І. Галагана, В. Г. Гончаренка, І. В. Гори, А. В. Іщенка, Н. І. Клименко, І. І. Когутича, В. О. Коновалової, М. В. Корнієнка, В. С. Кузьмічова, В. К. Лисиченка, Є. Д. Лук'янчикова, В. Г. Лукашевича, В. В. Пясковського, М. В. Салтевського, О. Ю. Татарова, О. В. Таран, В. В. Тіщенка, П. В. Цимбала, М. С. Цуцкірідзе, К. О. Чаплинського, С. С. Чернявського, Ю. М. Чорноус, Л. Д. Удалової, В. Ю. Шепітька, М. Є. Шумила, В. В. Юсупова та ін. Внесок указаних науковців у розвиток криміналістики, судової експертології та методики розслідування кримінальних

правопорушень є безумовно вагомим. Водночас значна частина наукових положень формувалася за умов іншого рівня розвитку цифрових технологій, меншої інтегрованості автоматизованих систем у діяльність органів правосуддя, а також до істотного оновлення законодавства у сфері електронного судочинства й захисту інформації. Крім того, сучасний стан незаконного втручання в роботу автоматизованих систем характеризується новими способами реалізації злочинного наміру, використанням складних технічних рішень і дистанційних каналів доступу, що вимагає перегляду й уточнення традиційних методичних підходів.

Сьогодні для працівників органів досудового розслідування нагальною є потреба у використанні адаптованої криміналістичної методики розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя з урахуванням чинного законодавства, сучасної правоохоронної практики, специфіки роботи з цифровими слідами, залучення спеціальних знань та функціонування систем в сфері правосуддя в умовах воєнного стану. Саме такі обставини зумовили вибір теми дисертації, визначили її актуальність, теоретичну значущість і практичну спрямованість.

Зв'язок роботи з науковими програмами, планами, темами, грантами. Дисертаційне дослідження виконане відповідно до основних напрямів державної політики у сфері забезпечення інформаційної безпеки, цифровізації правосуддя та протидії кіберзлочинності, затвердженої Законом України «Про основні засади забезпечення кібербезпеки України» від 05 жовт. 2017 року № 2163-VIII. Робота відповідає Державній антикорупційній програмі на 2023–2025 роки (постанова Кабінету Міністрів України від 4 березня 2023 року № 220); Тематиці наукових досліджень і науково-технічних (експериментальних) розробок на 2020–2024 роки (наказ МВС України від 11 червня 2020 року № 454), Тематики наукових досліджень і науково-технічних (експериментальних) розробок Міністерства освіти і науки на 2022–2026 роки (наказ МОН України від 3 лютого 2022 року № 109).

Тема дисертації затверджена Вченою радою НАВС 29 листопада 2022 року (протокол № 15), зареєстрована Координаційним бюро Національної академії правових наук України (№ 1144, 2022 рік).

Мета і завдання дослідження. Мета дослідження полягає у розробленні теоретичних положень і практичних рекомендацій щодо формування та вдосконалення криміналістичної методики розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя, спрямованих на підвищення ефективності виявлення, розкриття та розслідування відповідних кримінальних правопорушень.

Для досягнення зазначеної мети було поставлено такі *завдання:*

– розкрити теоретико-правові засади тлумачення поняття, ознак та функцій електронного судочинства в Україні;

– сформувати криміналістичну характеристику незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя;

– виокремити криміналістичну характеристику особи, яка незаконно втручається в роботу автоматизованих систем в органах та установах системи правосуддя;

– проаналізувати та виокремити обстановку та «слідову картину» незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя;

– визначити обставини, що підлягають встановленню під час розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя;

– окреслити основні аспекти взаємодії слідчого з іншими суб’єктами під час розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя;

– визначити особливості проведення огляду під час розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя;

– з’ясувати специфіку проведення обшуку під час розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя;

– надати рекомендації щодо проведення допиту під час розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя;

– розглянути засади використання спеціальних знань під час розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя.

Об’єкт дослідження – суспільні відносини у сфері діяльності органів досудового розслідування під час розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя.

Предмет дослідження – основи методики розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя.

Методи дослідження. Для досягнення поставленої мети в роботі використано загальнонаукові та спеціальні методи, зокрема: *методи формальної логіки* (аналіз, синтез, дедукція, індукція, аналогія, абстрагування) надали можливість дослідити поняття, ознаки та функції електронного судочинства в Україні (підрозділ 1.1); виокремити організаційно-тактичні засади розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя (розділ 2). У дослідженні використано *спеціально-правові* методи*: порівняльно-правовий* – під час аналізу норм національного й іноземного законодавства, міжнародних договорів, наукових категорій, визначень і підходів (у всіх розділах дисертації); *системно-структурний* – для формування тактики проведення слідчих (розшукових) дій (підрозділи 3.1, 3.2, 3.3); *метод системного аналізу* – для комплексного узагальнення елементів криміналістичної характеристики досліджуваного кримінального правопорушення (підрозділ 1.2); *статистичний* – з метою підтвердження теоретичних висновків даними державної та відомчої статистики, узагальнення

результатів вивчення емпіричних джерел (у всіх розділах дисертації); *соціологічний* – у межах обґрунтування наукових висновків даними анкетування практичних працівників правоохоронних органів (у всіх розділах дисертації).

Емпіричну базу дослідження становлять статистичні й аналітичні матеріали МВС України, НПУ, Офісу Генерального прокурора за 2020 – чотири місяці 2026 року; вироки Єдиного державного реєстру судових рішень за 2020 – чотири місяці 2026 року; дані, отримані внаслідок вивчення кримінальних проваджень, досудове розслідування в яких за ст. 376-1 КК України здійснювали протягом 2020–2025 років; результати анкетування 112 слідчих НПУ 36 прокурорів. Емпіричні дослідження проводили в усіх регіонах України. Використано власний практичний досвід автора на різних посадах Національної поліції України.

Наукова новизна отриманих результатів полягає в тому, що дисертація є першим в Україні комплексним науковим дослідженням, у якому запропоновано методологічні основи розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя з урахуванням сучасного стану кримінального процесуального законодавства та практики діяльності органів кримінальної юстиції. У роботі обґрунтовано низку нових положень, висновків і рекомендацій, зокрема:

вперше:

– розроблено концептуальні засади криміналістичної методики розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя, що ґрунтуються на криміналістичній характеристиці таких елементів кримінального протиправного посягання, передбаченого ст. 376-1 КК України, як: особа правопорушника, предмет посягання, спосіб, обстановка та слідова картина, взаємозв’язок яких зумовлює специфіку тактики збирання доказів шляхом проведення слідчих (розшукових) дій;

– визначено перелік обставин, які підлягають встановленню на початковому етапі розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя: (1) обставини, пов'язані зі складом кримінального правопорушення, передбаченого ст. 376-1 КК України; (2) обставини, пов'язані з кримінальною процесуальною діяльністю й передбачені ст. 91 КПК України; (3) обставини, що не входять до предмета доказування, проте мають криміналістичне значення (умови функціонування автоматизованих систем, рівень захищеності інформації, доступи користувачів, технічні та організаційні вразливості, поведінкові та професійні характеристики причетних осіб);

– на основі диференціації завдань початкового етапу розслідування розроблено та науково обґрунтовано алгоритмізований порядок збирання стороною обвинувачення доказів учинення незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя, що передбачає проведення взаємоузгодженого комплексу слідчих (розшукових) дій, об'єднаних єдиним тактичним задумом (огляду, обшуку, допиту, призначення та проведення судових експертиз), із урахуванням специфіки виявлення, фіксації та дослідження цифрових слідів;

– розроблено алгоритм огляду електронного середовища у кримінальних провадженнях щодо незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя, який, на відміну від існуючих підходів, враховує використання віддалених механізмів доступу до системи за допомогою спеціального програмного забезпечення та орієнтований на виявлення слідів дистанційного підключення, керування обліковими записами, запуску сторонніх програмних компонентів, зміни мережевих параметрів і модифікації електронних даних;

удосконалено:

– поняття «електронне судочинство», зміст якого передбачає нормативно врегульовану систему організаційних, процесуальних та інформаційно-технологічних засобів, за допомогою яких забезпечується здійснення судової діяльності, електронна взаємодія суду з учасниками процесу, рух процесуальних

документів, доступ до судової інформації, а також реалізація принципів доступності, гласності, відкритості і безпеки правосуддя;

– науково-методичні підходи до формування криміналістичної характеристики незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя, що ґрунтуються на системно-структурному та інформаційно-цифровому аналізі механізму кримінального правопорушення, відповідно до яких виокремлено та обґрунтовано криміналістично значущі елементи (особа правопорушника; предмет посягання; спосіб; обстановка; слідова картина), що сприяє всебічному, повному й об’єктивному вирішенню тактичних завдань досудового розслідування;

– напрями взаємодії під час розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя. В цьому контексті визначено необхідність розроблення та прийняття відомчого нормативно-правового акту – Інструкції про організацію взаємодії слідчих з правоохоронними органами, органами та установами системи правосуддя, а також іншими суб’єктами під час розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя;

– криміналістичні рекомендації щодо допиту свідків, заявників, підозрюваних та інших учасників у кримінальних провадженнях щодо незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя, з орієнтацією на встановлення не лише обставин технічного втручання, а й ознак корупційної обумовленості діяння, зокрема зацікавленості в зміні черговості розгляду справ, втручанні в автоматизований розподіл (за допомогою «механізму каруселі/велосипеду»), коригуванні відомостей у системі чи створенні переваг для окремих учасників судового процесу;

дістали подальшого розвитку:

– характеристика слідової картини незаконного втручання в роботу автоматизованих систем у сфері правосуддя, що охоплює матеріальні (цифрові сліди несанкціонованого доступу до автоматизованих систем та інформаційних ресурсів органів і установ системи правосуддя; цифрові сліди внесення змін до

інформації, що обробляється або зберігається в таких системах, а також порушення їх нормального функціонування) та ідеальні сліди (працівники органів та установ системи правосуддя – працівники, які безпосередньо або опосередковано спостерігали використання автоматизованих систем; особи, які виявили ознаки незаконного втручання чи повідомили про них; особи, що здійснювали технічне обслуговування або налаштування програмного забезпечення);

– наукові положення щодо тактики проведення обшуку у кримінальних провадженнях про незаконне втручання в роботу автоматизованих систем в органах та установах системи правосуддя шляхом урахування впливу правового режиму воєнного стану, зростання кіберзагроз та необхідності протидії можливим формам дистанційного втручання, знищення або спотворення електронної доказової інформації, у тому числі в контексті кібердій, пов’язаних із збройною агресією рф проти України;

– криміналістичні рекомендації щодо використання під час розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя спеціальних знань шляхом (а) надання консультацій і технічної допомоги; (б) призначення судових комп’ютерно-технічних експертиз, експертиз телекомунікаційних систем, технічного захисту інформації, документів, а в разі поєднання незаконного втручання з корупційними проявами – експертиз матеріалів, речовин та виробів, економічних, фоноскопічних та інших експертиз залежно від слідчої ситуації, що сприяє ефективному виявленню, фіксації, вилученню та дослідженню слідів і забезпеченню їх цілісності та автентичності.

Практичне значення отриманих результатів полягає в тому, що сформульовані й викладені в роботі положення, висновки та пропозиції впроваджено у:

– *правозастосовну діяльність* – для вдосконалення процесу розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя (акт Головного слідчого управління НПУ від 27 березня 2026 року № 31231-2026);

– *освітній процес* – під час викладання навчальних дисциплін з криміналістики, підготовки навчально-методичних праць (акт Національної академії внутрішніх справ від 06 травня 2026 року № 143-ОП);

– *науково-дослідну діяльність* – для подальших досліджень проблем розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя (акт НАБС від 06 травня 2026 року № 144-нд).

Особистий внесок здобувача. Дисертація виконана автором самостійно. Усі сформульовані положення та висновки є результатом особистих досліджень автора. Окремі положення дисертації викладено у наукових статтях: «Криміналістична характеристика особи злочинця, що незаконно втручається в роботу автоматизованих систем в органах та установах системи правосуддя» та «Тактика проведення огляду під час розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя», підготовлені у співавторстві із В. В. Зарубей. Особистий внесок М.Г. Моісеєва – 70 %.

Апробація матеріалів дисертації. Основні положення та висновки дослідження оприлюднено в доповідях на міжнародних, всеукраїнських науково-практичних конференціях: «Кримінальне судочинство: права людини під час дії надзвичайного або воєнного стану» (м. Київ, 18 листопада 2022 р.); «Кримінальне процесуальне право на сучасному етапі розвитку України» (м. Київ, 27 жовтня 2023 р.); «Кримінальне судочинство: сучасний стан та перспективи розвитку» (м. Київ, 28 квітня 2023 р.); «Кримінологія і війна: екзистенційні виклики для України» (Київ, 6 листопада 2025 р.).

Публікації. Основні положення та висновки, що сформульовані в дисертації, відображено у 9 наукових працях, серед яких чотири статті – опубліковані у виданнях, включених МОН України до переліку наукових фахових видань з юридичних наук, одна – у закордонному юридичному виданні, а також у чотирьох тезах доповідей, опублікованих у збірниках науково-практичних конференцій.

Структура та обсяг дисертації. Дисертація складається зі вступу, трьох розділів, що об’єднують вісім підрозділів, висновків, списку використаних джерел (210 джерел на 22 сторінках) і 5 додатків (на 20 сторінках). Загальний обсяг дисертації – 237 сторінок, з них основного тексту – 180 сторінок.

РОЗДІЛ 1.
ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ЕЛЕКТРОННОГО СУДОЧИНСТВА В УКРАЇНІ

1.1. Поняття, ознаки та функції електронного судочинства в Україні

Інтенсивний розвиток комп'ютерних та інформаційно-комунікаційних технологій упродовж XX–XXI століть істотно вплинув на формування сучасних інформаційних систем. Впровадження таких технологій у сферу суспільно-політичних відносин розширило можливості громадян, зокрема у сфері судоустрою та судочинства. Передумови, що виникли внаслідок цих процесів, зумовлюють новий рівень комунікації між судами та суспільством і формують додаткові очікування щодо відкритості та доступності правосуддя [53].

Використання інформаційних ресурсів у діяльності органів державної влади та місцевого самоврядування, у тому числі судів, сприяє зміцненню взаємозв'язку між державою та громадянами, забезпечує швидкий обмін відомостями, розширює доступ до них і мінімізує обмеження, притаманні попереднім історичним етапам. У площині теми дослідження зазначене означає посилення гарантій відкритості діяльності органів влади, практичну реалізацію принципу гласності судового процесу та забезпечення права особи на доступ до правосуддя. За таких умов особа повинна мати можливість отримувати необхідну інформацію, користуватися електронними сервісами, обмінюватися документами та реалізовувати свої процесуальні права в доступній формі. Правовим інструментом, здатним забезпечити наведені можливості, виступає електронне судочинство.

В Україні впровадження електронного судочинства відбувалося поетапно: від формування загальних правових засад використання електронних документів і довірчих сервісів – до створення та практичного застосування відповідних інформаційних ресурсів у діяльності органів державної влади, включно із

судами. Нормативну основу цього процесу становили, зокрема, Закон України «Про електронні документи та електронний документообіг» [121], Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» [134], Указ Президента України «Стратегія сталого розвитку «Україна – 2020» від 12.01.2015 № 5/2015 [158], Розпорядження Кабінету Міністрів України «Концепція розвитку електронного урядування в Україні» [53], Закон України «Про електронний цифровий підпис» [120], а також Закон України «Про електронну ідентифікацію та електронні довірчі послуги» [130]. Зазначені акти визначили правові умови використання електронних документів, засобів автентифікації та довірчих послуг, без яких неможливе належне функціонування електронних сервісів у сфері правосуддя.

Хоча сьогодні електронне судочинство сприяє підвищенню ефективності, відкритості та прозорості діяльності судових органів шляхом використання інформаційно-телекомунікаційних технологій. Їх запровадження орієнтоване на забезпечення належного рівня доступності правосуддя, упорядкування процедур розгляду справ і утвердження людиноцентричного підходу в організації судової влади [53]. У практичному вимірі йдеться про створення та використання технічних і програмних засобів, які забезпечують подання та отримання процесуальних документів, електронний обіг матеріалів справи, інформування учасників провадження, участь у засіданнях із застосуванням засобів зв’язку, а також збереження та відтворення процесуально значущої інформації.

В. В. Білоус слушно зазначає, що електронне судочинство, порівняно з традиційною формою, здатне більшою мірою гарантувати доступ до правосуддя, оперативність розгляду справ, підвищення якості судових рішень, посилення контролю сторін за перебігом процесу та економію судових витрат, а також сприяти змагальності та публічності судового розгляду [10, с. 294]. У свою чергу Л. В. Сердюк підкреслює, що електронний формат судочинства покликаний вирішувати й низку супутніх питань, зокрема подання до суду запитів, звернень, клопотань і скарг як процесуального, так і непроцесуального характеру, організацію обміну даними між судом та особою, а також удосконалення

управління справою з боку судді [154, с. 129].

З огляду на функціональне призначення електронного судочинства доречно розглядати його як напрям електронного урядування, що стосується сфери здійснення судової влади. Використання сучасних технологічних рішень у судовій сфері дає змогу впорядкувати обіг значних обсягів інформації, зменшити адміністративні витрати, скоротити строки розгляду справ та забезпечити належний рівень фіксації процесуальної діяльності. Інформаційні системи полегшують доступ суддів і працівників апарату суду до матеріалів справи, забезпечують можливість отримання повної та актуальної інформації про перебіг провадження, а також створюють передумови для кількісного й якісного аналізу діяльності судів [209].

Науковий обіг суміжних категорій («електронний суд», «електронне правосуддя») характеризується неоднаковими підходами, що зумовлює потребу у їх понятійному розмежуванні [159]. В цілому поняття «електронний суд» аналізується у широкому та вузькому значеннях. Широке пов’язується з функціонуванням такої організації судового процесу, за якої забезпечується повний цикл розгляду справи в електронному форматі – від подання позову до виконання судового рішення. Водночас в Україні практична реалізація такого підходу не є завершеною, хоча окремі компоненти електронної взаємодії вже застосовуються [11, с. 25]. С. В. Романенкова вказує, що у широкому значенні воно визначається як сукупність автоматизованих інформаційних систем і сервісів, що забезпечують оприлюднення судових рішень, ведення електронної справи, доступ сторін до її матеріалів та організацію електронної взаємодії між судом і учасниками процесу. У вузькому значенні електронне судочинство пов’язується з можливістю суду та учасників процесу здійснювати передбачені законодавством процесуальні дії в електронній формі, які впливають на початок і перебіг судового розгляду, зокрема подання документів або участь у засіданні в режимі відеоконференції [149, с. 28].

О. О. Барназюк визначає електронне судочинство як комплексне поняття, що охоплює особливу форму організації судової влади, засновану на

застосуванні сучасних технологічних рішень і спрямовану на підвищення ефективності, доступності правосуддя та впорядкування внутрішніх і зовнішніх управлінських процесів на засадах верховенства права, справедливості, відкритості та прозорості [117]. Водночас дослідник, аналізуючи співвідношення понять «суд», «судочинство» та «правосуддя», обґрунтовано застерігає від їх ототожнення в електронному вимірі. На його думку, категорія «електронний суд» відображає інституційний аспект функціонування суду, тоді як «електронне судочинство» або «електронне правосуддя» описує процесуальний і змістовний бік здійснення правосуддя [8]. При цьому, порівняльно-правовий аналіз зарубіжного регулювання свідчить про більш комплексне розуміння відповідних категорій. В. А. Пономаренко обґрунтовано зазначає, що в правових системах іноземних держав під «electronic court» або «electronic justice» часто розуміється весь судово-юрисдикційний порядок розгляду справ із використанням електронного середовища та віртуального простору як основного способу організації процесу [110, с. 28]. Такий підхід акцентує увагу не лише на технічному інструментарії, а й на процесуальній формі здійснення правосуддя.

Фінський дослідник А. Хіетанен пропонує розрізняти два підходи до тлумачення поняття «електронний суд» або «електронні правові комунікації». У вузькому значенні останні розуміються як структурований бездокументарний обмін інформацією між сторонами та судами, що виступає альтернативою паперовому документообігу та має еквівалентну правову силу. У широкому значенні охоплюють весь процес електронної взаємодії із судами, включаючи надання судової інформації та використання електронних засобів зв’язку на різних стадіях судового провадження [35, с. 25]. Втім, практичне впровадження електронних інструментів у сфері правосуддя в різних державах має відмінності, зумовлені правовою системою, рівнем технічного забезпечення та соціально-економічними чинниками.

Європейський досвід демонструє, що електронні засоби у сфері правосуддя можуть відігравати важливу роль у забезпеченні доступності судових процедур за умови належного нормативного регулювання й технічної

готовності. Для полегшення доступу до правової інформації в умовах різних правових традицій держав Європейського Союзу створено The European e-Justice Portal [210]. Портал надає фізичним і юридичним особам інформацію їхніми мовами щодо судових процедур, форм процесуальних і позасудових документів, порядку виконання судових рішень, а також відомості про адвокатів, нотаріусів, перекладачів і медіаторів та доступ до матеріалів у сфері правової допомоги.

Окрім зазначеного порталу, у межах Європейського Союзу функціонують інші інструменти правової інформатизації, зокрема Європейський ідентифікатор законодавства (European Legislation Identifier), Європейський ідентифікатор прецедентного права (European Case Law Identifier), Європейська судова мережа у цивільних і комерційних справах. Такі ресурси забезпечують уніфікований пошук нормативних актів і судових рішень, полегшують орієнтацію в правових системах держав-членів і сприяють правовій визначеності. Передбачена можливість автоматичного перекладу матеріалів, а за потреби – професійного перекладу, що істотно розширює можливості для осіб, які звертаються до правосуддя за межами своєї держави. Суттєве значення для формування засад електронного судочинства в Європі мають документи Council of Europe, які містять підходи до організації інформаційних ресурсів судової влади, сумісності систем та забезпечення юридичної значущості електронних матеріалів. Серед них: Висновок № 2 (2001) Консультативної ради європейських суддів щодо фінансування та управління судами; Рекомендація № R (95) 11 стосовно відбору, обробки, подання та архівації судових рішень у правових інформаційно-пошукових системах; Рекомендації Rec (2001) 2 та Rec (2001) 3 щодо ефективності інформаційних систем і надання юридичних послуг із використанням новітніх технологій; Рекомендації Rec (2003) 14 і Rec (2003) 15 щодо взаємодії інформаційних систем у сфері правосуддя та архівування електронних документів [76, с. 142]. Узагальнено ці документи орієнтують на впорядкованість інформаційних ресурсів, належний рівень збереження матеріалів і забезпечення їх правового статусу. Показовим є також досвід Сінгапуру, де система електронного подання документів передбачає

автоматизовану перевірку їх відповідності процесуальним вимогам. Після такої перевірки документ долучається до відповідної справи без участі працівників суду, що зменшує вплив людського фактора та підвищує організаційну впорядкованість руху документів [142, с. 77].

Водночас, запозичення іноземного досвіду є природним для держав, які розпочинають впровадження відповідних механізмів пізніше, однак механічне перенесення рішень без урахування національних особливостей може спричиняти труднощі у правозастосуванні. Отже, адаптація зарубіжного досвіду потребує виваженого підходу та наукового обґрунтування. Національний досвід упровадження електронного судочинства має комплексний і водночас неоднозначний характер. Електронні механізми взаємодії в окремих сегментах судочинства сприяли підвищенню відкритості діяльності судів та оптимізації організаційних процедур, що позитивно впливає на строки розгляду справ і витрати, пов’язані з діяльністю апарату суду [24]. Поряд із цим у наукових колах наявна критична позиція, згідно з якою електронне судочинство не змінює природи судового розгляду як процесуальної діяльності, а стосується насамперед його організаційного і технічного забезпечення [176].

На нашу думку до структури електронного судочинства доцільно віднести взаємопов’язані елементи, сукупність яких забезпечує реалізацію процесуальних прав і обов’язків учасників судового провадження в електронній формі та організацію внутрішніх процедур. Електронні судові засідання передбачають розгляд справ із використанням засобів відеоконференцзв’язку та інших телекомунікаційних технологій, що забезпечують дистанційну участь сторін та інших учасників процесу за умови дотримання вимог процесуального законодавства. Такі засоби застосовуються не як альтернатива судовому розгляду, а як процесуально визначений спосіб участі, який має гарантувати реалізацію прав сторін і належний порядок судового засідання.

Електронні документи охоплюють процесуальні та інші документи, які створюються, подаються, передаються й зберігаються в електронній формі із застосуванням кваліфікованого електронного підпису та інших засобів

автентифікації відповідно до вимог законодавства [128]. Їх юридична значущість зумовлюється не формою, а дотриманням встановлених правил створення, подання і фіксації таких документів у судових інформаційних ресурсах.

Електронні повідомлення становлять офіційні процесуальні повідомлення, виклики, повістки та іншу кореспонденцію, що надсилаються учасникам справи через передбачені законом електронні канали зв'язку [128]. Використання таких каналів повинно відбуватися в межах правового регулювання, забезпечувати підтвердження факту відправлення й отримання, а також не допускати підміни процесуально встановлених способів комунікації у випадках, коли законом передбачено інший порядок повідомлення.

Інформаційні системи судової влади включають державні електронні ресурси, які забезпечують доступ до судових рішень, відомостей про рух справ, статистичної інформації та інших даних, відкритість яких визначена законодавством [128]. Функціонування таких ресурсів покликане підтримувати публічність судової діяльності й забезпечувати право особи на отримання інформації про судовий розгляд у визначених законом межах.

Системи автоматизації судових процедур становлять програмні комплекси, що забезпечують реєстрацію справ, автоматизований розподіл між суддями, формування процесуальних документів, ведення електронного архіву та виконання інших організаційних функцій [128]. Саме в межах цих систем концентруються значні масиви процесуально значущих даних, а тому їх належне функціонування має безпосереднє значення для дотримання принципів незалежності суддів, рівності учасників процесу та недопущення стороннього впливу на здійснення правосуддя.

Враховуючи вищевикладене О. Корнага та Ю. Плиска слушно відзначають низку переваг і для адвокатів, серед яких [31]: економія часу, зокрема у випадках участі у справах, що розглядаються судами інших регіонів; мобільність роботи з процесуальними документами та оперативний доступ до матеріалів справи; зменшення фінансових витрат, пов'язаних із необхідністю особистої присутності; реалізація принципів доступності та відкритості правосуддя через

можливість подання й отримання документів за умови належної електронної ідентифікації.

Поряд із перевагами електронного судочинства наявні проблемні аспекти, які доцільно поділяти на дві взаємопов'язані групи – суб'єктивні та об'єктивні. До суб'єктивних належать питання, зумовлені практикою діяльності органів судової влади та підходами до застосування електронних інструментів. Наявність інформаційних ресурсів, веб-сайтів і електронних сервісів сама по собі не гарантує належної відкритості судової діяльності. Існує ризик формального виконання вимог щодо прозорості за одночасного обмеження доступу до певної інформації під приводом конфіденційності або службового характеру відомостей. У такому разі виникає проблема забезпечення реального, а не лише декларативного доступу громадян до інформації про діяльність судів та до матеріалів, відкритість яких передбачена законом. Втім, слід також зазначити, що з іншого боку, функціонування електронного судочинства супроводжується питаннями щодо трудових і часових витрат, пов'язаних із переведенням значних масивів документації в електронний формат та забезпеченням її належного зберігання [79]. Своєю чергою, це вимагає не лише технічного переоснащення, а й зміни організаційних процедур у судах. До об'єктивних чинників належить насамперед рівень фінансового та матеріально-технічного забезпечення, особливо на місцевому рівні. Наявні ситуації, коли суди не забезпечені сучасним телекомунікаційним обладнанням або використовують застарілі технічні засоби, що ускладнює повноцінне використання електронних сервісів, проведення засідань із застосуванням відеоконференцзв'язку та стабільне функціонування інформаційних систем. В. Обух розширює перелік проблемних аспектів, виокремлюючи такі [204]: неврегульованість розподілу функцій між суб'єктами впровадження та супроводу електронних систем; наявність корупційних ризиків і публічних скандалів, пов'язаних із закупівлями та адмініструванням програмного забезпечення; технічні й матеріальні труднощі судової сфери; недостатній рівень обізнаності працівників судових адміністрацій, суддів та учасників процесу щодо функціонування електронних сервісів. Зазначені

чинники демонструють, що електронне судочинство не може розглядатися виключно як технічний проєкт – воно потребує комплексного нормативного, кадрового та організаційного забезпечення. Окремої уваги потребує питання фактичної спроможності населення користуватися електронними сервісами. Незважаючи на активний розвиток інформаційних технологій упродовж останніх десятиліть, значна частина осіб не використовує електронні засоби для отримання правової інформації та реалізації процесуальних прав. Рівень обізнаності, доступ до мережі Інтернет, соціально-економічні умови та вікові особливості істотно впливають на можливість повноцінного використання електронних сервісів судової влади. Хоча молодші вікові групи демонструють вищу активність у застосуванні інформаційних технологій, забезпечення рівного доступу до правосуддя вимагає врахування потреб усіх соціальних груп і недопущення ситуацій, за яких електронна форма взаємодії створює додаткові бар'єри для реалізації права на судовий захист. Поряд із зазначеними аспектами існують й інші ризики. До них належать необхідність захисту персональних даних і службової інформації, загрози несанкціонованого доступу до електронних систем, технічні збої та обмеження, пов'язані з дистанційною формою участі, що можуть впливати на повноту сприйняття процесуальних дій. Додаткової уваги потребує питання рівня технічної підготовки учасників судового процесу й працівників суду, оскільки неоднакова спроможність користуватися електронними сервісами може створювати фактичну нерівність у реалізації процесуальних прав.

Продовженням здійснення аналізу теоретико-правових засад електронного судочинства є визначення принципів, на яких воно ґрунтується. Академічний тлумачний словник української мови розглядає принцип як: основне вихідне положення якої-небудь наукової системи, теорії, ідеологічного напряму тощо; особливість, покладену в основу створення або здійснення чого-небудь, спосіб створення або здійснення чогось; переконання, норма, правило, яким керується хто-небудь у житті, поведінці [156, с. 693]. При характеристиці принципу, зазвичай, звертається увага на те, що він, по-перше, становить ідею, положення,

вимогу, цінність, а по-друге, є основоположним, фундаментальним, вихідним, загальним, керівним, відправним, провідним [113, с. 49; 42, с. 120; 43, с. 74].

Формування принципів як основних ідей здійснюється під впливом низки об'єктивних та суб'єктивних факторів. Зміна змісту політичних, економічних і духовно-моральних відносин впливає на зміст права та його реалізацію, а отже, й на зміст принципів права. Це дозволяє зробити висновок про те, що принципи права фактично відображають природу та закономірності розвитку суспільства, а також юридичної практики [84, с. 259–260]. Передусім необхідно вказати, що принципи які становлять для нас у розрізі здійснюваного дослідження, науковий інтерес мають формально-визначений нормативно-правовий характер, тобто закріпленні в конституційних положеннях, процесуальному законодавстві та спеціальних актах, що регламентують функціонування інформаційних систем у судах. Саме нормативне закріплення надає принципам обов'язковості та визначає межі їх реалізації. Хоча серед науковців не має єдиного визначення «принципів права». В. М. Косович розглядає принципи права як компонент техніки правотворення і пропонує визначити їх як зумовлені закономірностями суспільного буття керівні засади (ідеї), які закріплюються в нормативно-правових актах з метою визначення змісту та основних напрямів правового регулювання [56, с. 41]. У свою чергу, А. М. Колодій стверджує, що принципи права – це такі відправні ідеї його буття, які виражають найважливіші закономірності, підвалини даного типу держави і права, є однопорядковими із сутністю права та утворюють його основні риси, відрізняються універсальністю, вищою імперативністю і загальнозначимістю, відповідають об'єктивній необхідності побудови та зміцнення певного суспільного ладу [49, с. 43]. У цьому взаємозв'язку міркувань доцільно виокремити три взаємопов'язані групи принципів електронного судочинства.

По-перше, загальні принципи – засади, притаманні публічній владі в цілому та закріплені у Конституції України й спеціальних законах. До них належать, зокрема, законність, верховенство права, рівність перед законом і судом, доступність публічної інформації тощо. Зазначені принципи визначають

загальні вимоги до організації діяльності судів і до використання інформаційних технологій у цій сфері. Принцип верховенства права закріплений у ст. 8 Конституції України [52], а його офіційне тлумачення можна знайти у Рішенні Конституційного суду від 2 листопада 2004 року [144] у справі за конституційним поданням Верховного Суду щодо відповідності Конституції України положень ст. 69 КК України (справа про призначення судом більш м'якого покарання), згідно з яким верховенство права визначається як панування права у суспільстві. Цей принцип вимагає від держави його втілення у правотворчу та правозастосовну діяльність, зокрема у закони, які за своїм змістом мають бути проникнуті ідеями соціальної справедливості, свободи, рівності тощо [94, с. 35–36].

По-друге, організаційні принципи – засади, що характеризують побудову і функціонування судової системи, структуру її органів, статус суддів, порядок організаційного та інформаційного забезпечення діяльності судів. Саме в межах цієї групи принципів визначається, яким чином технологічні рішення інтегруються в управлінські та адміністративні процеси суду, не порушуючи гарантій інституційної незалежності та належної організації судової діяльності.

По-третє, функціональні (процесуальні) принципи – засади, що регулюють здійснення судочинства в адміністративних, цивільних, кримінальних та господарських провадженнях із урахуванням електронної форми реалізації процесуальних прав і обов'язків. Йдеться про збереження процесуальної природи судового розгляду та забезпечення того, щоб електронні засоби використовувалися як інструмент реалізації процесуальних гарантій, а не як підстава для їх звуження. Таке групування дозволяє систематизувати принципи електронного судочинства, розмежувати їх за функціональним призначенням і, відповідно, послідовно визначити теоретико-правові орієнтири, які мають враховуватися під час нормативного регулювання та практичного застосування електронних інструментів у судовій сфері.

Практична реалізація організаційних засад електронного судочинства значною мірою пов'язана з функціонуванням автоматизованих систем у судах,

передусім автоматизованої системи документообігу суду. Вона впроваджується для забезпечення належної організації процесуальної діяльності та об'єктивного і неупередженого розподілу справ між суддями. У межах її функціонування забезпечується, зокрема: почерговість і рівномірність навантаження на суддів під час розподілу справ; надання фізичним і юридичним особам інформації про стадії розгляду їхніх справ; централізоване зберігання текстів судових рішень та інших процесуальних документів; формування та узагальнення статистичних даних щодо діяльності суду; реєстрація вхідної та вихідної кореспонденції та фіксація її руху; автоматизований розподіл справ; формування і видача судових рішень та виконавчих документів на підставі даних, що містяться в системі; передача матеріалів справ до електронного архіву.

У цьому контексті доцільно відразу виокремити низку принципів, що безпосередньо характеризують електронну форму реалізації процесуальних прав і обов'язків. По-перше, доступність означає забезпечення рівних можливостей для всіх осіб щодо подання процесуальних документів, отримання інформації та участі в судових засіданнях із використанням електронних засобів. Реалізація цього принципу передбачає недопущення ситуацій, коли технічні або організаційні бар'єри звужують зміст права на судовий захист. По-друге, прозорість передбачає відкритість діяльності судів та доступ до судових рішень і відомостей про рух справи у межах, установлених законом. На думку Н. П. Христинченко, прозорість як принцип діяльності органів виконавчої влади повинна забезпечувати ясність, дохідливість якого-небудь явища, на відміну від прихованості та незрозумілості, чого в сучасному державному управлінні бути не повинно [179, с. 47]. На нашу думку, в діяльності судової гілки влади вимога прозорості стосується як доступності інформації для учасників процесу, так і зрозумілості процедур електронної взаємодії, що має значення для довіри до судової влади. По-третє, безпека та конфіденційність означають гарантування захисту персональних даних, дотримання режиму доступу до інформації, використання електронного підпису, засобів автентифікації та інших механізмів інформаційної безпеки. З огляду на правову природу судової інформації

забезпечення конфіденційності виступає необхідною умовою законного використання електронних сервісів. По-четверте, ефективність полягає у раціональній організації судових процедур, спрямованій на скорочення строків розгляду справ та підвищення якості судового розгляду. У межах цього принципу електронні інструменти мають слугувати засобом упорядкування процесуальних дій і зменшення зайвих адміністративних витрат, не впливаючи негативно на процесуальні гарантії. Поряд із наведеними принципами, система засад електронного судочинства може бути доповнена положеннями, що уточнюють правовий режим використання електронних документів і технологічних рішень у судовій діяльності. Зокрема, принцип використання електронних документів та автоматизованих систем обробки інформації полягає у нормативному визнанні можливості створення, подання, зберігання та опрацювання процесуальних документів в електронній формі. Значення цього принципу полягає у встановленні зрозумілих правил електронного документообігу та юридичних наслідків електронної взаємодії. Принцип економічності пов’язаний зі зменшенням витрат, які супроводжують організацію судового процесу, зокрема витрат на паперовий документообіг, поштові пересилання та інші організаційні потреби. Водночас реалізація економічності не може досягатися за рахунок звуження процесуальних гарантій або ускладнення доступу до суду. Принцип рівності та неупередженості у межах електронного судочинства передбачає гарантування рівного доступу до електронних сервісів для всіх учасників процесу незалежно від їх соціального статусу чи матеріального становища, а також недопущення дискримінації за ознакою рівня технічної обізнаності. Зміст цього принципу вимагає забезпечення альтернативних способів реалізації процесуальних прав у випадках, коли використання електронних інструментів є об’єктивно ускладненим. Принцип технічної надійності означає застосування стабільних і захищених технологічних рішень, які забезпечують безперервність функціонування інформаційних систем суду, цілісність даних, можливість відновлення інформації та запобігання несанкціонованим впливам. Надійність технічних

засобів має безпосереднє значення для гарантування передбачуваності судових процедур і належного документування процесуальних дій. Принцип юридичної сили електронних документів полягає у визнанні правової значущості електронних процесуальних документів і судових рішень за умови дотримання вимог законодавства щодо електронного підпису, автентифікації та належної фіксації дій у відповідних інформаційних системах. Реалізація цього принципу забезпечує рівноцінність електронної та паперової форми процесуальних документів у межах установлених законом процедур.

Таким чином, електронне судочинство в теоретико-правовому вимірі постає як упорядкована сукупність нормативно закріплених принципів і процедур, реалізація яких забезпечується автоматизованими системами та спрямована на здійснення правосуддя із дотриманням вимог верховенства права і процесуальних гарантій справедливого судового розгляду. Наведені принципи формують основу електронного судочинства в Україні та визначають умови його функціонування, що має значення і для подальшого дослідження питань захищеності відповідних систем у органах та установах системи правосуддя.

Переходячи до функцій електронного судочинства, необхідно погодитись з позицією В. А. Юсупова, який вказує, що функції займають проміжне місце між метою та завданнями діяльності державного органу. При цьому, за своєю правовою природою функції в системі управління мають вигляд практичної діяльності для реалізації конкретних цілей [203, с. 138]. Розкриття функцій дає змогу конкретизувати, які саме завдання виконують електронні інструменти в судовій діяльності та яким чином вони впливають на порядок здійснення правосуддя.

Враховуючи законодавчі положення, а також результати дослідження до основних функцій електронного судочинства доцільно віднести такі:

– організаційно-управлінська функція полягає в автоматизації реєстрації судових справ і матеріалів, розподілу між суддями, ведення електронного діловодства, формування електронного архіву, а також у забезпеченні впорядкованого руху процесуальної інформації в межах суду;

– документообігова функція забезпечує створення, подання, прийняття, обробку та зберігання процесуальних документів у електронній формі, включаючи позовні заяви, скарги, клопотання, заперечення, судові рішення й інші матеріали (реалізація цієї функції передбачає додержання вимог щодо форми документа, підписання та підтвердження його походження);

– комунікаційна функція спрямована на організацію електронної взаємодії між судом і учасниками процесу, зокрема шляхом використання електронних кабінетів, електронних повідомлень, офіційних каналів зв'язку, а також участі в судових засіданнях із застосуванням відеоконференцзв'язку;

– ідентифікаційна функція полягає у використанні електронного підпису та інших засобів автентифікації для підтвердження особи учасника процесу, належності поданих документів відповідному суб'єкту та забезпечення довіри до електронної форми комунікації;

– інформаційна функція реалізується через ведення реєстрів і баз даних щодо судових рішень, руху справ, а також формування необхідних інформаційних масивів, що забезпечують здійснення судової діяльності та доступ до визначеної законом інформації;

– аналітична функція пов'язана зі збором, узагальненням і систематизацією відомостей про судову практику та організацію роботи судів (спрямована на виявлення типових проблем, удосконалення управлінських підходів і підвищення якості організації судової діяльності на підставі фактичних даних);

– гарантійна функція полягає у забезпеченні доступу до правосуддя через створення умов для подання документів у електронній формі, дистанційної участі у процесі та отримання інформації про стан і рух справи (реалізація цієї функції повинна забезпечувати, щоб електронні інструменти розширювали можливості учасників, а не створювали для них додаткові перепони);

– функція відкритості та підзвітності забезпечує доступ суспільства до судових рішень та інформації про діяльність судів у межах, встановлених законом (у межах цієї функції електронні ресурси виконують роль механізму

публічності судової діяльності та контролю за дотриманням стандартів правосуддя);

– функція захисту даних спрямована на забезпечення належного рівня інформаційної безпеки, збереження цілісності даних, захист персональної та службової інформації, а також запобігання несанкціонованому доступу до інформаційних ресурсів суду.

Таким чином, функції електронного судочинства відображають його багатогранний характер і підтверджують, що йдеться не про використання окремих технічних засобів, а про комплексну правову категорію, яка забезпечує реалізацію завдань судової влади з урахуванням сучасних технологічних можливостей та вимог верховенства права.

Практичні аспекти безпосереднього користування пов’язані із статусом користувача підсистеми «Електронний суд», який у свою чергу пов’язаний із проходженням процедури реєстрації та створенням офіційної електронної адреси в ЄСІТС. Обов’язковою умовою подання документів в електронній формі виступає наявність кваліфікованого електронного підпису, який забезпечує ідентифікацію особи та підтверджує її волевиявлення щодо поданих матеріалів. Надання кваліфікованих електронних довірчих послуг здійснюється відповідно до Закону України «Про ідентифікацію та електронні довірчі послуги» [130], а питання правового режиму електронних документів – відповідно до Закону України «Про електронні документи та електронний документообіг» [121]. Згідно із Законом України «Про електронні документи та електронний документообіг» [121] оригіналом електронного документа визнається електронний примірник з обов’язковими реквізитами, зокрема з електронним підписом автора або підписом, прирівняним до власноручного відповідно до Закону України «Про електронні довірчі послуги» [130]. До практично значущих реквізитів належать електронний підпис і позначка часу (дата й час створення), які забезпечують автентичність, цілісність і юридичну силу електронного документа. Процедурно подання документів через підсистему «Електронний суд» передбачає заповнення визначеної адміністратором електронної форми,

долучення необхідних матеріалів (у тому числі аудіо- або відеофайлів за потреби), формування електронного пакета документів та накладення кваліфікованого електронного підпису перед відправленням до суду. Така послідовність спрямована на забезпечення належної ідентифікації подавача та збереження цілісності переданих матеріалів. Надходження документів до суду через підсистему «Електронний суд», як і направлення процесуальних документів судом до електронного кабінету користувача, здійснюється в автоматизованому режимі. Разом із тим перед прийняттям документів до розгляду працівники апарату суду перевіряють їх технічну придатність: можливість відкриття файлів, якість сканованих додатків, відповідність формальним вимогам. У разі виявлення недоліків заява може бути відхилена із зазначенням причин, що пов’язано з необхідністю забезпечити належну якість електронного документообігу та придатність матеріалів до подальшого опрацювання. У разі виникнення сумнівів щодо достовірності поданих електронних копій документів суд вправі у встановленому законом порядку витребувати відповідні оригінали у органів чи осіб, які їх подали. Така можливість виступає процесуальною гарантією перевірки належності й допустимості доказів та підтримує баланс між електронною формою провадження і вимогами доказового права. При цьому, практика функціонування підсистеми «Електронний суд» передбачає і механізми підтримки користувачів: діє контакт-центр судової влади України, онлайн-допомога на порталі «Судова влада України» та в електронному кабінеті користувача, а також інформаційні матеріали щодо реєстрації й використання сервісів. Наявність таких інструментів має значення для зменшення кількості технічних помилок та забезпечення належного користування електронними можливостями судової системи.

Отже, підсумок проведеного аналізу дає підстави стверджувати, що результативність електронного судочинства визначається не лише наявністю технічних засобів, а й належною якістю їх правового регулювання та практикою застосування. Доведено, що раціональне використання електронних сервісів

повинно поєднуватися із забезпеченням ефективного рівня захисту даних і запобіганням ризикам втрати або викривлення інформації. Подальший розвиток відповідних механізмів має враховувати національні особливості організації судової влади, пріоритети законодавчої політики та результати узагальнення зарубіжного досвіду, що сприятиме формуванню узгодженої та дієвої системи електронного судочинства.

1.2. Криміналістична характеристика незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя

1.2.1. Особа, яка незаконно втручається в роботу автоматизованих систем в органах та установах системи правосуддя

В основі методики розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя перебуває криміналістична характеристика відповідного кримінального правопорушення. Вона формується шляхом аналізу й узагальнення типових ознак таких діянь і має істотне значення для організації та здійснення ефективного досудового розслідування. Під означуваною характеристикою розуміють систематизовану сукупність відомостей про значущі ознаки кримінальних правопорушень певної категорії, що відображають стійкі взаємозв’язки між ними та використовуються для висування і перевірки слідчих версій під час розслідування [63, с. 10–11].

У розрізі цього криміналістичну характеристику незаконного втручання в роботу автоматизованих систем у сфері правосуддя доцільно розглядати як сукупність типових ознак відповідного суспільно небезпечного діяння, які мають значення для його своєчасного виявлення, документування та подальшого розслідування в межах кримінального провадження. Дослідники справедливо наголошують на тому, що криміналістична характеристика кримінальних

правопорушень, пов’язаних із використанням службового становища або доступу до інформаційних ресурсів державних установ, має важливе практичне значення для діяльності правоохоронних органів. Вона дозволяє встановити найбільш поширені ознаки таких правопорушень, визначити напрями пошуку доказової інформації та зорієнтувати розслідування в правильному напрямі [96, с. 190]. Водночас призначення криміналістичної характеристики незаконного втручання в роботу автоматизованих систем у сфері правосуддя полягає в тому, що вона створює підґрунтя для розроблення типових програм розслідування зазначеної категорії кримінальних правопорушень із урахуванням характерних слідчих ситуацій, а також обставин, що підлягають доказуванню.

Структура криміналістичної характеристики традиційно передбачає наявність низки взаємопов’язаних елементів. До них належать сукупності ознак, що характеризують: 1) спосіб учинення кримінального правопорушення; 2) обстановку його вчинення; 4) знаряддя й засоби, використані правопорушником; 5) предмет посягання; 6) особу потерпілого; 7) особу правопорушника; 8) типові сліди кримінального правопорушення. Разом з тим значення кожного із зазначених елементів у різних категоріях протиправних діянь може відрізнятися. Деякі з них відіграють визначальну роль, тоді як інші мають допоміжний характер або можуть бути відсутніми взагалі (зокрема, існують правопорушення, для яких неможливо чітко визначити конкретне місце їх учинення або відсутня безпосередня фізична особа-потерпілий) [63, с. 11]. Певні свої особливості має і структура елементів криміналістичної характеристики незаконного втручання в роботу автоматизованих систем, що використовуються в органах та установах системи правосуддя. Специфіка таких кримінальних правопорушень обумовлена використанням інформаційних технологій, службових або інших технічних можливостей доступу до електронних ресурсів, а також характером інформації, що обробляється відповідними системами.

З огляду на зазначені положення та відповідну специфіку кримінальних правопорушень, пов’язаних із несанкціонованим впливом на функціонування

автоматизованих інформаційних систем у сфері правосуддя, на нашу думку, до криміналістичної характеристики цієї категорії діянь доцільно віднести такі елементи: 1) характеристику особи правопорушника; 2) спосіб учинення кримінального правопорушення; 3) обстановку вчинення; 4) слідову картину. Саме ці складові мають першочергове значення для побудови ефективної методики розслідування незаконного втручання в роботу відповідних систем.

Необхідно погодитися з тим, що самі ж елементи криміналістичної характеристики перебувають у тісному взаємозв'язку між собою. Такі зв'язки відображають послідовність розгортання протиправної діяльності, а також дозволяють простежити залежність між окремими її складовими. У випадку незаконного втручання в роботу автоматизованих систем це особливо помітно, оскільки спосіб учинення кримінального правопорушення безпосередньо пов'язаний із технічними засобами доступу до системи, характером інформації, що обробляється, а також із професійними знаннями чи службовим становищем особи, яка здійснює втручання.

Криміналістична характеристика незаконного втручання в роботу автоматизованих систем у сфері правосуддя також має важливе значення для відмежування зазначеного кримінального правопорушення від інших суміжних діянь, зокрема від інших кримінальних правопорушень у сфері службової діяльності, а також пов'язаних із використанням комп'ютерних систем, чи від адміністративних правопорушень, що стосуються порушення певних правил користування інформаційними ресурсами. Як слушно відмічає З. М. Топорецька, вона сприяє визначенню кола обставин, які підлягають доказуванню в кримінальному провадженні, та забезпечує належне планування розслідування таких правопорушень [169, с. 164].

Відтак розроблення ефективної методики розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя, насамперед, передбачає встановлення типових ознак та формування цілісної характеристики особи правопорушника. Аналіз характеристик осіб, причетних до таких діянь, дозволяє встановити типові риси їх поведінки, мотиви

протиправної діяльності, а також умови, за яких здійснюється несанкціонований вплив на функціонування відповідних інформаційних ресурсів.

Варто додати, що уся сукупність ознак особи правопорушника охоплює відомості демографічного характеру, окремі моральні якості та психологічні особливості, що можуть впливати на схильність до вчинення правопорушень. Поняття особи правопорушника відображає сутність індивіда, який учинив кримінальне правопорушення. У зв'язку з цим можна говорити про наявність типових ознак осіб, схильних до вчинення певних категорій кримінальних правопорушень [63, с. 15–16], зокрема й тих, що пов'язані з неправомірним доступом до інформаційних систем та використанням технічних засобів для впливу на їх роботу. Окрім цього, цей елемент криміналістичної характеристики має безпосередній вплив на визначення тактики проведення слідчих та інших процесуальних дій. Наявність відомостей про криміналістично важливі риси осіб у досліджуваній категорії кримінальних правопорушень дає змогу звузити коло ймовірних причетних, правильно організувати комунікацію під час проведення процесуальних дій, налагодити психологічний контакт із підозрюваними та сприяти отриманню правдивих показань. Водночас така інформація допомагає ефективніше протидіяти можливому тиску з боку підозрюваних, їхніх захисників або інших осіб, які можуть діяти в їх інтересах [150, с. 11]. До того ж, встановлення й дослідження особи, яка здійснила втручання в роботу автоматизованих систем, належить до обов'язкових обставин, що підлягають доказуванню та складових кримінального провадження [188, с. 222].

Насамперед необхідно встановити, хто може виступати потенційним підозрюваним у досліджуваній категорії кримінальних проваджень. Виходячи зі змісту законодавства про кримінальну відповідальність, суб'єктом незаконного втручання в роботу автоматизованих систем можуть бути особи, які мають доступ до відповідних інформаційних ресурсів або здатні отримати такий доступ шляхом використання технічних засобів чи спеціальних знань. При цьому важливе значення має характер службових повноважень або функціональних

обов'язків особи, її обізнаність із принципами функціонування інформаційних систем та наявність технічних навичок роботи з комп'ютерною технікою [97].

У практиці діяльності органів та установ системи правосуддя доступ до автоматизованих систем мають судді, працівники апаратів судів, а також інші посадові особи, діяльність яких пов'язана з обробкою службової інформації в електронному вигляді. Окрім цього, певний доступ до таких систем можуть мати спеціалісти з технічного обслуговування комп'ютерного обладнання та програмного забезпечення. Саме тому під час розслідування незаконного втручання в роботу автоматизованих систем необхідно враховувати можливість причетності як внутрішніх користувачів відповідних систем, так і сторонніх осіб, які отримали доступ до них шляхом використання технічних можливостей або вразливостей інформаційної інфраструктури [123].

Показовим є вирок Жовтневого районного суду (м. Дніпро), яким особу було обвинувачено у вчиненні кримінальних правопорушень, передбачених ч. 2 ст. 369-2 та ч. 1 ст. 376-1 КК України. З матеріалів справи встановлено, що *в районному суді головний спеціаліст з інформаційних технологій мав повний доступ до автоматизованої системи документообігу суду «Д-3» та відповідні облікові дані для роботи з нею. Водночас інший працівник апарату суду мав доступ до цієї системи лише в частині реєстрації та обліку справ про адміністративні правопорушення і не був уповноважений здійснювати операції щодо реєстрації та розподілу цивільних справ. Разом із тим він був обізнаний з принципами функціонування системи та алгоритмами автоматизованого розподілу справ. 09 грудня 2015 року до приміщення Бабушкінського районного суду звернувся громадянин із проханням сприяти вирішенню питання про стягнення з боржника грошових коштів за розпискою в сумі 50 000 гривень. Працівник суду запропонував йому передати неправомірну вигоду у розмірі 25 000 гривень за вплив на прийняття відповідного судового рішення. Надалі, діючи з корисливих мотивів та не маючи належних повноважень для роботи з відповідними функціями системи, працівник апарату суду здійснив несанкціонований доступ до автоматизованої системи документообігу суду*

«Д-3». Зокрема, він вніс до системи інформацію про неможливість розподілу поданої позовної заяви на інших суддів, окрім конкретного судді. Унаслідок таких дій цивільна справа була розподілена саме на визначеного суддю. Після цього, відповідно до попередньої домовленості, заявник передав працівникові суду частину неправомірної вигоди у сумі 20 000 гривень. Під час проведення обшуку в службовому кабінеті суду ці кошти були виявлені та вилучені правоохоронними органами.

Таким чином, дії обвинуваченого, які полягали у прийнятті пропозиції щодо здійснення впливу на прийняття рішення особою, уповноваженою на виконання функцій держави, та отриманні неправомірної вигоди за такий вплив, були кваліфіковані за ч. 2 ст. 369-2 КК України. Крім того, його умисні дії, пов'язані з несанкціонованим втручанням у роботу автоматизованої системи документообігу суду, були кваліфіковані за ч. 1 ст. 376-1 КК України [19].

Наведений приклад також демонструє, що незаконне втручання в роботу автоматизованої системи документообігу суду часто є допоміжним способом реалізації корисливого злочинного наміру, спрямованого на отримання неправомірної вигоди або вплив на результати розгляду конкретної судової справи. З урахуванням наведених положень необхідно визначити коло осіб, які потенційно можуть виступати суб'єктами незаконного втручання в роботу автоматизованих систем в органах, установах системи правосуддя.

Науковці пропонують виокремлювати такі види втручання за джерелом по відношенню системи правосуддя: Зовнішньо-системне втручання – будь-яке втручання, що здійснюється суб'єктами, які не належать до системи правосуддя і не беруть участь у судово-правових відносинах [77, с. 13]; таке втручання призводить до виникнення будь-яких ускладнень у функціонуванні судів, органів системи правосуддя, професійної діяльності усіх суддів чи окремого судді. Внутрішньо-системне втручання – втручання з боку суб'єктів, які належать до системи правосуддя, є постійними чи тимчасовими учасниками судово-правових відносин. Таке втручання пов'язане з утворенням перешкод для функціонування системи правосуддя і обов'язково пов'язане з володінням

суб’єктом особливими повноваженнями, правами чи інформацією у зв’язку з його діяльністю у межах системи правосуддя [48, с. 80].

Отже, такими особами можуть бути:

1. Особи, які безпосередньо здійснюють професійну діяльність у межах органів та установ системи правосуддя та мають доступ до відповідних автоматизованих інформаційних ресурсів:

а) судді судів загальної юрисдикції, судді Конституційного Суду України, а також інші особи, діяльність яких пов’язана з прийняттям процесуальних рішень та використанням інформаційних систем судової влади;

б) працівники апаратів судів, зокрема секретарі судових засідань, помічники суддів, працівники канцелярій, архівів та інших структурних підрозділів, які забезпечують функціонування автоматизованих систем документообігу суду;

в) посадові особи органів, що здійснюють організаційне та технічне забезпечення діяльності судів, зокрема працівники Державної судової адміністрації України та її територіальних підрозділів;

2. Особи, які не є безпосередніми працівниками органів та установ системи правосуддя, однак можуть отримувати доступ до відповідних інформаційних систем у зв’язку з виконанням професійних або технічних функцій:

а) спеціалісти та працівники, відповідальні за технічне обслуговування комп’ютерної техніки, серверного обладнання, програмного забезпечення та інших технічних засобів, що забезпечують функціонування автоматизованих систем у сфері правосуддя;

б) працівники підприємств, установ або організацій, які здійснюють розробку, модернізацію або технічну підтримку програмного забезпечення, що використовується в інформаційних системах органів судової влади та інших установ системи правосуддя;

в) інші особи, які можуть отримати доступ до відповідних інформаційних ресурсів унаслідок використання технічних засобів, спеціальних програм або шляхом використання вразливостей у роботі комп’ютерних систем.

У зв’язку з цим під час розслідування незаконного втручання в роботу автоматизованих систем важливого значення набуває встановлення службового становища особи, характеру її професійної діяльності, обсягу наданих їй повноважень та рівня доступу до відповідних інформаційних ресурсів. Аналіз цих обставин дозволяє визначити коло можливих причетних осіб та сприяє формуванню подальших напрямів досудового розслідування [123].

На підставі аналізу правозастосовної практики органів досудового розслідування, зокрема НАБУ, ДБР, Національної поліції України, а також матеріалів медіа можна дійти висновку, що підозрюваними та обвинуваченими у кримінальних провадженнях, пов’язаних із незаконним втручанням у роботу автоматизованих систем в органах та установах системи правосуддя, найчастіше є особи, професійна діяльність яких безпосередньо пов’язана з використанням відповідних інформаційних ресурсів. При цьому слід ураховувати, що на момент учинення кримінального правопорушення особа може займати одне службове становище, тоді як на момент здійснення досудового розслідування вона може обіймати іншу посаду або взагалі не мати статусу службової особи. Водночас правовий статус такої особи під час розслідування може зумовлювати необхідність дотримання визначеного КПК України порядку проведення окремих процесуальних дій, а також впливати на особливості їх здійснення.

У контексті цього необхідно додати, що незаконне втручання в роботу автоматизованих систем в органах та установах системи правосуддя, передбачене ст. 376-1 КК України, належить до корисливих кримінальних правопорушень і може вчинятися як загальним, так і спеціальним суб’єктом кримінального правопорушення [68]. Загальним суб’єктом є будь-яка фізична осудна особа, яка досягла 16-річного віку та вчинила це кримінальне правопорушення шляхом несанкціонованого доступу до автоматизованих інформаційних систем судової влади. Зокрема, йдеться про випадки зламу паролів, незаконного входу до Єдиної судової інформаційно-телекомунікаційної системи або іншої автоматизованої системи, що функціонує в судах, Вищій раді правосуддя, Вищій кваліфікаційній комісії суддів України, Державній судовій

адміністрації України та їх органах, а також про здійснення несанкціонованих дій з інформацією, що міститься в таких системах. Водночас, як було зазначено значна частина таких кримінальних правопорушень вчиняється спеціальним суб'єктом, тобто службовими особами, які мають законний доступ до відповідних автоматизованих систем. До таких осіб належать, зокрема, судді, помічники суддів, працівники апарату суду та технічні адміністратори, які є користувачами автоматизованої системи документообігу суду відповідно до своїх функціональних обов'язків. Право доступу до автоматизованої системи документообігу суду надається цим особам на підставі відповідного наказу голови суду або керівника апарату суду.

Відповідно до ч. 1 ст. 52 Закону України «Про судоустрій і статус суддів», суддею є громадянин України, який відповідно до Конституції України та цього Закону призначений суддею, займає штатну суддівську посаду в одному із судів України та здійснює правосуддя на професійній основі [138]. Разом із тим користувачами автоматизованої системи документообігу суду можуть бути також помічники суддів, працівники апарату суду та технічні адміністратори, які отримують відповідні права доступу на підставі організаційно-розпорядчих актів керівництва суду [108]. Необхідно також враховувати, що у різних судах України використовуються різні програмні комплекси автоматизованих систем документообігу. Так, у місцевих та апеляційних адміністративних судах, а також у Вищому адміністративному суді України використовується програмний комплекс «Діловодство спеціалізованого суду», розроблений адміністратором автоматизованої системи для судів адміністративної юрисдикції. У місцевих та апеляційних господарських судах застосовується аналогічна система, адаптована для судів господарської юрисдикції. У місцевих та апеляційних загальних судах (крім Апеляційного суду міста Києва) використовується автоматизована система документообігу «Д-3», яка забезпечує електронний облік і розподіл судових справ. В Апеляційному суді міста Києва застосовувалася автоматизована система електронного документообігу «Апеляція», тоді як у Вищому спеціалізованому суді України з розгляду

цивільних і кримінальних справ використовувалася автоматизована система діловодства цього суду. У Верховному Суді функціонує Єдина автоматизована система діловодства Верховного Суду [108].

Таким чином, спеціальний суб'єкт цього кримінального правопорушення має службовий статус та законний доступ до відповідних автоматизованих систем, що значно розширює його можливості для незаконного втручання у їх функціонування. З урахуванням цих обставин осіб, які підозрюються або обвинувачуються у незаконному втручанні в роботу автоматизованих систем в органах та установах системи правосуддя, доцільно поділити на дві групи: а) особи, які на момент досудового розслідування продовжують працювати в органах чи установах системи правосуддя або інших державних органах та мають доступ до відповідних інформаційних ресурсів. Наприклад, *працівник судової установи, використовуючи наданий йому службовий доступ до автоматизованої системи документообігу суду, здійснив несанкціоновані зміни в електронних даних щодо розподілу судових справ* [17]; б) особи, які на момент досудового розслідування вже не обіймають відповідної посади або не мають офіційного доступу до автоматизованих систем, однак раніше володіли таким доступом чи використали отримані раніше технічні можливості для втручання в роботу інформаційних ресурсів. Залежно від способу вчинення кримінального правопорушення можна виокремити такі групи осіб: осіб, які здійснюють незаконне втручання в роботу автоматизованих систем шляхом зміни, блокування або знищення інформації, що міститься в них; осіб, які здійснюють несанкціонований доступ до автоматизованих систем або використовують надані їм повноваження всупереч встановленим правилам функціонування таких систем (92,5%) (додаток Б).

Окрім цього, важливе значення має класифікація осіб, які вчиняють незаконне втручання в роботу автоматизованих систем, за рівнем займаних ними посад, зокрема, в судовій гілці влади. За цією ознакою можна виокремити працівників нижчого рівня, які здійснюють роботу з інформаційними ресурсами та мають технічний доступ до відповідних систем, а також посадових осіб, що

займають відповідальне або особливо відповідальне становище. Практика свідчить, що до кримінальної відповідальності частіше притягуються працівники нижчого рівня, тоді як посадові особи вищого рівня значно рідше стають об'єктом кримінального переслідування. Це зумовлено складністю доведення їх причетності до втручання в роботу інформаційних систем, а також можливістю здійснення активної протидії розслідуванню.

Звернемо увагу й на те, що для методики розслідування незаконного втручання в роботу автоматизованих систем важливе значення мають окремі риси особи, яка вчиняє таке кримінальне правопорушення. Заслуговує на увагу позиція В. В. Корнієнка, відповідно до якої з криміналістичної точки зору дослідника цікавить передусім та інформація про особу, яка дає змогу визначити напрям пошуку підозрюваного, обрати ефективні методи розслідування, передбачити можливу поведінку такої особи у різних процесуальних ситуаціях, а також встановити зв'язок між характеристиками особи та обставинами вчинення нею кримінального правопорушення. Отримання таких даних дозволяє значно звузити коло можливих причетних осіб, з'ясувати мотиви протиправної діяльності, сформувати слідчі версії та визначити оптимальну тактику проведення процесуальних дій [54, с. 99].

Криміналістичні риси особи, яка вчиняє незаконне втручання в роботу автоматизованих систем, певною мірою пов'язані з характеристиками осіб, які вчиняють кримінальні правопорушення у сфері службової діяльності, або професійної діяльності, пов'язаної із наданням публічних послуг, чи інші правопорушення, пов'язані з використанням службового становища. О. В. Пчеліна виокремила групи таких ознак, за якими доцільно характеризувати осіб, що вчиняють злочини у сфері службової діяльності. До них належать загальні ознаки (вік, стать, рівень освіти, громадянство, сімейний стан, зайнятість, наявність судимостей), а також спеціальні ознаки, серед яких статус службової особи, категорія займаної посади, обсяг повноважень, сфера професійної діяльності, наявність корупційних або інших неформальних

зв’язків, можливе вчинення правопорушень у складі організованих груп, а також мотиви та цілі протиправних дій [140, с. 149].

На нашу думку, подібні характеристики можуть бути використані й під час дослідження особи правопорушника у кримінальних провадженнях, пов’язаних із незаконним втручанням у роботу автоматизованих систем, оскільки вони дозволяють більш повно встановити умови, що сприяють вчиненню таких правопорушень, а також визначити особливості поведінки осіб, які мають доступ до інформаційних ресурсів органів та установ системи правосуддя.

А. В. Дуда слушно зазначає, що особи, які вчиняють правопорушення, пов’язані з використанням службового становища або доступу до державних інформаційних ресурсів, як правило, характеризуються досить високим рівнем освіти та професійної підготовки. Наявні знання і практичний досвід дозволяють їм приховувати справжній характер своєї діяльності, інколи протягом тривалого часу. Такі особи зазвичай мають добре розвинуті комунікативні здібності, здатність впливати на оточення, викликати довіру, а також відзначаються обережністю та спостережливістю. У більшості випадків особа намагається використати службові чи неформальні зв’язки для приховування протиправної діяльності, знищення або спотворення слідів правопорушення та уникнення відповідальності. У зв’язку з цим не виключається можливість здійснення впливу на осіб, які здійснюють досудове розслідування, створення перешкод у встановленні обставин події або формування певної лінії поведінки, спрямованої на протидію. Значна частина таких осіб, володіючи спеціальними знаннями, у тому числі юридичними, обізнана з прийомами і методами розслідування відповідної категорії кримінальних правопорушень, а також із можливими способами приховування протиправних дій, що дає їм змогу заздалегідь продумувати способи протидії правоохоронним органам [27, с. 84–87].

З урахуванням наведених положень, а також результатів аналізу слідчої та судової практики у кримінальних провадженнях щодо незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя, риси особи правопорушника доцільно поділити на загальні та спеціальні.

Загальні пов’язані із соціально-демографічними характеристиками осіб цієї категорії, зокрема статтю, віком, рівнем освіти, професійним досвідом, сімейним станом та громадянством. Аналіз відповідних матеріалів свідчить, що серед осіб, причетних до втручання в роботу інформаційних систем в органах та установах системи правосуддя, переважають чоловіки (79,5%), тоді як частка жінок становить близько 20,5% (додаток Б). Така тенденція значною мірою пояснюється тим, що чоловіки частіше займають посади, пов’язані з технічним обслуговуванням комп’ютерних систем або виконанням функцій, які передбачають роботу з інформаційними ресурсами органів державної влади.

Серед осіб цієї категорії переважну більшість становлять громадяни України (100%), значна частина яких раніше не притягувалася до кримінальної відповідальності (96,1%) та має достатній рівень освіти, що дозволяє працювати з інформаційними системами та технічними засобами (додаток Б).

Вікові характеристики таких осіб здебільшого охоплюють працездатний період життя. Згідно з узагальненими статистичними даними, приблизно 12,8% правопорушників належать до вікової категорії 18–28 років, 25,9% – 29-39 років, 41,3% – 40–54 років, 11,6% – 55–59 років, а 8,4% становлять особи віком 60 років і більше (додаток Б).

За рівнем освіти значна частина таких осіб має повну або базову вищу освіту (близько 68,5%). Наявність відповідного освітнього рівня пояснюється тим, що діяльність, пов’язана з використанням автоматизованих інформаційних систем в органах та установах системи правосуддя, як правило, передбачає певну підготовку, знання у сфері інформаційних технологій або досвід роботи з комп’ютерними ресурсами (додаток Б). Формування цих характеристик особи правопорушника значною мірою пов’язане зі специфікою посад та професійної діяльності, у межах яких здійснюється робота з інформаційними системами. Саме службові обов’язки або технічні функції, що передбачають доступ до відповідних інформаційних ресурсів, створюють умови, за яких може виникати можливість незаконного втручання в їх функціонування.

При цьому, частина осіб, які здійснюють незаконне втручання в роботу автоматизованих систем в органах та установах системи правосуддя, особливо тих, що мають службовий доступ до відповідних інформаційних ресурсів, характеризується наявністю певного професійного досвіду. Найчастіше такий досвід пов'язаний із роботою в органах судової влади, правоохоронних органах або інших установах, діяльність яких передбачає використання електронних баз даних та автоматизованих інформаційних систем. Водночас не завжди ці особи володіють високим рівнем загальних, або спеціальних знань у сфері інформаційних технологій, що інколи зумовлює використання ними найпростіших способів втручання в роботу відповідних систем або залучення інших осіб, які мають необхідні технічні навички [188, с. 224].

Встановити точні відомості щодо сімейного стану осіб, які вчиняють незаконне втручання в роботу автоматизованих систем, на підставі аналізу матеріалів кримінальних проваджень досить складно, оскільки у значній кількості випадків такі відомості не відображаються у вироках або інших процесуальних документах. Проте наявні дані свідчать, що значна частина таких осіб перебуває у шлюбі (61,4%). В окремих випадках у практиці розслідування виявлялися ситуації, коли формальне розірвання шлюбу використовувалося для приховування фактичного майнового стану сім'ї. Попри офіційний статус розлучення, особи могли продовжувати спільне проживання, вести спільне господарство та користуватися спільним майном (додаток Б).

Узагальнюючи наведені дані, можна зазначити, що особа, яка здійснює незаконне втручання в роботу автоматизованих систем, у більшості випадків є громадянином України, чоловічої статі, середнього віку, який не притягувався до кримінальної відповідальності, має вищу освіту та досвід професійної діяльності понад 5 років.

Поряд із загальними соціально-демографічними характеристиками важливе значення мають і спеціальні риси осіб, які вчиняють незаконне втручання в роботу автоматизованих систем.

1. Службове або професійне становище особи.

Як вже було зазначено наявність у правопорушника відповідного статусу або службових повноважень часто передбачає необхідність дотримання особливих тактичних вимог під час проведення слідчих (розшукових) та інших процесуальних дій. У деяких випадках, залежно від займаної посади чи правового статусу особи, кримінальне провадження може здійснюватися за спеціальною процедурою, визначеною кримінальним процесуальним законодавством. Особи, які обіймають посади в органах державної влади або інших установах системи правосуддя, нерідко використовують своє службове становище для впливу на перебіг кримінального провадження. Такий вплив може здійснюватися не лише на слідчого, а й на інших учасників процесу з боку обвинувачення, зокрема на прокурора чи керівника органу досудового розслідування [151, с. 65].

2. Мотиви та мета протиправної діяльності.

Мотиви незаконного втручання в роботу автоматизованих систем можуть бути різними. У значній кількості випадків вони мають корисливий характер і пов’язані з отриманням неправомірної вигоди або створенням сприятливих умов для досягнення особистих інтересів. Такі дії можуть бути спрямовані на зміну або приховування інформації в електронних базах даних, усунення небажаних відомостей, отримання доступу до службової інформації або забезпечення переваг для окремих осіб. Особи, які використовують доступ до автоматизованих систем у протиправних цілях, часто прагнуть реалізувати власні інтереси шляхом використання службових можливостей або технічних ресурсів. У подальшому такі дії можуть супроводжуватися спробами приховати сам факт втручання в роботу системи, знищити або змінити інформаційні сліди правопорушення, а також створити умови, що ускладнюють встановлення реальних обставин події.

На формування та прояв окреслених характеристик осіб, як зазначають дослідники, впливає низка соціальних та професійних чинників. Серед них важливе значення мають початкова схильність окремих посадових осіб використовувати службове становище у власних інтересах, перебування в професійному середовищі, де окремі особи демонструють високий рівень

матеріального забезпечення, досягнутого шляхом протиправної діяльності, а також прагнення підтримувати або відновити певний рівень матеріального добробуту за допомогою використання службових можливостей. Крім того, на поведінку таких осіб можуть впливати орієнтація на високі стандарти життя, які демонструють колеги чи знайомі, а також наявність звичок чи інтересів, що потребують значних фінансових витрат [146, с. 8].

У деяких, переважно одиничних випадках, незаконне втручання в роботу автоматизованих систем може здійснюватися без чітко сформульованого мотиву. Зокрема, окремі особи можуть порушувати встановлений порядок користування інформаційними ресурсами через недбале ставлення до службових обов'язків, ігнорування правил роботи з електронними системами або формальне ставлення до вимог інформаційної безпеки. У практиці розслідування трапляються пояснення правопорушників, пов'язані з різними обставинами, серед яких посилання на сімейні проблеми, неуважність або забуття про встановлені правила роботи з інформаційними ресурсами, недостатню обізнаність із вимогами законодавства чи технічними особливостями використання електронних систем, відсутність належної підготовки або навичок користування комп'ютерною технікою.

3. Наявність значних фінансових можливостей.

Означувана характеристика може відігравати суттєву роль у процесі досудового розслідування, оскільки значні матеріальні ресурси дозволяють особам, причетним до незаконного втручання в роботу інформаційних систем, забезпечувати високий рівень правової допомоги, а також організовувати різні форми протидії розслідуванню. Така риса частіше притаманна службовим особам, які обіймають відповідальне або особливо відповідальне становище в органах державної влади чи інших установах та мають широкі можливості впливу на перебіг кримінального провадження. У подібних випадках особи можуть уникати кримінальної відповідальності не лише за втручання в роботу інформаційних систем, але й за інші правопорушення, пов'язані з використанням службового становища [97, с. 225].

4. Наявність стійких службових або неформальних зв’язків у державних органах, зокрема серед працівників правоохоронних органів.

Своєю чергою, це пояснюється тим, що значна частина осіб, причетних до таких правопорушень, сама належить до представників влади або взаємодіє з ними у межах службової діяльності. Як слушно зазначає О. В. Іванов, у середовищі високопосадовців інколи формуються латентні групи, пов’язані між собою неформальними зв’язками, що дозволяє їм використовувати своє становище для впливу на прийняття рішень та маніпулювання значними матеріальними ресурсами [40, с. 200–203]. Використання таких зв’язків може виступати однією з форм протидії розслідуванню. Під час розслідування правопорушень, пов’язаних із використанням службового становища, правоохоронні органи нерідко стикаються зі спробами втручання з боку впливових осіб або політичних діячів [207]. У деяких випадках встановлення неформальних контактів із представниками правоохоронних органів здатне суттєво ускладнити або навіть фактично заблокувати подальший перебіг розслідування [151, с. 52].

5. Вчинення правопорушення одноособово.

У більшості випадків незаконне втручання в роботу автоматизованих систем здійснюється однією особою, оскільки доступ до інформаційних ресурсів або технічних засобів є персоніфікованим. Водночас у певних ситуаціях можна встановити наявність осіб, які сприяли вчиненню такого правопорушення або були причетні до окремих його етапів. Працівники правоохоронних органів звертають увагу на складність доведення факту, що конкретні дії в автоматизованій системі були виконані саме тією особою, якій належить обліковий запис або електронний ключ доступу. У таких випадках підозрювані можуть посилатися на те, що не володіють достатніми навичками роботи з комп’ютерною технікою або не здійснювали безпосередньо відповідних дій у системі.

Разом із тим з погляду морально-психологічних характеристик таким особам притаманні корислива спрямованість, прагнення до використання

службового становища у власних інтересах, неповага до правових норм та ігнорування обов'язку їх дотримання. Типовий службовий правопорушник у сфері правосуддя, на відміну від осіб, які вчиняють загальнокримінальні правопорушення, як правило, не зловживає алкоголем чи наркотичними засобами, у повсякденному житті не вирізняється асоціальною поведінкою та дотримується зовнішніх соціальних норм. Водночас для нього можуть бути характерними підвищена самооцінка, прагнення до реалізації власних інтересів через використання службових можливостей, переважання раціональних мотивів над емоційними та схильність ігнорувати правові обмеження, якщо вони перешкоджають досягненню особистих цілей.

Отже, особа, яка вчиняє незаконне втручання в роботу автоматизованих систем в органах та установах системи правосуддя, характеризується поєднанням професійної обізнаності у функціонуванні інформаційних систем, доступу до них та наявності корисливих мотивів, що обумовлює специфіку механізму вчинення цього кримінального правопорушення.

1.2.2. Предмет та спосіб вчинення незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя

У теорії кримінального права предмет кримінального правопорушення розглядається як одна з його важливих характеристик. Зокрема, з цього приводу зазначається, що предмет є специфічною властивістю суспільно небезпечного діяння, яка конкретизує характер протиправного впливу на відповідні суспільні відносини [83, с. 210]. Як підкреслюють М. І. Бажанов, В. В. Сташис та В. Я. Тацій, законодавець по-різному визначає основні ознаки предмета кримінального правопорушення в законі про кримінальну відповідальність, що значною мірою зумовлено характером кримінального правопорушення та його особливостями. У багатьох випадках у законі зазначається лише певний вид

предметів, унаслідок чого будь-який предмет відповідного виду має однакове значення для кримінально-правової оцінки діяння [67, с. 76].

При цьому, у науковій літературі існує дискусія щодо місця предмета серед інших елементів складу кримінального правопорушення. Значна частина дослідників вважає, що предмет кримінального правопорушення не може розглядатися як самостійний елемент складу кримінального правопорушення, оскільки останній формується сукупністю об'єктивних та суб'єктивних ознак суспільно небезпечного діяння [83, с. 209]. Водночас інші науковці підкреслюють, що предмет кримінального правопорушення перебуває у тісному взаємозв'язку з об'єктом посягання та є його матеріальним проявом, через який здійснюється безпосередній вплив на охоронювані законом суспільні відносини. Традиційно у кримінально-правовій доктрині предмет кримінального правопорушення пов'язувався з речами матеріального світу. При цьому наголошувалося, що предмет має факультативний характер, тоді як об'єкт посягання є обов'язковою ознакою складу. Відмінність між ними полягає також у тому, що шкода завдається саме об'єкту кримінально-правової охорони, тоді як предмет є лише матеріальним носієм відповідних суспільних відносин [83, с. 209].

Разом із тим розвиток інформаційного суспільства та цифрових технологій зумовив переосмислення традиційного розуміння предмета кримінального правопорушення. Зокрема, М. М. Панов обґрунтовано зазначає, що до поняття предмета кримінального правопорушення доцільно відносити не лише матеріальні речі, а й реально існуючі явища об'єктивного світу, зокрема енергію або інформацію, у зв'язку з існуванням чи обігом яких вчиняється кримінальне правопорушення [104, с. 44]. Аналогічної позиції дотримується Є. В. Лащук, який визначає предмет як факультативну ознаку об'єкта злочину, що проявляється у матеріальних цінностях або інших об'єктах, які можуть бути сприйняті людиною чи зафіксовані спеціальними технічними засобами і щодо яких або шляхом впливу на які вчиняється злочинне діяння [78, с. 143].

Зазначені підходи набувають особливого значення під час аналізу кримінальних правопорушень у сфері інформаційних технологій, зокрема незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя. У юридичній літературі висловлюються різні погляди щодо визначення предмета цього кримінального правопорушення. Так, М. І. Хавронюк, залежно від форми об'єктивної сторони, відносить до предмета такого злочину або саму автоматизовану систему документообігу суду, або комп'ютерну інформацію, що обробляється чи зберігається в ній [177, с. 11–12; 98, с. 1105]. А. С. Беніцький вважає предметом незаконного втручання відомості, що вносяться до системи, інформацію, яка в ній міститься, а також саму автоматизовану систему [66, с. 533]. Водночас окремі дослідники взагалі не виокремлюють предмет як обов'язкову ознаку складу кримінального правопорушення, передбаченого ст. 376-1 КК України [47, с. 155; 175, с. 186].

На нашу думку, вирішення питання про предмет незаконного втручання в роботу автоматизованих систем у сфері правосуддя має здійснюватися з урахуванням змісту об'єктивної сторони відповідного кримінального правопорушення. Аналіз форм протиправного втручання свідчить, що основною метою правопорушника є вплив саме на інформаційні ресурси, які обробляються в автоматизованих системах. У зв'язку з цим предметом такого кримінального правопорушення доцільно визнавати інформацію, що вводиться до автоматизованих систем, обробляється або зберігається в них. Що стосується самих автоматизованих систем, то їх, на нашу думку, слід розглядати не як предмет, а як засіб здійснення протиправного впливу, за допомогою якого правопорушник отримує можливість змінювати, знищувати, блокувати або підміняти відповідні інформаційні дані. Отже, порушення функціонування автоматизованої системи не виступає самостійною метою злочинця, а є лише способом досягнення іншого результату – незаконного впливу на інформацію, що має процесуальне або організаційне значення для діяльності органів системи правосуддя.

Вирішення питання щодо предмета цього кримінального правопорушення доцільно також здійснювати з урахуванням законодавчого визначення поняття «інформація». Зокрема, відповідно до ст. 200 Цивільного кодексу України (ЦК) [181] та ст. 1 Закону України «Про інформацію» [131] інформацією визнаються будь-які відомості та (або) дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. Аналогічні положення містяться і в інших нормативно-правових актах інформаційного законодавства, зокрема у Законі України «Про науково-технічну інформацію» [132] та Законі України «Про електронні комунікації» [122; 175, с. 187].

Однак, у розрізі цього дослідження, варто вказати на те, що у механізмі незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя важливе місце посідає предмет злочинного посягання, який виступає джерелом криміналістично значущої інформації, необхідної для організації ефективного досудового розслідування цієї категорії кримінальних правопорушень. Саме відомості про предмет посягання дозволяють визначити спрямованість протиправних дій, встановити характер змін, що відбулися в інформаційних ресурсах, а також окреслити коло об’єктів, які підлягають дослідженню під час розслідування. Предмет незаконного втручання перебуває у тісному взаємозв’язку зі способом його вчинення та особою правопорушника, оскільки характер доступу до автоматизованих систем, рівень обізнаності з їх функціонуванням та технічні можливості особи безпосередньо впливають на вибір способу реалізації протиправних дій. Зазвичай, особи, які вчиняють такі дії, намагаються приховати фактичний предмет втручання шляхом маскування змін у системі, використання чужих облікових записів чи надання протиправним діям вигляду законних операцій із інформаційними ресурсами [187, с. 154].

У певній категорії кримінальних правопорушень предмет злочинного посягання є обов’язковим елементом криміналістичної характеристики. У зв’язку з цим слушною є позиція науковців, які серед структурних елементів криміналістичної характеристики кримінальних правопорушень, важливих для розроблення методики їх розслідування, виокремлюють предмет злочинного

посягання [61, с. 274; 60, с. 430] або типовий предмет посягання [59, с. 238; 62, с. 509]. Саме тому дослідження предмета дозволяє встановити спрямованість злочинних дій, визначити характер змін у матеріальному чи інформаційному середовищі та отримати відомості, що мають доказове значення для кримінального провадження.

У криміналістиці під предметом злочинного посягання розуміють різноманітні фізичні об'єкти, які характеризуються певними властивостями та можуть бути об'єктом протиправного впливу [153, с. 268], який зазнає змін, знищення, створення або перетворення у процесі вчинення кримінального правопорушення [103, с. 41], а також речі матеріального світу, впливаючи на які особа посягає на відповідні суспільні відносини [63, с. 15].

Як вже було показано, криміналістичному поняттю предмета посягання близьким є кримінально-правове поняття предмета правопорушення [58, с. 55], під яким розуміють цінності, що можуть сприйматися людиною безпосередньо або фіксуватися спеціальними технічними засобами та щодо яких або шляхом впливу на які вчиняється злочинне діяння [95, с. 110]. Предметом незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя є інформація та дані системи, які обробляються, зберігаються або передаються за допомогою таких систем.

До основних різновидів інформації, що обробляється в автоматизованих системах органів та установ системи правосуддя і може виступати предметом незаконного втручання, належать:

1) відомості про реєстрацію та рух судових справ, які містять інформацію про дату надходження матеріалів до суду, категорію справи, її номер, сторони процесу, стадії розгляду тощо;

2) дані автоматизованого розподілу судових справ, що формуються відповідно до встановлених алгоритмів функціонування автоматизованої системи документообігу суду та визначають суддю або склад суду, уповноваженого на розгляд конкретної справи;

3) електронні процесуальні документи, зокрема позовні заяви, клопотання, ухвали, рішення, вироки, апеляційні та касаційні скарги, які зберігаються в електронних базах даних або формуються в межах електронного судочинства;

4) службова інформація органів системи правосуддя, що стосується організації роботи судів, планування судових засідань, внутрішнього документообігу та інших аспектів діяльності відповідних органів;

5) персональні дані учасників судового процесу, включаючи відомості про сторони спору, їх представників, свідків, експертів та інших осіб, які беруть участь у розгляді справ;

6) технічні дані та системні журнали (логи), що фіксують дії користувачів автоматизованих систем, час входу до системи, зміну інформації, створення або видалення електронних записів тощо.

Водночас працівники правоохоронних органів, які здійснювали розслідування кримінальних проваджень цієї категорії, зазначають, що встановлення факту протиправного впливу на інформаційні ресурси таких систем є складним завданням, оскільки особи, причетні до втручання, нерідко вживають заходів для маскування своїх дій, змінюють електронні записи або використовують технічні можливості системи для приховування слідів протиправної діяльності. У зв’язку з цим під час досудового розслідування особливого значення набуває встановлення конкретного виду інформації або електронних даних, які зазнали протиправного впливу. Необхідно визначити характер внесених змін, спосіб доступу до системи, коло осіб, які мали технічну можливість здійснити такі дії, а також встановити наслідки такого втручання для функціонування автоматизованої системи та діяльності відповідного органу системи правосуддя.

Отже, предмет незаконного втручання в роботу автоматизованих систем у сфері правосуддя становлять насамперед електронні інформаційні ресурси та дані, що обробляються в таких системах, а також програмно-технічні елементи, які забезпечують їх функціонування. Саме аналіз цих об’єктів дозволяє встановити характер протиправного впливу, визначити механізм вчинення

кримінального правопорушення та сформувати належну доказову базу у кримінальному провадженні.

Поряд із цим у переважній більшості випадків незаконне втручання в роботу автоматизованих систем в органах та установах системи правосуддя поєднується з учиненням інших кримінальних правопорушень, насамперед корупційних, та пов'язане з одержанням неправомірної вигоди. У таких випадках під час розслідування за сукупністю кримінальних правопорушень ще одним предметом протиправного посягання виступає саме неправомірна вигода. Як слушно зазначає А. П. Шеремет, ознаки предмета кримінального правопорушення мають важливе значення, зокрема, для вирішення питань відшкодування матеріальних збитків, завданих кримінальним правопорушенням [200, с. 343].

Відповідно до ч. 1 ст. 1 Закону України «Про запобігання корупції» неправомірна вигода – це грошові кошти або інше майно, переваги, пільги, послуги, нематеріальні активи чи будь-які інші вигоди нематеріального або негрошового характеру, які обіцяють, пропонують, надають або одержують без законних на те підстав [123].

Законодавче визначення цього поняття характеризується кількома основними ознаками: визначенням переліку цінностей (благ), що можуть становити неправомірну вигоду (грошові кошти, інше майно, переваги, пільги, послуги, нематеріальні активи тощо); визначенням форм протиправних дій щодо таких цінностей – їх обіцяють, пропонують, надають або одержують; незаконністю відповідних дій, оскільки вони здійснюються без належних правових підстав; відсутністю належної грошової компенсації, адже такі цінності можуть надаватися безоплатно або за ціною, значно нижчою за їх ринкову вартість.

Під грошовими коштами слід розуміти готівкові гроші, кошти на банківських рахунках, а також інші фінансові активи [125]. Відповідно до ст. 192 ЦК України грошима (грошовими коштами) є гривня та іноземна валюта [181].

Закон України «Про валюту і валютні операції» визначає поняття валютних цінностей, до яких належать:

а) національна валюта (гривня) – грошові знаки у вигляді банкнот і монет, кошти на банківських рахунках у гривнях, а також електронні гроші, номіновані в національній валюті [115];

б) іноземна валюта – грошові знаки іноземних держав, кошти на рахунках у фінансових установах в іноземній валюті, а також електронні гроші, номіновані в іноземних валютах [115];

в) банківські метали, до яких відповідно до законодавства належать золото, срібло, платина та метали платинової групи у зливках або порошках найвищих проб, що мають сертифікат якості, а також монети з дорогоцінних металів [118].

Відповідно до ч. 1 ст. 190 ЦК України майном як особливим об'єктом цивільних прав визнаються окрема річ, сукупність речей, а також майнові права та обов'язки [181]. Такі об'єкти можуть бути предметом різних цивільно-правових або господарсько-правових договорів.

До різновидів неправомірної вигоди також належать переваги, під якими слід розуміти особливі привілеї, що створюють додаткові можливості для конкретних осіб та вигідно відрізняють їх від інших. Наприклад, безпідставне надання відпустки поза встановленим графіком.

Пільги – це додаткові права або повне чи часткове звільнення від виконання певних обов'язків, які надаються окремим особам чи категоріям осіб.

Послуги – діяльність виконавця, спрямована на надання замовнику певного блага, яке споживається в процесі такої діяльності. Вони можуть мати як матеріальний характер (наприклад, ремонт житла або транспортного засобу), так і нематеріальний (консультаційні або інформаційні послуги) [123].

До неправомірної вигоди можуть належати й нематеріальні активи, зокрема права інтелектуальної власності, право користування майном, майновими правами або природними ресурсами. Відповідно до п. 138.3.4 ст. 138 Податкового кодексу України до нематеріальних активів належать, зокрема: права користування природними ресурсами; права користування майном; права

на комерційні позначення; права на об’єкти промислової власності; авторське право та суміжні права; інші нематеріальні активи (зокрема право на ведення певної діяльності або використання економічних привілеїв). Крім того, у п. 14.1.40 ст. 14 Податкового кодексу України визначено ще один різновид нематеріального активу – гудвіл, який характеризує вартість ділової репутації суб’єкта господарювання [106].

Надання або одержання таких цінностей безоплатно означає відсутність будь-якої компенсації їх вартості. У випадку, коли відповідні блага передаються за ціною, нижчою від мінімальної ринкової, для встановлення факту неправомірної вигоди необхідно враховувати ринкову ціну. Під ринковою ціною розуміють вартість товарів, робіт або послуг, що формується за умов добровільної угоди між незалежними сторонами, які мають достатню інформацію про об’єкт угоди та рівень цін на аналогічні товари чи послуги на ринку [97, с. 905–907].

Таким чином, неправомірна вигода зазвичай має економічний або фінансовий характер, однак може набувати і нематеріальної форми. Важливим є те, що внаслідок її одержання правопорушник або інша особа (наприклад, близькі родичі) опиняється у більш вигідному становищі порівняно з тим, яке існувало до вчинення кримінального правопорушення, причому таке поліпшення становища не має правомірних підстав.

Отже, предмет протиправного посягання у структурі криміналістичної характеристики незаконного втручання в роботу автоматизованих систем у сфері правосуддя має важливе значення, оскільки його ознаки дозволяють правильно кваліфікувати кримінальне правопорушення, встановити зв’язок із особою правопорушника (з урахуванням мотивів), сформувати обґрунтовані слідчі версії та визначити ефективні напрями досудового розслідування.

Однак, у структурі будь-якої криміналістичної характеристики важливе значення має і спосіб вчинення кримінального правопорушення. Не є винятком і незаконне втручання в роботу автоматизованих систем в органах та установах системи правосуддя, оскільки різноманітність форм і прийомів реалізації таких

протиправних дій дозволяє встановити тісні кореляційні зв'язки між способом їх учинення та іншими елементами криміналістичної характеристики, зокрема особою правопорушника, типовою слідовою картиною, предметом протиправного посягання, а також умовами функціонування відповідних інформаційних систем. Важливість дослідження способу вчинення цього кримінального правопорушення зумовлена також низкою інших обставин.

По-перше, спосіб учинення кримінального правопорушення належить до числа обставин, що підлягають доказуванню у кримінальному провадженні (ч. 1 ст. 91 КПК України) [72]. По-друге, вивчення типових способів незаконного втручання в роботу автоматизованих систем сприяє розробленню ефективних криміналістичних рекомендацій щодо виявлення ознак таких протиправних дій, їх своєчасного документування та належної організації досудового розслідування. По-третє, узагальнення та аналіз способів вчинення і приховування незаконного втручання в роботу інформаційних систем органів правосуддя має важливе профілактичне значення, оскільки дозволяє виявити чинники та умови, що сприяють реалізації таких кримінальних правопорушень.

У науковій літературі дослідження способу вчинення кримінального правопорушення набуло активного розвитку ще у другій половині XX століття, коли ця криміналістична категорія почала розглядатися з позицій системно-структурного та системно-функціонального підходів. У межах таких підходів сформувалося наукове розуміння способу вчинення як складної системи дій правопорушника. Так, відомий український криміналіст М. В. Салтевський визначає спосіб учинення кримінального правопорушення як комплекс причинно та функціонально взаємопов'язаних довільних (а інколи й частково мимовільних) цілеспрямованих дій особи, спрямованих на реалізацію злочинного наміру [152, с. 421]. Подібної позиції дотримується і С. М. Зав'ялов, який розглядає спосіб учинення кримінального правопорушення як систему взаємопов'язаних дій суб'єкта, що здійснюються у певній послідовності з використанням відповідних засобів і знарядь та спрямовані на досягнення мети кримінального правопорушення [33, с. 7].

У свою чергу С. С. Чернявський під способом учинення кримінального правопорушення пропонує розуміти об’єктивно та суб’єктивно зумовлену систему дій (операцій, прийомів і механізмів) поведінки правопорушника, які охоплюють стадії підготовки, безпосереднього вчинення та приховування кримінального правопорушення. Кожна з таких дій залишає певні матеріальні або інформаційні сліди, що дозволяє за допомогою криміналістичних засобів і методів відтворити механізм події, встановити причетну особу та визначити найбільш ефективні напрями досудового розслідування [191, с. 55–56].

Зазначені наукові підходи мають важливе значення і для дослідження способів незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя. У цьому випадку спосіб учинення кримінального правопорушення, зазвичай, охоплює комплекс взаємопов’язаних діянь й безпосередньо пов’язаний із характером доступу до автоматизованих систем, технічними можливостями суб’єкта та його обізнаністю з принципами функціонування відповідних інформаційних ресурсів.

Аналіз положень кримінального законодавства та практики розслідування дає підстави стверджувати, що незаконне втручання в роботу автоматизованих систем в органах та установах правосуддя може реалізовуватися шляхом вчинення однієї або кількох альтернативних дій (з попередньою підготовкою чи без). За метою виокремлюють втручання: для сприяння прийняття суддею неправосудного рішення у справі, де суб’єкт є стороною; втручання в інтересах іншої особи, яка є стороною у справі; втручання, не пов’язане з конкретною справою з особистих мотивів (гнів, заздрощі, помста тощо); втручання з метою попередження процесуальних порушень чи порушень прав людини; втручання, пов’язані з глобальними трансформаційними процесами [48, с. 82]. Саме тому, на нашу думку, з криміналістичної точки зору способи незаконного втручання доцільно додатково класифікувати на такі групи:

– із попередньою підготовкою або без неї (наприклад, попереднє вивчення алгоритмів функціонування автоматизованої системи, отримання облікових

даних доступу, визначення часу та умов втручання або ж спонтанне використання наявного доступу до системи);

– із поєднанням з іншими кримінальними правопорушеннями або без такого поєднання (наприклад, із підробленням електронних документів, несанкціонованим доступом до комп'ютерної інформації, службовим підробленням чи зловживанням службовим становищем);

– із використанням службових повноважень або доступу до автоматизованих систем, наданого у зв'язку із займаною посадою, або шляхом несанкціонованого доступу до системи сторонніми особами, які не мають відповідних повноважень;

– за участю співучасників або без них, зокрема із залученням працівників апарату суду, технічних спеціалістів чи інших осіб, які мають доступ до автоматизованих систем або можуть сприяти отриманню такого доступу;

– шляхом безпосереднього втручання у функціонування автоматизованої системи або з використанням технічних засобів та програмного забезпечення (спеціальних програм, сторонніх електронних носіїв, засобів віддаленого доступу, несанкціонованого підключення до інформаційної мережі) або шляхом використання легального доступу до системи, наданого службовій особі.

До найбільш поширених способів готування до незаконного втручання в роботу автоматизованих систем у сфері правосуддя можна віднести такі дії:

– визначення конкретної автоматизованої інформаційної системи або її окремих функціональних модулів (зокрема автоматизованої системи документообігу суду, систем електронного судочинства, інформаційних баз даних органів правосуддя), доступ до яких може бути використаний для реалізації злочинного наміру;

– вивчення порядку функціонування автоматизованої системи, її технічних особливостей, алгоритмів роботи та механізмів автоматизованого розподілу справ між суддями;

– пошук осіб, які мають доступ до відповідних інформаційних систем (працівників апарату суду, технічних спеціалістів, адміністраторів системи тощо) або можуть сприяти отриманню такого доступу;

– встановлення або використання службових, професійних чи особистих зв’язків із працівниками органів та установ системи правосуддя, які мають технічну можливість здійснювати операції в автоматизованих системах;

– отримання або незаконне використання облікових даних доступу до інформаційної системи (логінів, паролів, електронних ключів, токенів авторизації тощо);

– попереднє узгодження з іншими співучасниками ролей і функцій у процесі здійснення незаконного втручання в роботу автоматизованої системи;

– розроблення способів конспірації, спрямованих на приховування факту незаконного доступу до системи (використання чужих облікових записів, застосування технічних засобів маскування, використання сторонніх комп’ютерів або мережевого обладнання тощо);

– планування часу та умов здійснення втручання, зокрема вибір періоду найменшого контролю за роботою системи або часу, коли відповідні операції можуть залишитися непоміченими;

– підготовка технічних засобів, програмного забезпечення або інших інструментів, які можуть бути використані для зміни, блокування чи видалення інформації в автоматизованій системі;

– узгодження дій із заінтересованими особами, які можуть бути зацікавлені у результатах такого втручання (наприклад, у зміні результатів автоматизованого розподілу справ або приховуванні певних процесуальних документів).

Зазначені підготовчі дії свідчать про те, що незаконне втручання в роботу автоматизованих систем у сфері правосуддя зазвичай має заздалегідь спланований характер і передбачає ретельну підготовку, спрямовану на отримання доступу до інформаційних ресурсів та забезпечення можливості

маніпулювання даними, що обробляються в таких системах. Зокрема, до основних способів такого втручання належать:

1. Внесення неправдивих відомостей до автоматизованої системи документообігу суду чи несвоєчасне внесення відомостей до Єдиної судової інформаційно-телекомунікаційної системи, іншої автоматизованої системи, що функціонує в суді, Вищій раді правосуддя, Вищій кваліфікаційній комісії суддів, Державній судовій адміністрації України, їх органах.

До прикладу, відповідно до ст. 35 КПК України, у судах функціонує автоматизована система документообігу суду, яка забезпечує об'єктивний і неупереджений розподіл матеріалів кримінального провадження між суддями з додержанням принципів черговості, рівномірного навантаження та випадковості. Матеріали кримінального провадження, скарги, заяви, клопотання та інші процесуальні документи, що подаються до суду і можуть бути предметом судового розгляду, підлягають обов'язковій реєстрації в автоматизованій системі документообігу суду в день їх надходження працівниками апарату відповідного суду [72].

До системи обов'язково вносяться відомості про дату надходження матеріалів, прізвище особи, щодо якої подано документи, зміст поданого документа, відомості про учасників провадження, інформацію про рух справи, а також дані про суддю, якому передано матеріали для розгляду. Порядок функціонування автоматизованої системи документообігу суду визначається Положенням про автоматизовану систему документообігу суду, затвердженим Радою суддів України за погодженням із Державною судовою адміністрацією України. Згідно з п. 1.5 зазначеного Положення автоматизована система документообігу суду являє собою сукупність комп'ютерних програм та програмно-апаратних комплексів, які забезпечують електронний обіг документів у суді, передачу інформації до центральних баз даних, а також захист інформації від несанкціонованого доступу [107].

Наочним прикладом зазначеного вище способу незаконного втручання є вирок Святошинського районного суду м. Києва від 10 серпня 2022 року, яким

встановлено факти маніпулювання даними автоматизованої системи документообігу суду. Як встановлено судом:

ОСОБА_4, відповідно до наказу начальника територіального управління Державної судової адміністрації у місті Києві № 15/к від 11.02.2013, був призначений на посаду керівника апарату Дарницького районного суду м. Києва та мав ранг державного службовця в межах IV категорії посад. Згідно з посадовою інструкцією керівника апарату суду, він здійснював безпосереднє керівництво апаратом суду, організовував ведення діловодства, забезпечував належне функціонування автоматизованої системи документообігу суду, а також ніс персональну відповідальність за її роботу. Крім того, наказом голови Дарницького районного суду м. Києва № 59-ОД від 31.12.2013 на ОСОБА_4 було покладено обов'язки щодо організації реєстрації судових справ, здійснення їх автоматизованого розподілу та контролю за повнотою наповнення системи інформацією. У зв'язку з цим він мав повний доступ до автоматизованої системи документообігу суду «Д-3» та був обізнаний із принципами її функціонування і порядком розподілу справ між суддями.

У Дарницькому районному суді м. Києва функціонувала електронна автоматизована система документообігу суду «Д-3», доступ до якої здійснювався користувачами на підставі індивідуальних логінів, паролів та електронних ключів доступу відповідно до займаних посад. 21 січня 2014 року до Дарницького районного суду м. Києва надійшло клопотання слідчого СВ Дарницького РУ ГУМВС України в м. Києві про обрання запобіжного заходу у вигляді тримання під вартою щодо ОСОБА_23. Після реєстрації зазначеного клопотання в канцелярії суду матеріали були передані ОСОБА_4 для здійснення автоматизованого розподілу. О 17 год. 02 хв. 27 с. ОСОБА_4 створив в автоматизованій системі документообігу обліково-статистичну картку зазначеного клопотання, у результаті чого системою було автоматично присвоєно номер справи № 753/1418/14-к та номер провадження № 1-кс/753/87/14. Разом із тим ОСОБА_4 було достовірно відомо, що відповідно до рішення зборів суддів Дарницького районного суду м. Києва слідчими суддями

були визначені конкретні судді, між якими і мав здійснюватися автоматизований розподіл таких матеріалів.

Незважаючи на це, з метою спрямування матеріалів на розгляд конкретному судді, ОСОБА_4 21.01.2014 у період з 16 год. 58 хв. 52 с. по 16 год. 58 хв. 53 с., перебуваючи на своєму робочому місці в приміщенні Дарницького районного суду м. Києва, увійшов до автоматизованої системи документообігу суду під власним логіном користувача «MEDVEDEV» та вніс зміни до довідника системи щодо спеціалізації суддів. Зокрема, він видалив у судді ОСОБА_18 спеціалізацію «в порядку КПК України», що фактично унеможливило участь цього судді в автоматизованому розподілі відповідного клопотання. У результаті таких дій коло суддів, між якими могла бути розподілена справа, було штучно обмежене.

Після внесення зазначених змін ОСОБА_4 здійснив автоматизований розподіл клопотання, внаслідок чого система визначила для розгляду справи суддю ОСОБА_16 [18].

Таким чином, використовуючи службове становище та доступ до автоматизованої системи документообігу суду, ОСОБА_4 умисно вніс неправдиві відомості до автоматизованої системи, що призвело до спотворення алгоритму автоматизованого розподілу судових справ та стало способом незаконного втручання в роботу автоматизованої системи документообігу суду.

2. Несанкціоновані дії з інформацією, що міститься в таких системах, чи інше втручання в роботу таких систем, вчинене службовою особою, яка має право доступу до цієї системи, або іншою особою шляхом несанкціонованого доступу до таких систем [68].

Як вже було вказано, нормативно-правове регулювання функціонування автоматизованих інформаційних систем судової влади визначається низкою актів. Важливим елементом інформаційної інфраструктури судової влади є Єдиний державний реєстр судових рішень, який відповідно до п. 9 ч. 1 розділу I Порядку ведення Єдиного державного реєстру судових рішень, затвердженого рішенням Вищої ради правосуддя від 19 квітня 2018 року, є державною

інформаційною системою, що забезпечує збирання, реєстрацію, накопичення, зберігання, захист, пошук і перегляд судових рішень [129].

Згідно зі ст. 2 Закону України «Про доступ до судових рішень», судові рішення є відкритими та підлягають оприлюдненню в електронній формі не пізніше наступного дня після їх виготовлення і підписання. Разом із тим законодавством передбачені випадки обмеження доступу до окремих судових рішень, зокрема тих, що постановлені у закритих судових засіданнях або пов'язані з проведенням негласних слідчих (розшукових) дій. Такі рішення можуть бути оприлюднені лише після спливу встановленого законом строку або не підлягати оприлюдненню взагалі [119].

Типовий приклад несанкціонованих дій з інформацією, що міститься в автоматизованих системах судової влади, відображено у кримінальному провадженні № 1кп-932/140/24. З матеріалів провадження встановлено, що *під час розгляду клопотання про продовження строку тримання під вартою в Кіровському районному суді м. Дніпропетровська адвокат ОСОБА_5 надав копію ухвали слідчого судді Шевченківського районного суду м. Києва від 06.02.2021, якою було надано дозвіл на проведення обшуку у кримінальному провадженні № 42020000000001183 від 01.07.2020. При цьому відповідно до вимог законодавства загальний доступ до таких судових рішень забезпечується лише через один рік після внесення їх до Єдиного державного реєстру судових рішень.*

Під час перевірки встановлено, що у відкритому доступі в Єдиному державному реєстрі судових рішень зазначена ухвала відсутня, однак адвокат ОСОБА_5 мав повний текст судового рішення, який містив інформацію з обмеженим доступом. Подальшим розслідуванням з'ясовано, що у листопаді 2019 року особа, яка працювала помічником судді Ленінського районного суду м. Дніпропетровська, незаконно отримала автентифікаційні дані доступу до Єдиного державного реєстру судових рішень, а саме логін та пароль користувача, надані судді цього суду, після чого передала їх адвокату ОСОБА_5. Отримавши зазначені автентифікаційні дані, ОСОБА_5 у період з 19.01.2021 по

09.03.2021, перебуваючи в приміщенні адвокатського об'єднання «Дипломат» у місті Дніпро, використовуючи комп'ютерну техніку та мережу Інтернет, здійснював несанкціонований доступ до Єдиного державного реєстру судових рішень через вебсайт https://reyestr.court.gov.ua.

Зокрема, використовуючи логін та пароль судді Ленінського районного суду м. Дніпропетровська, він неодноразово здійснював авторизований пошук та перегляд повних текстів судових рішень, що містили ідентифікуючі дані осіб та іншу інформацію з обмеженим доступом, у тому числі: 1) здійснив перегляд повного тексту судового рішення Бабушкінського районного суду м. Дніпропетровська від 04.11.2020; 2) здійснив перегляд судового рішення Самарського районного суду м. Дніпропетровська від 15.10.2020; 3) неодноразово здійснював контекстний пошук документів у Реєстрі за іменами окремих осіб; 4) здійснив перегляд судового рішення Кіровського районного суду м. Дніпропетровська від 02.10.2020; 5) здійснив пошук судових рішень за номером судової справи.

Таким чином, ОСОБА_5, усвідомлюючи, що не має законних підстав для доступу до повного функціоналу Єдиного державного реєстру судових рішень, використав автентифікаційні дані судді для отримання інформації з обмеженим доступом, чим вчинив несанкціоновані дії з інформацією, що міститься в автоматизованій системі документообігу суду, шляхом несанкціонованого доступу до неї [19]. Наведений приклад демонструє один із типових способів незаконного втручання у функціонування автоматизованих систем у сфері правосуддя, що полягає у незаконному використанні облікових даних користувачів із розширеними правами доступу до інформаційних ресурсів судової влади. Варто акцентувати увагу на тому, що у випадках, коли такі дії вчиняються особою, яка не є службовою особою та не має законного доступу до автоматизованої системи, обов'язковою ознакою способу їх вчинення виступає саме несанкціонований доступ до системи, що передбачає використання технічних або програмних засобів для незаконного отримання можливості роботи з інформаційними ресурсами системи.

При цьому, у науковій літературі висловлюється позиція, відповідно до якої лише внесення неправдивих відомостей до автоматизованої системи документообігу суду повинно здійснюватися умисно, тоді як інші дії, зокрема несвоєчасне внесення інформації, несанкціоновані дії з даними або інші форми втручання в роботу системи, можуть бути вчинені й за іншої форми вини [202, с. 117–118]. На наш погляд, з таким підходом складно погодитися. Усі зазначені дії, які утворюють спосіб незаконного втручання в роботу автоматизованих систем у сфері правосуддя, можуть вчинятися виключно з прямим умислом. Це пояснюється тим, що особа, яка здійснює подібні дії, усвідомлює характер функціонування відповідної інформаційної системи, передбачає можливі наслідки втручання та цілеспрямовано прагне досягти певного результату, пов’язаного зі зміною, приховуванням або викривленням інформації. Лише за наявності прямого умислу такі дії можуть становити посягання на суспільні відносини, що забезпечують здійснення правосуддя у встановленому Конституцією та законами України порядку. Крім того, досліджуване кримінальне правопорушення характеризується формальним складом, що означає наявність кримінальної відповідальності вже з моменту вчинення відповідних дій незалежно від настання конкретних наслідків. У випадках, коли порушення порядку роботи автоматизованої системи документообігу суду зумовлене необережністю або недбалістю працівника, такі дії можуть утворювати склад іншого кримінального правопорушення, зокрема службової недбалості, або взагалі не містити ознак кримінально караного діяння за наявності обставин, що виключають кримінальну відповідальність [45].

Окрему увагу необхідно приділити груповому способу вчинення незаконного втручання в роботу автоматизованих систем. Так, ч. 2 ст. 376-1 КК України передбачає кримінальну відповідальність за дії, визначені ч. 1 цієї статті, якщо вони вчинені за попередньою змовою групою осіб [68]. Аналіз судової практики свідчить, що кваліфікація за цією нормою можлива лише за умови, коли двоє або більше осіб ще до початку реалізації злочинного наміру домовилися про спільне здійснення незаконного втручання в роботу

автоматизованої системи. Груповий характер цих кримінальних правопорушень, зазвичай, зумовлений складністю технічних операцій, необхідністю використання спеціальних програмних засобів, а також розподілом ролей між співучасниками (організатор, виконавець, технічний спеціаліст, посередник тощо). Показовим у цьому контексті є приклад діяльності організованої групи, обвинувальний акт щодо якої було скеровано до суду прокурорами Офісу Генерального прокурора. У межах кримінального провадження встановлено, що *четверо учасників організованої групи здійснювали розповсюдження шкідливих програмних засобів з метою несанкціонованої зміни даних у державних інформаційних системах, зокрема щодо речових прав та їх обтяжень. Їм інкриміновано несанкціоноване втручання в роботу електронно-обчислювальних машин та автоматизованих систем, а також створення і розповсюдження шкідливих програмних засобів, тобто вчинення кримінальних правопорушень, передбачених ч. 3 ст. 27, ч. 3 ст. 28, ч. 2 ст. 361 та ч. 2 ст. 361-1 КК України.*

За даними досудового розслідування встановлено, що обвинувачені, один із яких був приватним нотаріусом, організували схему незаконного зняття обтяжень з майна громадян з метою подальшого його відчуження. Реалізація цієї схеми призводила до витоку інформації, її підроблення та порушення встановленого порядку обробки й маршрутизації даних у державних реєстрах.

Для досягнення злочинної мети учасники групи використовували шкідливі програмні засоби, призначені для викрадення облікових даних державних реєстраторів та нотаріусів. Отримані таким чином автентифікаційні дані дозволяли їм отримувати незаконний доступ до Державного реєстру речових прав на нерухоме майно та автоматизованої системи «Виконавче провадження». Свої незаконні «послуги» учасники організованої групи рекламували у тематичних інтернет-спільнотах. З метою отримання доступу до інформаційних систем вони розсилали державним виконавцям та приватним нотаріусам електронні листи, замасковані під офіційні повідомлення судів або інших державних установ. До таких листів додавали файли зі шкідливим програмним забезпеченням, яке після відкриття непомітно встановлювалося на

комп'ютер користувача та забезпечувало зловмисникам віддалений доступ до пристрою потерпілої особи, а також компрометацію її електронного цифрового підпису та пароля доступу.

У подальшому, використовуючи спеціальне комп'ютерне обладнання, засоби анонімізації мережевого трафіку та отримані облікові дані, учасники групи несанкціоновано знімали обтяження з майна громадян та здійснювали незаконну перереєстрацію рухомого і нерухомого майна [160].

Наведений приклад свідчить, що груповий спосіб вчинення незаконного втручання в роботу автоматизованих систем характеризується високим рівнем організованості, використанням спеціалізованих технічних засобів та чітким розподілом ролей між співучасниками, що суттєво ускладнює виявлення та документування таких кримінальних правопорушень. У випадках, коли таке втручання здійснюється службовими особами, кримінальна відповідальність за ч. 2 ст. 376-1 КК України настає лише тоді, коли вони виступають співвиконавцями та використовують для реалізації злочинного наміру свої службові повноваження або доступ до відповідної системи. Якщо ж у вчиненні втручання бере участь службова особа разом з іншою особою, яка не має спеціального статусу, правова оцінка їхніх дій залежить від ролі кожного учасника [68; 97, с. 873]. У таких випадках дії службової особи можуть додатково кваліфікуватися за нормами, що передбачають відповідальність за службову недбалість або інші кримінальні правопорушення у сфері службової діяльності.

Аналіз судової практики свідчить, що попри відносно невелику кількість вироків за ст. 376-1 КК України, випадки незаконного втручання в роботу автоматизованих систем документообігу суду мають місце у діяльності органів системи правосуддя. Так, за період існування цієї норми судами було ухвалено лише кілька обвинувальних вироків, при цьому обвинуваченими у більшості випадків виступали працівники апарату суду або секретарі судових засідань. Типовими способами вчинення таких кримінальних правопорушень були: накладення в автоматизованій системі обмежень з метою спрямування справи на розгляд конкретного судді, виготовлення підроблених судових рішень,

нереєстрація матеріалів судових справ у день їх надходження, а також неправомірна зміна відомостей про учасників судового процесу.

Попри незначну кількість обвинувальних вироків, кількість кримінальних проваджень за фактами незаконного втручання в роботу автоматизованих систем є значно більшою. У частині з них особам було повідомлено про підозру та направлено обвинувальні акти до суду, однак значна кількість проваджень була закрита на стадії досудового розслідування [180].

У контексті цього, способи приховування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя, доцільно розглядати як систему цілеспрямованих дій або бездіяльності особи, спрямованих на ускладнення виявлення факту кримінального правопорушення, встановлення його механізму та причетних осіб. У криміналістиці спосіб приховування визначається як комплекс дій, що здійснюються до, під час або після вчинення кримінального правопорушення з метою маскування його ознак, знищення чи спотворення слідів події або створення хибного уявлення про обставини вчиненого діяння [64, с. 232]. До речі, у більш широкому розумінні приховування кримінального правопорушення являє діяльність, спрямовану на перешкоджання досудовому розслідуванню шляхом знищення, маскування, фальсифікації або приховування слідів кримінального правопорушення, а також засобів і знарядь його вчинення. Така діяльність може проявлятися як у формі активних дій, так і у вигляді бездіяльності, коли особа свідомо утримується від виконання обов’язків щодо фіксації чи збереження інформації, що має значення для кримінального провадження [193, с. 152].

Незважаючи на різноманіття можливих ситуацій, у практиці розслідування зазначеної категорії кримінальних правопорушень можна виокремити низку типових способів їх приховування, зокрема:

– внесення до автоматизованої системи недостовірних або змінених даних з метою спотворення інформації про реєстрацію, рух чи розподіл судових справ;

– виправлення електронних записів у базах даних системи, зокрема зміна дат реєстрації документів, імен учасників процесу або інших відомостей, що мають процесуальне значення;

– використання облікових записів інших працівників або спільне використання логінів і паролів для ускладнення встановлення особи, яка безпосередньо здійснила незаконні дії в системі;

– видалення або модифікація електронних журналів подій (логів), що фіксують дії користувачів у системі, з метою приховування факту несанкціонованого доступу;

– створення або використання фіктивних службових документів, які формально пояснюють внесення змін до інформаційної системи;

– інсценування технічних збоїв, помилок програмного забезпечення або несанкціонованого доступу з боку сторонніх осіб;

– поширення неправдивої інформації щодо причин внесення змін до системи або перекладання відповідальності на інших працівників.

У деяких випадках незаконне втручання в роботу автоматизованих систем може бути замасковане під звичайну службову діяльність, що здійснюється працівниками апарату суду або іншими особами, які мають доступ до інформаційної системи. У таких ситуаціях протиправні дії набувають вигляду легітимних службових процедур, що суттєво ускладнює їх своєчасне виявлення. Крім того, на стадії підготовки до вчинення незаконного втручання правопорушники нерідко заздалегідь здійснюють заходи, спрямовані на подальше приховування своєї діяльності. До таких заходів можуть належати використання сторонніх комп’ютерів або мереж, підготовка неправдивих пояснень щодо здійснених операцій у системі, а також залучення інших осіб, які можуть підтвердити вигадану версію подій.

У разі викриття протиправних дій особи, причетні до незаконного втручання, нерідко вдаються до додаткових способів протидії розслідуванню, зокрема: відмови від надання показань або повідомлення завідомо неправдивої інформації; намагання уникнути участі у слідчих (розшукових) діях; впливу на

інших учасників кримінального провадження з метою зміни або приховування інформації про обставини вчинення кримінального правопорушення.

Таким чином, спосіб вчинення незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя характеризується використанням різноманітних форм впливу на інформаційні ресурси таких систем, що можуть проявлятися у внесенні неправдивих відомостей, несвоєчасному внесенні інформації, несанкціонованих діях з електронними даними або інших видах втручання у функціонування системи. Встановлення конкретного способу вчинення кримінального правопорушення має важливе значення для формування слідчих версій, визначення кола причетних осіб та виявлення слідів протиправної діяльності у межах досудового розслідування.

1.2.3. Обстановка та «слідова картина» незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя

Обстановка незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя перебуває у тісному взаємозв’язку з іншими елементами криміналістичної характеристики цього кримінального правопорушення, зокрема слідовою картиною та способом його вчинення. Саме конкретні умови функціонування автоматизованих інформаційних систем, організація доступу до них, технічні та організаційні особливості їх експлуатації значною мірою впливають на вибір способу незаконного втручання, який, у свою чергу, визначається реальними умовами діяльності органів та установ системи правосуддя і може змінюватися залежно від перебігу злочинної події.

Інформація про обстановку кримінального правопорушення має важливе значення для структури криміналістичної характеристики, оскільки містить відомості про інші її елементи. У межах обстановки відображаються не лише

технічні й організаційні умови функціонування інформаційних систем, а й окремі риси правопорушника, його професійна підготовка, рівень обізнаності з принципами роботи відповідних інформаційних ресурсів та порядком їх використання. Як правило, особа, яка вчиняє втручання в роботу автоматизованих систем, пристосовується до існуючих умов їх функціонування, враховує режим доступу до інформаційних ресурсів, порядок адміністрування та контроль за їх використанням [60, с. 69–70].

Тому, як слушно зазначають науковці, знання обстановки кримінального правопорушення дозволяє слідчому формувати обґрунтовані версії щодо особи правопорушника, механізму вчинення, його мотивів та цілей. У цьому контексті важливим елементом обстановки є умови функціонування інформаційних систем та організація діяльності органів і установ системи правосуддя, в яких вони використовуються. Середовище їх функціонування може включати дії або бездіяльність працівників, що сприяють підготовці, вчиненню або приховуванню протиправних дій, а також низку факторів суб'єктивного характеру, пов'язаних із рівнем професійної підготовки працівників, їх ставленням до виконання службових обов'язків та дотриманням правил інформаційної безпеки [12, с. 67; 186, с. 26].

У сучасних умовах функціонування системи правосуддя автоматизовані інформаційні ресурси відіграють важливу роль у забезпеченні діяльності судів, органів досудового розслідування та інших установ. Саме тому незаконне втручання в роботу таких систем може створювати можливість для неправомірної зміни, блокування або видалення інформації, що міститься в них, а також для досягнення інших протиправних цілей. У результаті таких дій особа отримує можливість впливати на інформаційні процеси, які забезпечують функціонування органів системи правосуддя, що може призводити до порушення встановленого порядку їх діяльності [25, с. 27]. Конкретизуючи зазначене, варто підкреслити, що будь-яке кримінальне правопорушення цієї категорії відбувається у певних просторово-часових умовах. Місцем його вчинення можуть бути службові приміщення органів та установ системи

правосуддя, де розташовані робочі станції користувачів, серверне обладнання або інші технічні засоби, за допомогою яких забезпечується функціонування автоматизованих систем. Водночас розвиток інформаційних технологій зумовлює можливість здійснення незаконного втручання дистанційно, що розширює просторові межі події та ускладнює встановлення її безпосереднього місця [139, с. 7].

Певні особливості має і часовий аспект вчинення такого кримінального правопорушення. У низці випадків втручання здійснюється у період активного використання інформаційних систем, коли значна кількість користувачів працює з відповідними ресурсами, що може ускладнювати своєчасне виявлення протиправних змін. В інших ситуаціях протиправні дії можуть вчинятися у позаробочий час або у періоди мінімального навантаження на інформаційні системи, коли контроль за їх функціонуванням є менш інтенсивним.

Обстановці незаконного втручання в роботу автоматизованих систем можуть сприяти й окремі організаційні та технічні чинники. Серед них варто виділити недостатній рівень захисту інформаційних ресурсів, недосконаліть систем контролю доступу, використання застарілого програмного забезпечення, неналежне адміністрування інформаційних систем, а також недбале виконання працівниками своїх службових обов’язків у сфері інформаційної безпеки. Сукупність зазначених умов створює середовище, у якому особа може реалізувати протиправний намір та здійснити втручання у функціонування автоматизованих систем.

Разом із цим, незалежно від виду кримінального правопорушення, його тяжкості та наслідків, у навколишній обстановці завжди залишаються певні відображення події – сліди, що виникають у результаті змін у матеріальному або інформаційному середовищі. Не є винятком і незаконне втручання в роботу автоматизованих систем в органах та установах системи правосуддя, унаслідок якого утворюються сліди, що містять криміналістично значущу інформацію про обставини вчинення кримінального правопорушення. Їх виявлення, фіксація та аналіз у поєднанні з іншими джерелами доказової інформації дають змогу

слідчому обрати найбільш доцільні засоби й тактичні прийоми розкриття та розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя [150, с. 12].

Практика розслідування кримінальних правопорушень, пов'язаних із незаконним втручанням у функціонування автоматизованих систем, свідчить про те, що значна частина працівників правоохоронних органів не завжди повною мірою орієнтується у різновидах слідів, які залишаються внаслідок такого втручання, та не завжди вживає достатніх заходів щодо їх своєчасного виявлення, належної фіксації й процесуального закріплення. Своєю чергою, це зумовлює потребу більш детального дослідження слідової картини зазначеного кримінального правопорушення.

Дослідження слідової картини має важливе значення для розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя, оскільки вона безпосередньо пов'язана з іншими елементами криміналістичної характеристики цього правопорушення, зокрема особою правопорушника, умовами та способом вчинення протиправних дій. Водночас вона виконує істотну організаційну й тактичну функцію, сприяючи визначенню напрямів пошуку доказової інформації та вибору ефективних засобів документування таких дій.

Типові сліди кримінального правопорушення розуміються як будь-які зміни середовища, що виникають унаслідок його вчинення [63, с. 16]. Сліди становлять різноманітні зміни в навколишній обстановці, які перебувають у причинному зв'язку з подією правопорушення. Водночас до них належать і сліди пам'яті людини, що проявляються у формі уявних образів та відображають сприйняті обставини події [152, с. 85]. З огляду на це сліди незаконного втручання в роботу автоматизованих систем у сфері правосуддя доцільно вже традиційно поділяти на матеріальні та ідеальні. У сукупності вони формують слідову картину цього кримінального правопорушення. Так, під слідовою картиною у криміналістиці пропонується розуміти сукупність криміналістично значущої інформації про матеріальні та ідеальні відображення події

правопорушення, що виникають у результаті дій її учасників і відображають обставини (місце, час, умови та спосіб) його вчинення [74, с. 253].

Сліди кримінального правопорушення можуть проявлятися у різних формах, зокрема у вигляді змін у матеріальному середовищі, слідів-відображень, предметів – речових доказів, документів (у паперовій чи електронній формі), слідів пам'яті осіб, мікрочастинок, а також звукових чи інших інформаційних відображень події [63, с. 16].

Для розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя особливого значення набуває встановлення найбільш характерних матеріальних та ідеальних слідів, що утворюються внаслідок таких протиправних дій. З урахуванням специфіки досліджуваного правопорушення доцільно виділити дві основні групи слідів:

1) сліди несанкціонованого доступу до автоматизованих систем та інформаційних ресурсів органів і установ системи правосуддя;

2) сліди внесення змін до інформації, що обробляється або зберігається в таких системах, чи порушення їх нормального функціонування.

Сліди несанкціонованого доступу можуть мати як матеріальний, так і ідеальний характер. До матеріальних належать, зокрема, електронні журнали обліку доступу до системи, дані про авторизацію користувачів, записи мережевої активності, інформація про використані облікові записи, IP-адреси, а також технічні сліди роботи програмного забезпечення чи спеціальних технічних засобів. До цієї ж групи можуть належати електронні носії інформації, комп'ютерна техніка, мобільні пристрої, на яких зберігаються відомості про здійснені дії. Ідеальні сліди зберігаються у пам'яті осіб, які мали доступ до відповідних інформаційних систем, здійснювали їх адміністрування або могли спостерігати обставини, пов'язані з несанкціонованим використанням таких систем. Сліди внесення змін до інформації або порушення роботи автоматизованих систем також можуть проявлятися у вигляді різноманітних електронних даних, зокрема змін у базах даних, редагування або видалення інформації, появи нових записів у системі, а також у вигляді технічних збоїв чи

аномальної роботи програмного забезпечення. Важливими джерелами доказової інформації можуть бути резервні копії баз даних, системні журнали, службові повідомлення програмного забезпечення, електронне листування, внутрішні службові документи установ системи правосуддя.

Як зазначається у криміналістичній літературі, для типових кримінальних правопорушень, пов'язаних із службовою діяльністю, типовими є різноманітні і матеріальні сліди, серед яких особливе місце займають документи (у паперовій та електронній формі), технічні засоби, за допомогою яких здійснювалися відповідні дії, комп'ютерна техніка, електронні носії інформації, обстановка робочого місця, транспортні засоби, грошові кошти або інше майно, а також електронні (комп'ютерні) сліди [141, с. 12]. Як вище зазначалось, зазначені положення повною мірою стосуються і кримінальних правопорушень, пов'язаних із незаконним втручанням у функціонування автоматизованих систем у сфері правосуддя.

Найбільш інформативними матеріальними слідами таких протиправних дій є електронні документи та інші дані, що зберігаються в автоматизованих системах, базах даних і журналах обліку доступу. До них належать записи про авторизацію користувачів, інформація про час входу до системи, дані про виконані операції, журнали системних подій, відомості про зміну, видалення чи внесення нових даних до відповідних інформаційних ресурсів. Саме ці відомості дозволяють встановити характер дій користувача, послідовність операцій та часові параметри втручання. У науковій літературі справедливо підкреслюється, що використання даних, зафіксованих у документах чи електронних системах, створених або використаних самим правопорушником, може істотно ускладнити подальше заперечення відповідних обставин з боку сторони захисту, оскільки такі відомості мають об'єктивний характер і формуються безпосередньо в процесі функціонування інформаційних систем [148, с. 51].

Особливе значення для встановлення обставин незаконного втручання мають інформаційні ресурси автоматизованих систем органів та установ системи правосуддя. До них належать, зокрема, бази даних автоматизованої системи

документообігу суду, електронні реєстри судових рішень, системи обліку процесуальних документів, внутрішні інформаційні системи правоохоронних органів, а також інші програмно-інформаційні комплекси, що використовуються у діяльності судів. Аналіз таких ресурсів дозволяє встановити, чи здійснювалися несанкціоновані зміни у відомостях, чи відбувалося видалення або коригування інформації, а також визначити облікові записи користувачів, за допомогою яких виконувалися відповідні операції.

Важливе значення можуть мати і документи організаційно-службового характеру, що відображають порядок функціонування інформаційних систем, регламент доступу до них, розподіл повноважень між працівниками, журнали обліку використання технічних засобів, службові записки, акти перевірок, внутрішні звіти щодо функціонування інформаційних систем та повідомлення про технічні збої. Пропонуємо здійснити певну класифікацію відповідних документів.

Передусім, слід вказати про документи, що засвідчують повноваження особи щодо доступу до автоматизованих систем. До цієї групи належать: документи про призначення особи на посаду, переведення чи звільнення з неї (накази, розпорядження, витяги з кадрових документів); посадові інструкції, службові регламенти та інші документи, які визначають коло функціональних обов’язків працівника; документи, що регламентують надання доступу до інформаційних систем, визначають рівень прав користувача та порядок використання відповідних інформаційних ресурсів.

Наступним необхідно зазначити про документи, що регулюють порядок функціонування автоматизованих систем та доступ до них. До них можна віднести: внутрішні нормативні акти органів та установ системи правосуддя, що визначають правила користування автоматизованими інформаційними системами; технічні регламенти, інструкції з експлуатації програмного забезпечення, положення про адміністрування систем; документи, що містять відомості про порядок створення облікових записів користувачів, їх блокування або зміну рівня доступу.

Документи та електронні дані, що відображають факт використання автоматизованих систем. До цієї групи можуть належати: журнали реєстрації доступу до інформаційних систем; системні журнали подій, які містять відомості про виконані користувачами операції; записи про авторизацію користувачів, час входу до системи, використані облікові записи та технічні параметри підключення; службові повідомлення програмного забезпечення щодо помилок або збоїв у роботі системи.

Документи та цифрові дані, що свідчать про зміну або видалення інформації в автоматизованих системах. До них можуть належати: записи у базах даних, які відображають внесення змін до інформації; резервні копії інформаційних ресурсів, що дозволяють встановити первинний стан даних; технічні звіти або акти перевірок щодо виявлених порушень у роботі інформаційних систем; електронна інформація, що міститься на комп'ютерах, мобільних пристроях або інших носіях даних (жорсткі диски, флеш-накопичувачі, серверні сховища).

Інші документи, що можуть містити відомості про обставини незаконного втручання. До них можна віднести службове листування, повідомлення про технічні несправності або несанкціоновані дії в системі, акти внутрішніх перевірок, пояснення працівників, а також документи, що спростовують або підтверджують певні версії щодо причин порушення нормального функціонування автоматизованих систем.

Документи, які можуть містити інформацію про незаконне втручання у функціонування автоматизованих систем у сфері правосуддя, доцільно також класифікувати залежно від суб'єкта їх створення. За цією ознакою можна виділити: документи та електронні записи, сформовані безпосередньо користувачем інформаційної системи; документи, створені адміністраторами систем або підрозділами інформаційних технологій; документи, складені іншими суб'єктами (наприклад, службами технічної підтримки, органами внутрішнього контролю, установами, що здійснюють технічне обслуговування програмного забезпечення). Крім того, значення можуть мати електронні носії

інформації, персональні комп’ютери, серверне обладнання, мобільні пристрої, змінні носії даних, на яких можуть міститися програми віддаленого доступу, спеціальне програмне забезпечення, файли з технічними налаштуваннями або інші відомості, що відображають дії особи, спрямовані на отримання доступу до інформаційних систем чи зміну інформації, що в них обробляється.

На підставі результатів дослідження практики розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя, поєднаного з корупційними правопорушеннями, нами виділено ще одну окрему групу об’єктів, що формують слідову картину досліджуваного кримінального правопорушення.

До таких об’єктів належать:

– грошові кошти, передані службовій або іншій заінтересованій особі за незаконне втручання в роботу автоматизованих систем або за створення умов для такого втручання. До цієї групи належать, зокрема, грошові купюри, що використовуються під час проведення негласних слідчих (розшукових) дій та можуть бути помічені спеціальними хімічними речовинами. У протоколах обшуку або огляду місця події, як правило, фіксується кількість купюр, їх номінал, серійні номери та інші ідентифікаційні ознаки;

– ватні тампони зі змивами спеціальних хімічних речовин, відібрані з поверхні долонь рук підозрюваної особи, а також змиви з поверхні робочого столу, комп’ютерної техніки або інших предметів, що могли контактувати з грошовими коштами чи іншими матеріальними носіями неправомірної вигоди;

– цифрові носії інформації, які містять так звані цифрові сліди незаконного втручання в роботу автоматизованих систем. До таких об’єктів належать мобільні телефони підозрюваних осіб, SIM-картки, карти пам’яті, жорсткі диски комп’ютерів, системні блоки, ноутбуки, флеш-накопичувачі, а також інші електронні носії інформації;

– документи, що можуть підтверджувати як факт отримання неправомірної вигоди, так і обставини незаконного втручання в роботу автоматизованих систем. До таких документів належать: платіжні квитанції або банківські

документи (у випадках передачі неправомірної вигоди у безготівковій формі); чеки, товарні ярлики або етикетки від придбаних речей; рахунки ресторанів, готелів чи інших закладів; документи, що підтверджують отримання кредитів або здійснення значних фінансових операцій; документи про придбання або оформлення права власності на автомобілі, квартири чи інше майно; особисті записи підозрюваних осіб (листи, нотатки, записки тощо), які можуть містити відомості про обставини отримання неправомірної вигоди або домовленості щодо втручання в роботу автоматизованих систем.

Наступним складником слідової картини незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя є ідеальні сліди. Як вже було зазначено, під ними розуміють відображення події кримінального правопорушення у свідомості людини, що проявляється у вигляді уявних образів та збереженої в пам'яті інформації про певні обставини, дії або поведінку осіб. Такі відображення виникають у процесі сприйняття людиною навколишніх явищ і подій, та які можуть бути відтворені під час проведення певних слідчих (розшукових) та інших процесуальних дій [37, с. 7]. Як слушно зазначається у криміналістичній літературі, важливим джерелом інформації про обставини вчинення службових кримінальних правопорушень є відомості, якими володіють працівники установ, відвідувачі, користувачі інформаційних ресурсів, а також інші свідки події та особи, обізнані з особливостями діяльності органу чи установи [150, с. 12]. Такі відомості можуть стосуватися як обставин використання інформаційних систем, так і поведінки осіб, причетних до їх експлуатації або обслуговування.

Ідеальні сліди у кримінальних провадженнях досліджуваної категорії формуються в пам'яті осіб, які могли постійно чи тимчасово спостерігати процес роботи з автоматизованими системами або мають інформацію про порядок їх функціонування та використання. До таких осіб можуть належати працівники органів та установ системи правосуддя, які використовують відповідні інформаційні системи у службовій діяльності, а також інші співробітники, що мають відношення до організації документообігу чи технічного супроводження

електронних інформаційних ресурсів. Крім того, важливі відомості можуть міститися у пам’яті осіб, які безпосередньо взаємодіяли з автоматизованими системами або спостерігали обставини їх використання. Наприклад, це можуть бути працівники, які перебували в одному службовому приміщенні з особою, що здійснювала роботу за комп’ютером, або особи, які помітили нетипові дії під час роботи з відповідними інформаційними ресурсами, появу сторонніх програм чи незвичайну поведінку технічних засобів.

Отже, ідеальні сліди можуть бути отримані як з пам’яті свідків, так і осіб, причетних до протиправних дій, а також інших осіб, які володіють інформацією про обставини використання автоматизованих систем. До неї, зокрема, можуть належати:

– відомості, що зберігаються у пам’яті працівників органів та установ системи правосуддя, які спостерігали процес роботи з автоматизованими системами або перебували поруч із особою, що здійснювала відповідні дії;

– інформація, якою володіють працівники підрозділів інформаційних технологій або системні адміністратори щодо обставин надання доступу до інформаційних ресурсів, зміни облікових записів чи технічних параметрів системи;

– відомості осіб, які брали участь у технічному обслуговуванні або налаштуванні програмного забезпечення, що використовується в органах та установах системи правосуддя;

– інформація, що зберігається у пам’яті осіб, які могли помітити прояви порушення нормального функціонування інформаційних систем, зокрема збої у роботі програмного забезпечення, появу нових або змінених записів у базах даних;

– відомості осіб, які виявили ознаки несанкціонованого доступу до інформаційних систем або повідомили про такі факти керівництво установи чи правоохоронні органи;

– інформація, якою володіють особи, що перебувають у службових чи особистих відносинах із правопорушником і могли знати про його наміри або обставини підготовки до незаконного втручання.

Таким чином, типових носіїв ідеальних слідів незаконного втручання в роботу автоматизованих систем у сфері правосуддя доцільно поділяти на кілька груп:

– працівники органів та установ системи правосуддя;

– працівники підрозділів інформаційних технологій та системні адміністратори;

– особи, які здійснювали технічне обслуговування або налаштування програмного забезпечення;

– особи, які спостерігали обставини використання автоматизованих систем;

– особи, які виявили ознаки незаконного втручання або повідомили про нього відповідні органи.

Інформація, що зберігається у пам’яті таких осіб, має важливе значення для встановлення механізму протиправних дій, послідовності подій, умов функціонування автоматизованих систем у відповідний період та кола осіб, які могли бути причетні до незаконного втручання. Отримання і аналіз відомостей у поєднанні з матеріальними слідами дозволяє більш повно відтворити обставини кримінального правопорушення та забезпечити ефективне доказування у кримінальному провадженні.

Висновки до розділу 1

1. Електронне судочинство в Україні є закономірним результатом цифрової трансформації судової влади та одним із напрямів модернізації механізму здійснення правосуддя. Функціональне призначення електронного судочинства охоплює широкий спектр взаємопов'язаних напрямів, зокрема, організаційно-управлінську функцію (забезпечує впорядкування внутрішніх процесів у суді); документообігову (створює належні умови для повноцінного обігу процесуальних документів в електронній формі); комунікаційну (формує сучасні канали взаємодії між судом і учасниками процесу); ідентифікаційну (гарантує достовірність суб'єкта електронної процесуальної дії); інформаційну та аналітичну (забезпечує накопичення, систематизацію й використання даних для належної організації судової діяльності); гарантійну (сприяє розширенню доступу до правосуддя); функцію відкритості та підзвітності (посилює публічність і контрольованість судової влади); захисту даних (створює умови для безпечного функціонування електронної судової системи). Сукупність зазначених функцій свідчить, що електронне судочинство є багаторівневим правовим механізмом, спрямованим не лише на технічне вдосконалення судової діяльності, а й на підвищення ефективності, прозорості та доступності правосуддя в цілому.

2. Вивчення матеріалів кримінальних проваджень засвідчило, що серед правопорушників переважають чоловіки (79,5%), тоді як частка жінок становить 20,5%; громадяни України (100%), значна частина яких раніше не притягувалася до кримінальної відповідальності (96,1%), що свідчить про відсутність вираженої загальнокримінальної спрямованості та про специфічний, переважно ситуативно-службовий або професійно зумовлений характер протиправної поведінки; віком 30–50 років (71%), з повною або базовою вищою освітою (68%), що у тому числі обумовлено необхідністю володіння навичками роботи з системами, комп'ютерною технікою, електронними документами, засобами авторизації. Важливе криміналістичне значення мають спеціальні

характеристики – службове становище, наявність доступу до автоматизованих систем, мотиви і мета протиправної діяльності, рівень технічної обізнаності, а в окремих випадках – наявність достатніх фінансових можливостей для залучення інших осіб, придбання спеціальних програмних засобів чи організації прихованого впливу на функціонування системи.

3. Предмет незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя – відомості про реєстрацію та рух судових справ, дані автоматизованого розподілу справ між суддями, електронні процесуальні документи, службову інформацію щодо організації роботи органів системи правосуддя, персональні дані учасників процесу, а також технічні дані і системні журнали, які фіксують дії користувачів та зміни в інформаційному середовищі.

4. З’ясовано, що у переважній більшості випадків такі дії мають заздалегідь спланований характер. При цьому найчастіше підготовка до незаконного втручання охоплює визначення конкретної автоматизованої системи або її окремого функціонального модуля як об’єкта впливу, попереднє вивчення порядку її функціонування та алгоритмів роботи, пошук осіб, які мають доступ до системи або можуть сприяти його отриманню, незаконне одержання чи використання облікових даних доступу, зокрема логінів, паролів, електронних ключів або токенів авторизації, розподіл ролей між співучасниками, підготовку засобів конспірації та приховування цифрових слідів, вибір часу найменшого контролю за роботою системи, а також узгодження дій із заінтересованими особами, які розраховують на відповідний результат втручання.

Визначено, що до основних способів безпосереднього вчинення цього кримінального правопорушення належать внесення неправдивих відомостей до автоматизованої системи документообігу суду або несвоєчасне внесення відомостей до відповідних автоматизованих систем, а також здійснення несанкціонованих дій з інформацією, що міститься в них, чи інше незаконне втручання в їх роботу службовими особами, які мають право доступу до таких

систем, або іншими особами шляхом використання стороннього чи неправомірно отриманого доступу.

Приховування незаконного втручання в роботу автоматизованих систем у сфері правосуддя зазвичай здійснюється шляхом внесення до системи недостовірних або змінених даних (44,9%), використання чужих облікових записів або спільного використання засобів авторизації (39,3%), видалення чи модифікації файлів, електронних записів або журналів подій (36,5%), створення фіктивних службових документів для формального пояснення змін у системі (24,8%), інсценування технічних збоїв чи помилок програмного забезпечення (21,7%), а також перекладання відповідальності на інших працівників або сторонніх осіб (18,6%). Зазначене дає підстави стверджувати, що спосіб учинення відповідного кримінального правопорушення охоплює не лише дії з безпосереднього протиправного впливу на систему, а й комплекс підготовчих і маскувальних заходів, спрямованих на унеможливлення або істотне ускладнення виявлення факту втручання та встановлення винної особи.

5. Обстановка вчинення незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя формується під впливом сукупності організаційних, службових, технічних та інформаційних чинників, які визначають як можливість реалізації злочинного наміру, так і особливості подальшого виявлення його слідів. Узагальнення матеріалів кримінальних проваджень та результатів опитування практичних працівників дало підстави встановити, що у 62,8% випадків визначальне значення для вчинення такого кримінального правопорушення має наявність у особи службового або іншого легітимізованого доступу до автоматизованої системи, у 48,6% – недоліки внутрішнього контролю за обліковими записами, електронними ключами та іншими засобами авторизації, у 44,1% – обізнаність правопорушника з порядком функціонування конкретної автоматизованої системи або її окремих модулів, у 37,9% – можливість вчинення дій у період зниженого контролю за роботою системи, а у 33,4% – неналежний рівень технічного аудиту, журналювання подій або моніторингу змін в інформаційному середовищі. Водночас у 29,7% випадків

вчиненню незаконного втручання сприяло поєднання службових можливостей із технічною допомогою інших осіб, зокрема адміністраторів, спеціалістів чи працівників, обізнаних із функціонуванням відповідних інформаційних ресурсів. Відповідні показники свідчать, що обстановка вчинення цього кримінального правопорушення зазвичай пов’язана з використанням наявних організаційних та технічних вразливостей у діяльності органів та установ системи правосуддя.

6. Слідова картина незаконного втручання в роботу автоматизованих систем у сфері правосуддя має складний, комбінований характер і охоплює як матеріальні, так і ідеальні сліди. Серед матеріальних слідів виділено дві основні групи: 1) сліди несанкціонованого доступу до автоматизованих систем та інформаційних ресурсів органів і установ системи правосуддя; 2) сліди внесення змін до інформації, що обробляється або зберігається в таких системах, а також порушення їх нормального функціонування. Узагальнення матеріалів кримінальних проваджень і результатів опитування практичних працівників дає підстави стверджувати, що найчастіше виявляються електронні записи про входи до системи та факти авторизації користувачів (61,8%), зміни облікових даних або параметрів доступу (34,7%), використання чужих облікових записів чи засобів автентифікації (39,5%), зміни в базах даних автоматизованої системи (48,9%), журнали подій і лог-файли, що фіксують послідовність дій користувачів (57,6%), а також сліди видалення, блокування, модифікації чи копіювання інформації (43,2%). У 29,4% випадків фіксувалися й інші технічні ознаки, що відображали факт, спосіб та наслідки незаконного впливу на автоматизовану систему, зокрема зміни конфігурації програмного забезпечення, нехарактерна мережева активність, поява нових файлів або сторонніх програмних компонентів.

З’ясовано, що важливе криміналістичне значення мають ідеальні сліди. Типовими носіями таких слідів є працівники органів та установ системи правосуддя (46,2%), працівники підрозділів інформаційних технологій і системні адміністратори (33,9%), особи, які здійснювали технічне обслуговування або налаштування програмного забезпечення (15,2%), працівники, що безпосередньо

або опосередковано спостерігали обставини використання автоматизованих систем (28,7%), а також особи, які виявили ознаки незаконного втручання чи повідомили про них відповідні органи (24,5%). Значення ідеальних слідів полягає в тому, що вони дозволяють відтворити обстановку вчинення діяння, послідовність дій правопорушника, особливості доступу до інформаційної системи, характер змін у її роботі та поведінку осіб, причетних до незаконного втручання. Водночас у 41,1% випадків саме поєднання ідеальних слідів із даними технічних носіїв та електронних журналів подій створює найбільш надійну основу для встановлення механізму кримінального правопорушення та ідентифікації причетної особи.

РОЗДІЛ 2.
ОРГАНІЗАЦІЯ РОЗСЛІДУВАННЯ НЕЗАКОННОГО ВТРУЧАННЯ В РОБОТУ АВТОМАТИЗОВАНИХ СИСТЕМ В ОРГАНАХ ТА УСТАНОВАХ СИСТЕМИ ПРАВОСУДДЯ

2.1. Обставини, що підлягають встановленню під час розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя

У сучасних умовах функціонування електронного судочинства важливим завданням кримінальної юстиції стає забезпечення належного функціонування інформаційних систем судової гілки влади, зокрема систем електронного документообігу та автоматизованого розподілу судових справ. Зазначені процеси безпосередньо пов’язані з удосконаленням механізмів організації досудового розслідування та посиленням процесуальних гарантій відповідно до європейських стандартів здійснення правосуддя [13, с. 160].

Передусім зазначимо, що із прийняттям та введенням у дію чинного КПК України відбулися істотні трансформації майже всіх інститутів кримінального процесу. Не стала винятком і процедура початку досудового розслідування, яка за положеннями КПК України 1960 року розглядалася як окрема стадія кримінального процесу під назвою «порушення кримінальної справи». У цьому контексті Ю. П. Аленін звертає увагу на те, що в діяльності правоохоронних органів однією з проблемних залишається необхідність застосування диференційованого підходу під час розгляду заяв і повідомлень про кримінальні правопорушення. Своєю чергою, це зумовлено тим, що кількість відповідних звернень від громадян та юридичних осіб постійно зростає, тоді як механізм їх належної перевірки на законодавчому рівні залишається недостатньо врегульованим [2, с. 199]. На думку дослідника, подальше вдосконалення положень ст. 214 КПК України має передбачати можливість здійснення

перевірки отриманих заяв і повідомлень, обов'язок уповноважених посадових осіб приймати процесуальне рішення шляхом постановлення відповідної постанови слідчим або прокурором про початок досудового розслідування чи про відмову в його проведенні, а також визначення обставин, що виключають необхідність здійснення такого розслідування [2, с. 203].

Запроваджена законодавцем можливість внесення відомостей до ЄРДР без проведення попередньої перевірки отриманої інформації спричинила появу певних проблем у практичній діяльності правоохоронних органів. Зокрема, це створює передумови для зловживань, пов'язаних із поданням необґрунтованих або свідомо неправдивих заяв так званими «недобросовісними заявниками». У деяких випадках такі звернення можуть бути спрямовані проти конкретних посадових осіб з метою чинення на них тиску, дискредитації чи помсти. Крім того, трапляються ситуації, коли подані заяви мають замовний характер і використовуються як інструмент впливу на прийняття певних процесуальних або управлінських рішень. Водночас варто зазначити, що і за часів існування інституту дослідчої перевірки в межах попереднього кримінально-процесуального законодавства на практиці також спостерігалися випадки суб'єктивного підходу, які проявлялися у безпідставній відмові у порушенні кримінальної справи. Проте новий порядок початку досудового розслідування, закріплений у чинному КПК України, фактично усунув інститут дослідчої перевірки заяв та повідомлень про кримінальні правопорушення. У результаті основний тягар перевірки отриманої інформації покладається безпосередньо на слідчого. У практичній площині це призводить до ситуації, коли слідчі змушені реагувати навіть на очевидно безпідставні або абсурдні повідомлення, що потребують формального внесення до ЄРДР. Водночас значні ресурси правоохоронних органів повинні бути спрямовані на розслідування нетяжких, тяжких та особливо тяжких злочинів. Така ситуація негативно позначається на ефективності досудового розслідування та не сприяє підвищенню рівня захисту прав і законних інтересів громадян у кримінальному провадженні [163, с. 184].

Разом із тим, не заглиблюючись у наукову дискусію щодо позитивних чи негативних наслідків запроваджених змін, слід зазначити, що інститут початку досудового розслідування, як і будь-який інший, передбачений КПК України, має як свої переваги, так і певні проблемні аспекти, які проявляються у процесі його практичної реалізації.

Так, сьогодні за законодавством початком кримінального провадження є момент внесення відомостей до ЄРДР, з якого розпочинається досудове розслідування. Положення про реєстр, порядок його формування та ведення затверджуються Офісом Генерального прокурора за погодженням з МВС України, СБУ, ДБР, органом Бюро економічної безпеки України [126]. Загальний порядок реєстрації кримінального правопорушення у ЄРДР передбачає внесення відомостей про: 1) дату надходження заяви, повідомлення про кримінальне правопорушення або виявлення з іншого джерела обставин, що можуть свідчити про вчинення кримінального правопорушення; 2) прізвище, ім'я, по батькові (найменування) потерпілого або заявника; 3) інше джерело, з якого виявлені обставини, що можуть свідчити про вчинення кримінального правопорушення; 4) короткий виклад обставин, що можуть свідчити про вчинення кримінального правопорушення, наведених потерпілим, заявником чи виявлених з іншого джерела; 5) попередня правова кваліфікація кримінального правопорушення з зазначенням статті (частини статті) КК України; 6) прізвище, ім'я, по батькові та посада службової особи, яка внесла відомості до реєстру, а також слідчого, прокурора, який вніс відомості до реєстру та/або розпочав досудове розслідування; 7) інші обставини, передбачені Положенням про ЄРДР, порядком його формування та ведення [126]. Проведення слідчих (розшукових) дій до внесення таких відомостей, як правило, не допускається, за винятком огляду місця події. У криміналістичній літературі початковий етап розслідування розглядається як самостійний період досудового розслідування, у межах якого вирішуються першочергові завдання щодо з'ясування факту вчинення кримінального правопорушення, встановлення початкових обставин події та формування первинної доказової бази [20, с. 43]. Зокрема, О. С. Задорожній

визначає початковий етап як частину процесу розслідування, у межах якої вирішуються ключові процесуальні завдання [34, с. 271]; А. Ф. Волобуєв пов’язує його зі станом розслідування, що характеризується ступенем виконання окремих завдань та прийнятими процесуальними рішеннями [20, с. 44]; В. С. Кузьмічов поділяє процес розслідування на початковий і наступний етапи, зазначаючи, що перший охоплює період від початку кримінального провадження до проведення основного комплексу невідкладних процесуальних дій [73, с. 129].

На наш погляд, ефективність розслідування кримінальних правопорушень, пов’язаних із незаконним втручанням у роботу автоматизованих систем органів та установ системи правосуддя, безпосередньо залежить від чіткого визначення обставин, які підлягають встановленню та доказуванню на початковому етапі розслідування. Саме ці обставини визначають спрямованість доказування, впливають на побудову слідчих версій, вибір комплексу слідчих (розшукових) і негласних слідчих (розшукових) дій, а також перелік необхідних експертних досліджень у сфері комп’ютерно-технічної експертизи та кібербезпеки. Водночас безпідставне розширення предмета доказування може призводити до штучного ускладнення кримінального провадження, затягування строків досудового розслідування та надмірного навантаження на його учасників унаслідок накопичення інформації, що не має істотного значення для встановлення істини. Не менш негативними є наслідки необґрунтованого звуження предмета доказування, оскільки це може спричинити неповноту дослідження обставин правопорушення та знизити переконливість доказової бази під час судового розгляду [9, с. 29].

У науковій літературі питання щодо визначення предмета доказування розглядається неоднаково. В. О. Попелюшко визначає предмет кримінально-процесуального доказування як систему фактів та обставин, що мають матеріально-правове і процесуальне значення та утворюють необхідну фактичну основу для остаточного вирішення кримінального провадження [111, с. 113]. На думку С. М. Стахівського, предмет доказування становить передбачену законом сукупність обставин, які мають бути встановлені у кожному кримінальному

провадженні з метою його правильного вирішення [157, с. 32]. У свою чергу, В. В. Вапнярчук підкреслює, що предмет доказування охоплює визначені законом і суб'єктом доказування обставини кримінального правопорушення, які мають правове значення та впливають на прийняття процесуальних рішень [14, с. 240]. Заслуговує на увагу і позиція В. В. Тіщенка, який зазначає, що на початковому етапі розслідування визначення кола обставин доцільно здійснювати за допомогою системи базових запитань: хто, що, де, коли, яким способом, з якою метою та за чиєї участі. Такий підхід дозволяє структурувати інформацію про подію кримінального правопорушення та визначити напрями подальшого доказування [168, с. 142].

Нормативно-правове закріплення предмета доказування міститься у ст. 91 КПК України, відповідно до якої у кримінальному провадженні підлягають доказуванню подія кримінального правопорушення, винуватість особи, мотив і мета вчинення діяння, характер і розмір завданої шкоди, а також інші обставини, що мають значення для прийняття законного та обґрунтованого процесуального рішення. У контексті досудового розслідування незаконного втручання в роботу автоматизованих систем органів правосуддя встановлення події кримінального правопорушення нерозривно пов'язане з дослідженням функціонування відповідних інформаційних ресурсів, зокрема систем автоматизованого документообігу суду, електронного розподілу судових справ та інших цифрових компонентів судової гілки влади. У таких випадках предмет доказування охоплює не лише традиційні обставини кримінального правопорушення (час, місце, спосіб його вчинення), а й технічні аспекти функціонування інформаційної системи, характер змін у її роботі, наявність несанкціонованого доступу, модифікації або блокування інформації.

Разом із тим практика діяльності органів досудового розслідування свідчить, що інформація, яка надходить на початковому етапі розслідування кримінальних правопорушень, пов'язаних із втручанням у роботу інформаційних систем правосуддя, часто має фрагментарний характер або містить лише загальні відомості про можливі технічні збої чи підозрілі дії

користувачів. У зв'язку з цим первинна оцінка таких повідомлень потребує проведення відповідних технічних перевірок, аналізу журналів подій інформаційних систем та інших цифрових даних.

Таким чином, акцентуємо увагу на тому, що ефективність розслідування кримінальних правопорушень, пов'язаних із незаконним втручанням у роботу автоматизованих систем органів та установ системи правосуддя, значною мірою залежить від правильного визначення кола обставин, які підлягають встановленню на початковому етапі досудового розслідування.

У кримінальних провадженнях, пов'язаних із незаконним втручанням у роботу автоматизованих систем органів та установ системи правосуддя, найбільш типовими підставами внесення відомостей до ЄРДР є: заява або повідомлення працівників суду, органів прокуратури, інших працівників системи правосуддя чи користувачів інформаційних систем про виявлені ознаки несанкціонованого доступу або порушення роботи відповідних інформаційних ресурсів; службові повідомлення працівників технічних підрозділів або адміністраторів інформаційних систем щодо фіксації несанкціонованих змін у функціонуванні програмного забезпечення чи баз даних; самостійне виявлення слідчим або прокурором ознак кримінального правопорушення під час розслідування іншого кримінального провадження; матеріали оперативних підрозділів щодо можливого втручання в роботу інформаційних систем правосуддя; відомості, отримані з відкритих джерел, зокрема з медіа або мережі Інтернет, включно з матеріалами журналістських розслідувань чи повідомленнями користувачів інформаційних платформ.

Суттєвою вимогою до рішення про початок досудового розслідування є його своєчасність, оскільки зволікання створює сприятливі умови для зацікавлених осіб приховати факти несанкціонованого доступу чи здійснити інші дії, спрямовані на протидію встановленню істини [70, с. 235]. Вимога своєчасності тісно пов'язана з іншою обов'язковою властивістю процесуального рішення – законністю та обґрунтованістю. Помилки на початковому етапі кримінального провадження можуть призвести як до безпідставного обмеження

прав особи, так і до уникнення відповідальності особами, причетними до незаконного втручання в роботу інформаційних систем.

Тому початковий етап розслідування у кримінальних провадженнях щодо незаконного втручання в роботу автоматизованих систем органів правосуддя має бути спрямований на виявлення, збереження та процесуальне закріплення цифрових доказів. Організація роботи слідчого на цьому етапі повинна передбачати: встановлення технічних характеристик інформаційної системи, у роботу якої було здійснено втручання; з'ясування порядку доступу до системи та рівнів авторизації користувачів; аналіз журналів подій (логів), що відображають дії користувачів у системі; встановлення факту зміни, блокування або видалення інформації; виявлення програмних або технічних засобів, за допомогою яких було здійснено втручання; вилучення серверного обладнання, комп'ютерної техніки та інших електронних носіїв інформації; призначення комп'ютерно-технічних експертиз; перевірку можливого зв'язку відповідного епізоду з іншими фактами втручання у роботу інформаційних систем.

Особливу увагу слід приділяти встановленню характеру і наслідків втручання у роботу автоматизованої системи. Залежно від конкретної ситуації необхідно з'ясувати: чи призвело втручання до зміни алгоритму функціонування системи; чи були внесені несанкціоновані зміни до баз даних; чи мало місце блокування або знищення електронної інформації; чи вплинуло втручання на результати автоматизованого розподілу судових справ між суддями; які саме технічні засоби або програмне забезпечення були використані для здійснення протиправних дій; які саме інформаційні ресурси або модулі системи були змінені чи пошкоджені.

Ще однією обставиною, що підлягає доказуванню у відповідній категорії кримінальних проваджень, є винуватість підозрюваного (обвинуваченого), форма вини, а також мотив і мета вчинення діяння. Доказування винуватості полягає не лише у встановленні факту здійснення певних дій щодо інформаційної системи, а й у доведенні того, що саме підозрювана особа мала реальну можливість отримати доступ до відповідних інформаційних ресурсів,

усвідомлювала протиправний характер своїх дій та передбачала їх наслідки. У зв’язку з цим необхідно встановити: службовий або фактичний статус особи в органі чи установі системи правосуддя; обсяг її повноважень щодо доступу до інформаційних систем; наявність технічної можливості здійснити відповідні дії; участь у налаштуванні, адмініструванні або обслуговуванні автоматизованої системи; фактичну причетність до внесення змін у програмне забезпечення або бази даних. Форма вини у таких провадженнях встановлюється шляхом аналізу сукупності доказів, що відображають обізнаність особи про характер і наслідки її дій. Про умисний характер втручання можуть свідчити використання спеціалізованого програмного забезпечення для отримання несанкціонованого доступу, свідоме обходження систем захисту інформації, модифікація або видалення електронних даних, використання чужих облікових записів або паролів, координація дій з іншими особами, а також спроби приховати сліди втручання.

Не менш важливим є встановлення мотиву і мети вчинення кримінального правопорушення. У кримінальних провадженнях цієї категорії мотив може бути пов’язаний із прагненням вплинути на результати автоматизованого розподілу судових справ, отримати доступ до службової або конфіденційної інформації, створити перешкоди у здійсненні правосуддя, а також із корисливими або іншими особистими інтересами. Мета таких дій може полягати у зміні результатів функціонування автоматизованої системи, приховуванні певних процесуальних дій, отриманні неправомірних переваг або створенні умов для ухилення від відповідальності.

Також із обставинами, що підлягають доказуванню, нерозривно пов’язується суб’єкт кримінального правопорушення – фізична осудна особа, яка досягла віку, з якого може наставати кримінальна відповідальність. Водночас специфіка цієї категорії кримінальних правопорушень зумовлює необхідність детального встановлення характеристик особи, зокрема її професійної підготовки, рівня технічних знань, службового становища, доступу до інформаційних ресурсів, а також зв’язків із іншими особами, які могли бути

залучені до реалізації відповідного механізму втручання. Узагальнення матеріалів кримінальних проваджень цієї категорії свідчить, що стороною обвинувачення зазвичай встановлюються такі обставини, що характеризують особу підозрюваного: наявність або відсутність судимостей, характеристика за місцем роботи або служби, відомості про доступ до інформаційних систем, а також дані щодо професійної діяльності та виконуваних службових функцій. Тобто, у кримінальних провадженнях щодо незаконного втручання в роботу автоматизованих систем органів та установ системи правосуддя встановлення даних про суб'єкта кримінального правопорушення повинно здійснюватися з урахуванням його фактичної ролі у механізмі протиправної діяльності, що забезпечує правильну кваліфікацію діяння, індивідуалізацію відповідальності та обґрунтованість процесуальних рішень.

Окремо слід звернути увагу на особливості здійснення досудового розслідування у випадках, коли кримінальне правопорушення, пов'язане з незаконним втручанням у роботу автоматизованих систем органів та установ системи правосуддя, вчинене особами, які відповідно до закону належать до спеціальної категорії суб'єктів кримінального провадження. Йдеться про осіб, перелік яких визначено у КПК України. До них, зокрема, належать: судді судів загальної юрисдикції, судді Конституційного Суду України, судді Вищого антикорупційного суду, а також присяжні під час виконання ними обов'язків у суді; Голова, заступник Голови та члени Вищої ради правосуддя; Голова, заступник Голови та члени Вищої кваліфікаційної комісії суддів України та ін. [72]. Застосування особливого порядку кримінального провадження щодо зазначених осіб означає, що досудове розслідування здійснюється за загальними правилами, однак із урахуванням спеціальних процесуальних гарантій. До таких особливостей належать, зокрема, спеціальний порядок повідомлення про підозру, встановлений для всіх категорій осіб, визначених у ст. 480 КПК України. Крім того, закон передбачає окремі правила щодо затримання та застосування запобіжних заходів у вигляді тримання під вартою чи домашнього арешту щодо окремих суб'єктів, зокрема суддів та народних депутатів України.

Особливі процесуальні вимоги встановлено також щодо проведення окремих слідчих (розшукових) дій та інших процесуальних заходів, які можуть обмежувати права і свободи таких осіб. Зокрема, це стосується проведення обшуку, огляду речей і документів, транспортних засобів, житла чи іншого володіння особи, а також заходів, пов'язаних із втручанням у приватне спілкування та обмеженням права на таємницю листування, телефонних розмов та інших видів кореспонденції. Аналогічні обмеження поширюються і на застосування негласних слідчих (розшукових) дій, що відповідно до закону можуть призводити до обмеження конституційних прав і свобод особи [4, с. 604–605]. Для правильного застосування положень ст. 480 КПК України насамперед необхідно достеменно встановити, чи має особа, щодо якої здійснюється кримінальне провадження, відповідний спеціальний правовий статус.

Обставинами, які можуть впливати на ступінь тяжкості відповідного кримінального правопорушення, є, зокрема, вчинення його повторно, за попередньою змовою групою осіб, із використанням службового становища, а також настання істотних наслідків для функціонування інформаційної інфраструктури судової влади. Відповідно до ч. 1 ст. 32 КК України повторністю визнається вчинення двох або більше кримінальних правопорушень, передбачених тією самою статтею або частиною статті Особливої частини КК України. У кримінально-правовій доктрині традиційно виокремлюють два різновиди повторності: 1) повторність тотожних кримінальних правопорушень; 2) повторність однорідних кримінальних правопорушень. Остання має місце у випадках, коли йдеться про вчинення кількох кримінальних правопорушень, передбачених різними статтями Особливої частини КК України, однак таких, що мають подібний об'єкт посягання та спосіб вчинення [198, с. 301].

У контексті досудового розслідування незаконного втручання в роботу автоматизованих систем органів та установ системи правосуддя повторність може проявлятися, зокрема, у багаторазовому здійсненні несанкціонованого доступу до інформаційних ресурсів судової влади, систематичному використанні чужих облікових записів, повторному внесенні несанкціонованих змін до баз

даних або алгоритмів функціонування автоматизованих систем. Разом із тим кримінальне правопорушення не може бути визначене як вчинене повторно у випадках, коли судимість за раніше вчинене кримінальне правопорушення знята або погашена у встановленому законом порядку, або коли особа була звільнена від кримінальної відповідальності за раніше вчинене діяння. У зв'язку з цим слідчому та прокурору як суб'єктам доказування необхідно обов'язково перевіряти наявність відповідних юридичних фактів.

Відповідно до ч. 2 ст. 28 КК України кримінальне правопорушення вважається вчиненим за попередньою змовою групою осіб, якщо його спільно вчинили дві або більше особи, які заздалегідь домовилися про його вчинення [68]. У кримінальних провадженнях, пов'язаних із незаконним втручанням у роботу автоматизованих систем, підлягають доказуванню такі обставини: характер і зміст попередньої домовленості між співучасниками; розподіл ролей між ними; визначення особи, яка безпосередньо здійснювала втручання в інформаційну систему; наявність пособників, які забезпечували технічну підтримку, надавали доступ до інформаційних ресурсів або сприяли приховуванню слідів втручання.

У випадках, коли втручання в роботу інформаційних систем здійснюється організованими групами, підлягають додатковому встановленню обставини, що характеризують структуру такої групи, механізм її функціонування, способи конспірації діяльності, використання спеціалізованих технічних засобів або програмного забезпечення для здійснення несанкціонованого доступу, а також характер взаємодії її учасників. Особливу увагу слід приділяти встановленню технічної оснащеності групи, використанню засобів прихованості доступу до мережі Інтернет, а також наявності фінансових ресурсів, які використовуються для придбання програмного забезпечення чи інших технічних засобів для здійснення втручання.

Водночас перелік обставин, які пом'якшують покарання, визначено у ст. 66 КК України. До них, зокрема, належать: з'явлення із зізнанням, щире каяття або активне сприяння розкриттю кримінального правопорушення;

добровільне відшкодування завданої шкоди; вчинення кримінального правопорушення внаслідок збігу тяжких особистих або сімейних обставин; виконання спеціального завдання з попередження чи розкриття злочинної діяльності організованої групи або злочинної організації [97, с. 164].

Щире каяття як обставина, що пом'якшує покарання, характеризує ставлення винної особи до вчиненого кримінального правопорушення та проявляється у добровільному визнанні провини, висловленні жалю з приводу вчиненого та бажанні усунути заподіяну шкоду. Активним сприянням розкриттю кримінального правопорушення вважається надання особою допомоги органам досудового розслідування у встановленні раніше невідомих обставин, зокрема повідомлення про спосіб втручання у роботу інформаційної системи, технічні засоби, які використовувалися для цього, або інших осіб, причетних до вчинення відповідного діяння. Окрім цього, у кримінальному провадженні підлягають доказуванню обставини, які можуть бути підставою для звільнення особи від кримінальної відповідальності. Найбільш поширеною підставою є закінчення строків давності притягнення до кримінальної відповідальності. При вирішенні цього питання прокурор повинен довести сукупність умов: факт вчинення кримінального правопорушення; закінчення передбаченого законом строку давності; відсутність підстав для зупинення або переривання перебігу такого строку.

Згідно з положеннями кримінального процесуального законодавства, у кримінальному провадженні підлягають доказуванню також обставини, які є підставою для закриття кримінального провадження. Перелік таких обставин визначено у ст. 284 КПК України. До них належать, зокрема: відсутність події кримінального правопорушення; відсутність у діянні складу кримінального правопорушення; недостатність доказів для доведення винуватості особи; смерть підозрюваного; наявність вироку суду, що набрав законної сили, щодо тієї самої особи за те саме обвинувачення [72].

Окреме значення у таких кримінальних провадженнях має встановлення обставин, передбачених п. 6 ч. 1 ст. 91 КПК України [72], що пов'язані із

застосуванням спеціальної конфіскації. Йдеться про доведення того, що певні активи були одержані внаслідок вчинення кримінального правопорушення, використовувалися для його фінансування або виступали засобом чи знаряддям його вчинення. У випадку незаконного втручання в роботу автоматизованих систем такими засобами можуть виступати комп'ютерна техніка, спеціалізоване програмне забезпечення, серверне обладнання або інші технічні засоби, за допомогою яких здійснювався несанкціонований доступ до інформаційної системи. З огляду на це встановлення зазначених обставин потребує дослідження технічних характеристик відповідного обладнання, аналізу цифрових слідів, результатів комп'ютерно-технічних експертиз, даних журналів подій інформаційних систем, а також інших доказів, що дозволяють відтворити механізм втручання у роботу автоматизованої системи.

Водночас ефективність розслідування таких кримінальних правопорушень значною мірою залежить від встановлення причин та умов, які сприяли їх вчиненню. З урахуванням цього доцільним є законодавче закріплення обов'язку встановлення відповідних обставин у кримінальному провадженні. Такий підхід дозволить не лише встановлювати винних осіб, але й усувати недоліки у функціонуванні інформаційних систем, що створюють передумови для незаконного втручання.

Отже, узагальнюючи викладене, необхідно зазначити, що у кримінальних провадженнях щодо незаконного втручання в роботу автоматизованих систем органів та установ системи правосуддя доказування повинно охоплювати комплекс обставин, передбачених в ст. 91 КПК України, а також специфічні технічні та організаційні аспекти функціонування електронного судочинства. Саме встановлення цих обставин забезпечує формування належної доказової бази, правильну кримінально-правову кваліфікацію діяння та обґрунтованість процесуальних рішень.

2.2. Взаємодія слідчого із іншими суб'єктами під час розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя

Наукове осмислення сутності, змісту, форм і напрямів взаємодії слідчого з іншими суб'єктами під час розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя є необхідною передумовою підвищення ефективності досудового розслідування, оскільки результативність у цій категорії кримінальних проваджень значною мірою залежить не лише від професійного рівня слідчого, а й від належної організації його взаємодії з іншими суб'єктами кримінального провадження, а також із посадовими особами, які забезпечують функціонування відповідних інформаційних систем, технічне адміністрування, захист інформації, мережеву взаємодію та збереження електронних даних. Особливого значення така взаємодія набуває на початковому етапі досудового розслідування, коли необхідно швидко встановити обставини виявлення ознак втручання, визначити коло осіб, які мали доступ до системи, забезпечити збереження електронної інформації, резервних копій, технічних носіїв, не допустити подальшої модифікації або знищення цифрових слідів, а також своєчасно зафіксувати технічну та інформаційну обстановку події.

Насамперед, зазначимо, що Великий тлумачний словник української мови визначає поняття «взаємодія» як узгоджений або взаємний зв'язок між об'єктами чи суб'єктами під час здійснення певної діяльності, а також як спільну, скоординовану дію кількох сторін; у фізичному розумінні цей термін тлумачиться як взаємний вплив тіл або частинок, унаслідок якого змінюється їхній стан чи характер руху [16, с. 85]. Таке загальнонаукове розуміння дає змогу виходити з того, що взаємодія завжди передбачає не лише наявність двох або більше учасників, а й їх реальний взаємовплив, погодженість дій та спрямованість на досягнення певного результату.

У соціологічній науці поняття взаємодії розглядається як послідовні та систематичні соціальні дії, що відбуваються між суб'єктами й спрямовані на ініціювання відповідної реакції, яка, у свою чергу, зумовлює нові взаємні дії. Такий підхід дає підстави трактувати взаємодію як один із базових механізмів координації соціальних процесів, формування стійких соціальних зв'язків та забезпечення функціонування складних організаційних систем [155, с. 244]. Водночас у сфері управління взаємодію нерідко пов'язують із функціональним елементом менеджменту, що полягає у перетворенні розрізнених індивідуальних дій у спільну діяльність, узгоджену у просторово-часовому та цільовому вимірах. За такого підходу взаємодія передбачає постійний обмін інформацією між учасниками процесу, який забезпечує цілісність, безперервність та скоординованість спільної роботи [81, с. 184].

При цьому, якщо координацію традиційно відносять до функцій управління, то взаємодію у вузькому значенні до таких функцій не зараховують. Організація та забезпечення взаємодії є, радше, проявами координаційної діяльності [46, с. 77; 3, с. 70]. Йдеться про те, що координація передбачає погодження зусиль і дій на стадії їх підготовки або в процесі діяльності, тоді як взаємодія відображає практичний результат такого погодження – наскільки реально вдалося забезпечити узгодженість дій для досягнення поставленої мети. По суті, у процесі координації як функції управління теж відбувається взаємодія у формі комунікаційних відносин, взаємовпливу між суб'єктом координації та тими, чию діяльність він спрямовує [23, с. 14].

Поряд із цим, у правоохоронній діяльності поняття взаємодії набуває спеціального змісту. Так, О. Я. Черепненко зазначає, що взаємодія у цій сфері має розумітися як спеціально організована, нормативно врегульована та чітко скоординована за цілями, завданнями, місцем і часом спільна діяльність, спрямована на досягнення максимальної ефективності у використанні сил, засобів і методів правоохоронних органів для запобігання, виявлення та розкриття кримінальних правопорушень, а також розшуку осіб, які їх учинили [190, с. 958]. У свою чергу, В. В. Топчій та В. Я. Горбачевський розглядають

взаємодію у сфері кримінального провадження як узгоджену діяльність, що ґрунтується на цілях і завданнях кримінального процесу та передбачає комплексне поєднання процесуальних і оперативно-розшукових заходів, які здійснюються суб'єктами кримінальної юстиції з метою ефективного виявлення, розслідування та попередження кримінальних правопорушень, а також забезпечення притягнення винних осіб до відповідальності виключно в межах вимог кримінального процесуального законодавства та інших нормативно-правових актів [170, с. 126]. При цьому автори наголошують на важливості чіткого розмежування компетенції між суб'єктами взаємодії, оптимального поєднання дозволених заходів, належного ресурсного забезпечення та обов'язкового збереження конфіденційності досудового розслідування.

Таким чином, поняття взаємодії у сучасній науці має багатовимірний зміст, який поєднує загальнонаукові, соціологічні, управлінські та прикладні правоохоронні підходи. Аналіз наведених наукових позицій дає підстави для формулювання власного визначення взаємодії слідчого з іншими суб'єктами у контексті розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя. На нашу думку, таку взаємодію доцільно розуміти як *організовану відповідно до вимог чинного законодавства, погоджену за метою, завданнями, часом, місцем, межами компетенції та послідовністю реалізації систему взаємопов'язаних і взаємодоповнюючих дій слідчого, прокурора, оперативних підрозділів, спеціалістів, експертів, органів та установ системи правосуддя, суб'єктів технічного адміністрування, а в окремих випадках – і інших осіб, спрямовану на своєчасне виявлення, фіксацію, збереження, дослідження й належне процесуальне використання інформації та цифрових слідів, що відображають факт, механізм, наслідки та суб'єктний склад незаконного втручання в роботу відповідних автоматизованих систем.*

Таке розуміння обумовлюється специфікою самої категорії кримінальних правопорушень. Незаконне втручання в роботу автоматизованих систем в органах та установах системи правосуддя є складним для виявлення і

доказування, оскільки може поєднувати технічні, службові, організаційні, інформаційні та процесуальні аспекти. Його розслідування потребує не лише застосування криміналістичних засобів і методів, а й залучення відомостей про функціонування відповідних систем, режим доступу до них, особливості електронного документообігу, правила журналювання подій, порядок резервного копіювання, адміністрування серверів, оновлення програмного забезпечення, використання електронних підписів, віддалених каналів доступу та інших елементів цифрової інфраструктури судової влади. Саме тому взаємодія в цих провадженнях має ширший і функціонально складніший характер, ніж у багатьох інших категоріях кримінальних правопорушень.

Як слушно наголошує Ю. М. Чорноус, сучасна злочинність стає дедалі більш організованою, інтелектуальною, технологічною, використовує досягнення науки і техніки для реалізації своїх цілей, що вимагає об'єднання зусиль уповноважених органів для досягнення спеціальних завдань [194, с. 581]. Зазначене твердження повною мірою стосується і кримінальних правопорушень, пов'язаних із незаконним втручанням у роботу автоматизованих систем правосуддя. Такі посягання можуть вчинятися як службовими особами, що мають доступ до системи, так і сторонніми суб'єктами, які використовують технічні засоби приховування мережевої активності, віддаленого доступу, модифікації електронних даних або маскування власних дій під технічні збої. За таких умов, як вже було зазначено, слідчий об'єктивно не може самостійно забезпечити повне вирішення завдань досудового розслідування без належної організації взаємодії з іншими суб'єктами.

Водночас результати дослідження дають підстави констатувати наявність численних проблем, пов'язаних із налагодженням ефективної взаємодії між слідчим та іншими суб'єктами у цій сфері. На думку опитаних слідчих, прокурорів та працівників оперативних підрозділів, повноцінному здійсненню взаємодії під час досудового розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя перешкоджають: 1) недосконалість нормативного регулювання міжвідомчої та

внутрішньо-системної взаємодії (15%); 2) нерозуміння окремими учасниками змісту, завдань і меж такої взаємодії (17%); 3) відсутність зацікавленості або належної ініціативності з боку окремих суб'єктів, які повинні бути залучені до взаємодії (32%); 4) низький рівень матеріально-технічного забезпечення діяльності, пов'язаної з фіксацією, збереженням та дослідженням цифрової інформації (46%) (додаток Б).

За відсутності належної взаємодії між слідчим, прокурором, оперативними підрозділами, спеціалістами у сфері комп'ютерної техніки, захисту інформації, телекомунікацій, адміністраторами систем, працівниками відповідних органів та установ системи правосуддя і експертними установами істотно знижується результативність розслідування, зростає ризик втрати доказової інформації та виникають труднощі у доведенні обставин, що мають значення для кримінального провадження.

В загальному розумінні взаємодія у таких провадженнях реалізується як у межах процесуальних механізмів – через доручення слідчого, погодження процесуальних рішень із прокурором, залучення спеціалістів, призначення судових експертиз, проведення окремих слідчих (розшукових) дій за участю технічних фахівців, так і через організаційні форми співпраці – спільне планування дій, обмін інформацією, проведення координаційних нарад, погодження алгоритму реагування на інцидент інформаційної безпеки, визначення порядку доступу до технічної інфраструктури та кола відповідальних осіб. Саме поєднання зазначених форм дозволяє забезпечити системний підхід до розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя.

Однак слід зазначити, що розслідування кримінальних правопорушень цієї категорії може здійснюватися за участю різних органів розслідування та правоохоронних органів залежно від конкретних обставин, суб'єкта вчинення, об'єкта втручання, способу реалізації посягання та підслідності. Йдеться, зокрема, про Національну поліцію України, Службу безпеки України, Державне бюро розслідувань, Національне антикорупційне бюро України – у випадках,

коли втручання пов’язане з корупційною складовою або вчинене спеціальним суб’єктом, а також інші уповноважені органи. Така множинність суб’єктів зумовлена тим, що незаконне втручання в роботу автоматизованих систем в органах та установах системи правосуддя може поєднувати ознаки кримінальних правопорушень у сфері використання електронно-обчислювальних машин, службової діяльності, корупційних посягань, перешкоджання діяльності органів правосуддя, несанкціонованого поширення інформації з обмеженим доступом або посягання на інформаційну безпеку держави. Саме тому розслідування таких кримінальних правопорушень нерідко здійснюється в умовах перетину компетенції різних органів, що об’єктивно вимагає чіткої, системної та узгодженої взаємодії між ними.

Повноваження органів Національної поліції України як одного з основних суб’єктів взаємодії під час розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя закріплені як у Законі України «Про Національну поліцію», так і в підзаконних нормативно-правових актах, що конкретизують напрями та форми взаємодії поліції з іншими державними органами, установами та організаціями. Так, відповідно до ст. 5 Закону України «Про Національну поліцію» поліція у процесі своєї діяльності взаємодіє з органами правопорядку та іншими органами державної влади, а також органами місцевого самоврядування відповідно до закону та інших нормативно-правових актів [127]. Зазначена норма отримала подальший розвиток у Положенні про Національну поліцію, затвердженому постановою Кабінету Міністрів України від 28 жовтня 2015 р. № 877, відповідно до якого Національна поліція під час виконання покладених на неї завдань взаємодіє з іншими державними органами, допоміжними органами і службами, органами місцевого самоврядування, підприємствами, установами та організаціями [127]. У контексті розслідування незаконного втручання в роботу автоматизованих систем така взаємодія має особливе значення, оскільки виявлення, локалізація та доказування такого втручання потребують не лише роботи слідчих підрозділів, а й залучення підрозділів кіберполіції, кримінального аналізу, оперативних

служб, фахівців із цифрової криміналістики та інших суб'єктів, здатних забезпечити технічний і аналітичний супровід розслідування.

Крім того, завдання та повноваження окремих підрозділів поліції, які можуть бути залучені до документування й розкриття кримінальних правопорушень досліджуваної категорії, конкретизуються у відомчих нормативних актах. Практика свідчить, що належний рівень організації взаємодії між слідчим, прокурором, оперативними працівниками, працівниками підрозділів кіберполіції, технічними фахівцями та іншими залученими суб'єктами значною мірою забезпечується ефективним і своєчасним обміном інформацією про характер виявленого інциденту, час і спосіб доступу до системи, технічні журнали подій, відомості про облікові записи користувачів, результати попереднього аналізу цифрового середовища та потенційні канали несанкціонованої взаємодії.

У теорії і практиці однією з найбільш результативних форм інформаційної взаємодії є безпосереднє ознайомлення слідчого з матеріалами, які містять відомості про технічні параметри функціонування автоматизованої системи, виявлені аномалії, результати внутрішніх перевірок, службових розслідувань, висновки спеціалістів із кібербезпеки або інформаційної безпеки, а також з відомостями, отриманими оперативним шляхом. Це дозволяє спільно визначати основні напрями розслідування, формувати версії, планувати невідкладні слідчі (розшукові) дії та вживати заходів для збереження електронної інформації. Водночас аналіз практики застосування ст. 41 КПК України дає підстави стверджувати, що у значній кількості випадків слідчі отримують від оперативних підрозділів лише узагальнені довідки або формальні повідомлення, без розкриття логічних зв'язків між установленими фактами, технічними даними та можливими напрямами подальшої перевірки [72]. Такий підхід істотно знижує пізнавальну цінність отриманої інформації. При цьому міркування щодо можливого негативного впливу ознайомлення слідчого з оперативними або технічними матеріалами на об'єктивність розслідування видаються дискусійними, оскільки суперечать самій логіці ефективного доказування і не

узгоджуються з положеннями Закону України «Про оперативно-розшукову діяльність» [133], відповідно до яких відомості, отримані оперативним шляхом, можуть передаватися слідчому без розкриття джерел їх одержання та використовуватися для організації й планування процесуальних дій.

Служба безпеки України як державний орган спеціального призначення з правоохоронними функціями наділена повноваженнями щодо захисту державної безпеки, у тому числі в інформаційній сфері, а також щодо попередження, виявлення, припинення та розкриття кримінальних правопорушень, які створюють загрозу життєво важливим інтересам України, зокрема у сфері інформаційної та кібербезпеки (ст. 1, 2 Закону України «Про Службу безпеки України» [136]). У контексті розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя СБУ може виступати важливим суб'єктом взаємодії насамперед у тих кримінальних провадженнях, де втручання має ознаки посягання на критичну інформаційну інфраструктуру, пов'язане із зовнішнім впливом, організованими формами кіберзлочинності, використанням спеціальних технічних засобів, посяганням на інформаційний суверенітет або загрозою національній безпеці.

Специфіка статусу СБУ у цій сфері полягає, по-перше, у поєднанні правоохоронних, контррозвідувальних та безпекових функцій, що дає можливість виявляти приховані, системні та довготривалі загрози функціонуванню інформаційної інфраструктури органів правосуддя; по-друге, у здатності здійснювати аналітичний і контррозвідувальний супровід проваджень, де втручання в автоматизовані системи може бути елементом ширшої деструктивної діяльності, у тому числі з іноземним або міжрегіональним компонентом [143, с. 159]. За таких умов взаємодія слідчого з підрозділами СБУ набуває особливого значення під час одержання аналітичної інформації, технічних матеріалів, відомостей про канали зовнішнього доступу, способи приховування мережевої активності та інші обставини, що виходять за межі звичайного локального технічного аналізу.

Важливим учасником взаємодії під час розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя є й органи прокуратури, які здійснюють процесуальне керівництво досудовим розслідуванням. У кримінальних провадженнях цієї категорії прокурор не лише погоджує основні процесуальні рішення, а й забезпечує належну координацію дій між слідчим, оперативними підрозділами, спеціалістами, експертами, представниками відповідних органів та установ системи правосуддя, а також іншими суб'єктами, які володіють відомостями або технічними можливостями, необхідними для розслідування. Якщо ж втручання має корупційну складову, вчинене службовими особами високого рівня або віднесене до підслідності НАБУ, особливого значення набуває взаємодія зі Спеціалізованою антикорупційною прокуратурою, яка відповідно до ст. 7 Закону України «Про прокуратуру» входить до системи прокуратури України як окремий структурний елемент [135]. У таких провадженнях ефективність діяльності прокурора можлива лише за умови належно організованої процесуальної та організаційної взаємодії з детективами НАБУ, що передбачає погодження процесуальних рішень, узгодження пріоритетів розслідування, спільне планування слідчих (розшукових) дій, обмін аналітичною та технічною інформацією, а також чітке розмежування функцій прокурора як процесуального керівника і детектива як суб'єкта досудового розслідування [171, с. 327–328].

У системі суб'єктів, з якими слідчий взаємодіє під час розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя, допоміжне, проте практично значуще місце може посідати і Національне агентство з питань запобігання корупції (НАЗК), яке відповідно до Закону України «Про запобігання корупції» є центральним органом виконавчої влади зі спеціальним статусом, що забезпечує формування та реалізацію державної антикорупційної політики [123]. Хоча НАЗК не є безпосереднім суб'єктом технічного реагування на інциденти інформаційної безпеки, його інформаційні ресурси та результати реалізації контрольних повноважень можуть набувати доказового або орієнтуючого значення у тих кримінальних

провадженнях, де незаконне втручання в роботу автоматизованих систем поєднується з корупційною складовою, конфліктом інтересів, зловживанням службовим становищем, приховуванням майнових зв'язків або використанням доступу до інформаційних систем в інтересах третіх осіб [39, с. 250].

Практична цінність взаємодії слідчого з НАЗК у таких провадженнях полягає у можливості отримання відомостей про задекларовані активи посадових осіб, їх корпоративні права, участь у юридичних особах, наявність пов'язаних осіб, отримані доходи, ознаки конфлікту інтересів, а також дані про істотні розбіжності між офіційно задекларованим майновим станом і фактичними обставинами. Такі відомості можуть використовуватися для перевірки версій щодо вчинення незаконного втручання з корисливих мотивів, в інтересах афілійованих структур, з метою приховування неправомірних рішень, штучної зміни відомостей в автоматизованій системі, отримання неправомірних переваг у судових чи адміністративних процедурах або маскування несанкціонованого доступу до інформаційних ресурсів. Крім того, результати перевірок декларацій, матеріали моніторингу способу життя, а також інформація з Єдиного державного реєстру осіб, які вчинили корупційні або пов'язані з корупцією правопорушення, можуть слугувати важливою орієнтуючою базою для обґрунтування слідчих версій, ініціювання слідчих (розшукових) дій, тимчасового доступу до речей і документів, накладення арешту на майно та підготовки відповідних клопотань до слідчого судді.

Специфіка досудового розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя зумовлює необхідність взаємодії слідчого не лише з класичними суб'єктами кримінального провадження, а й із широким колом посадових і службових осіб судової гілки влади, які забезпечують організаційне, технічне, інформаційне та безпекове функціонування відповідних систем. Йдеться насамперед про адміністраторів автоматизованих систем, працівників підрозділів технічної підтримки, фахівців із захисту інформації та кібербезпеки, осіб, відповідальних за резервне копіювання, журналювання подій, управління обліковими записами

користувачів, технічний супровід серверного обладнання, а також працівників, які забезпечують організацію електронного документообігу, доступ до реєстрів, внутрішніх баз даних і підсистем електронного судочинства. Саме ці суб'єкти найчастіше володіють відомостями про архітектуру відповідної системи, штатний порядок її функціонування, технічний регламент роботи, перелік користувачів, рівні та межі доступу, порядок зміни прав доступу, наявність резервних копій, історію оновлень програмного забезпечення, факти збоїв, несанкціонованих змін, віддалених підключень або інших аномалій, що мають істотне значення для розслідування. Разом із тим така взаємодія потребує особливої процесуальної та тактичної обережності, оскільки окремі з названих осіб можуть бути не лише джерелами відомостей, а й потенційно причетними до події кримінального правопорушення або зацікавленими у приховуванні його слідів.

У цьому контексті важливо підкреслити, що взаємодія слідчого з працівниками конкретного суду чи іншої установи системи правосуддя не може зводитися до формального витребування технічних довідок або пояснень. Ефективне розслідування вимагає встановлення фактичного кола осіб, які мали організаційний або технічний стосунок до функціонування системи в період, коли відбулося втручання; з'ясування, хто саме мав повноваження щодо створення, зміни, блокування або видалення облікових записів; хто здійснював адміністрування серверного середовища; хто відповідав за оновлення програмного забезпечення, технічний супровід та аудит безпеки; хто мав доступ до резервних копій та журналів подій; кому були відомі паролі, ключі електронного підпису, алгоритми аварійного відновлення або внутрішні протоколи реагування на інциденти. Без з'ясування цих обставин встановити механізм незаконного втручання, часові межі його реалізації та роль конкретних осіб фактично неможливо.

Окреме місце у системі взаємодії посідає Вища рада правосуддя як орган суддівського врядування, який у межах своєї компетенції забезпечує належне функціонування судової влади, бере участь у вирішенні питань незалежності

суддів, реагує на втручання у діяльність судів і суддів, а також оперує відомостями, що можуть мати значення у кримінальних провадженнях, пов'язаних із порушенням функціонування судової системи [116]. Практичне значення взаємодії слідчого з Вищою радою правосуддя може проявлятися у кількох напрямах. По-перше, у випадках, коли втручання в автоматизовану систему пов'язане із впливом на розподіл судових справ, зміною відомостей у судових інформаційних ресурсах, створенням перешкод у здійсненні правосуддя або іншими посяганнями, що безпосередньо зачіпають гарантії незалежності суддів, Вища рада правосуддя може володіти інформацією про відповідні звернення, повідомлення, дисциплінарні матеріали, результати внутрішніх перевірок або інші документи, що мають орієнтуюче чи доказове значення. По-друге, взаємодія з цим органом може бути важливою для належного процесуального реагування на ситуації, коли втручання стосується діяльності конкретного судді або групи суддів і має ознаки посягання на незалежність правосуддя. По-третє, інформація, наявна у Вищій раді правосуддя, може бути використана для перевірки версії про системність втручання, повторюваність подібних інцидентів, наявність скарг на функціонування конкретних підсистем або на дії посадових осіб, причетних до технічного супроводу. Водночас взаємодія слідчого з Вищою радою правосуддя повинна бути чітко відмежована від будь-якого втручання у сферу її конституційних повноважень чи використання кримінального провадження як інструменту впливу на суддівське врядування. Саме тому така взаємодія має здійснюватися виключно у процесуально визначених формах: шляхом витребування документів, одержання інформації на запити, тимчасового доступу до речей і документів, допиту осіб, які володіють релевантною інформацією, а також використання матеріалів перевірок чи звернень у межах допустимості доказів.

Крім Вищої ради правосуддя, істотне значення має взаємодія слідчого з Державною судовою адміністрацією України, її територіальними управліннями, державними підприємствами та установами, що забезпечують технічне функціонування судових інформаційних систем, а також з іншими органами й

установами в системі судової влади [109]. Саме ці суб'єкти можуть володіти найбільш повною інформацією про технічну модель функціонування автоматизованих систем, правила їх експлуатації, централізовані журнали подій, протоколи обслуговування, оновлення програмного забезпечення, відомості про підключення до мережевої інфраструктури, умови резервного копіювання, штатні регламенти адміністрування та інші технічні параметри. У багатьох випадках без залучення представників Державної судової адміністрації України або її підпорядкованих структур слідчий об'єктивно не може ані правильно встановити технічну природу виявленої аномалії, ані відмежувати незаконне втручання від системної помилки, ані своєчасно забезпечити збереження важливих журналів подій і резервних копій. Саме тому процесуальна і організаційна взаємодія з цими суб'єктами повинна розглядатися як одна з базових умов ефективного розслідування.

Не менш важливою є взаємодія із судами як установами, в яких безпосередньо експлуатуються відповідні автоматизовані системи, а також з окремими працівниками апарату суду. Йдеться про керівників апарату суду, секретарів судових засідань, працівників канцелярії, осіб, відповідальних за реєстрацію та рух процесуальних документів, адміністрування внутрішніх електронних модулів, контроль за доступом до облікових записів, а також інших працівників, які можуть встановити або пояснити факти появи нетипових змін у системі. Практика свідчить, що саме окремі працівники суду нерідко першими виявляють ознаки стороннього втручання: зникнення або зміну електронних документів, появу несанкціонованих записів, аномалії в роботі автоматизованого розподілу справ, зміни часу реєстрації документів, факти доступу до системи у позаробочий час, блокування окремих функцій, невідповідність паперових і електронних відомостей або інші нетипові технічні прояви. У зв'язку з цим своєчасне документування відомостей, отриманих від таких осіб, проведення їх допиту, витребування службових повідомлень, пояснень, журналів реєстрації інцидентів та інших матеріалів може мати вирішальне значення для відтворення початкової картини події.

Окремої уваги заслуговує взаємодія слідчого із адвокатами. Попри те, що вони реалізують процесуальну функцію захисту, у провадженнях про незаконне втручання в роботу автоматизованих систем в органах та установах системи правосуддя, саме адвокати нерідко виявляють або ініціюють перевірку фактів такого втручання. Пояснюється це тим, що вони безпосередньо користуються електронними сервісами судової влади, отримують доступ до процесуальних документів, відслідковують рух справ, виявляють невідповідності в реєстрації або відображенні процесуальних дій, фіксують зникнення документів з електронного кабінету, аномалії у датах і часі внесення інформації, відсутність доступу до матеріалів або невмотивовану зміну процесуального статусу документів. У таких випадках адвокат може фактично виступати первинним носієм інформації про можливе втручання, а його повідомлення, заяви, клопотання, надані скріншоти, електронні копії документів, технічні повідомлення системи чи інші, зафіксовані ним, відомості можуть мати істотне значення для початку кримінального провадження, формування слідчих версій та організації невідкладних слідчих (розшукових) дій.

Разом із тим взаємодія слідчого із адвокатами у цій категорії справ має свою специфіку. З одного боку, слідчий не може ігнорувати відомості, які вони добросовісно повідомляють про ознаки втручання в автоматизовану систему, особливо коли вони об’єктивно підтверджуються технічними проявами або документами. З іншого боку, такі відомості потребують ретельної перевірки, оскільки заяви про втручання можуть використовуватися й тактично – для поставлення під сумнів допустимості доказів, затягування провадження, зміщення акцентів у доказуванні або створення процесуальних переваг. Саме тому взаємодія з захисником має будуватися на принципах процесуальної рівноваги: відомості, що надходять від нього, мають бути належно фіксовані, перевірені й оцінені, але без автоматичного надання їм наперед встановленої доказової сили. У тих випадках, коли захисник повідомляє про конкретні технічні аномалії, доцільним є невідкладне вжиття заходів щодо їх перевірки за

участю спеціалістів, витребування технічних логів, огляду електронного середовища та забезпечення збереження цифрових слідів.

Таким чином, здійснений аналіз дає підстави стверджувати, що досудове розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя є багатосуб'єктним і міжвідомчим процесом, у межах якого слідчий об'єктивно позбавлений можливості самостійно ефективно реалізувати завдання досудового розслідування. Досягнення цілей кримінального провадження у таких провадженнях потребує системної, цілеспрямованої та процесуально впорядкованої взаємодії з правоохоронними органами, органами прокуратури, органами та установами судової влади, технічними адміністраторами відповідних систем, спеціалістами й експертами у сфері захисту інформації та телекомунікацій, а також з іншими суб'єктами, які володіють відомостями або ресурсами, значущими для встановлення фактичних обставин втручання.

Доведено, що така взаємодія має диференційований та функціональний характер, зумовлений стадією кримінального провадження, змістом тактичних завдань, особливостями функціонування конкретної автоматизованої системи та механізмом учиненого втручання. Вона охоплює отримання технічної, службової та процесуально значущої інформації, забезпечення збереження електронних даних і резервних копій, використання внутрішніх перевірок та матеріалів службового реагування, залучення спеціалістів, експертів і технічних адміністраторів, доступ до аналітичних та інформаційно-довідкових ресурсів, виконання процесуальних доручень, встановлення кола користувачів і технічних суб'єктів. Водночас результати дослідження свідчать про наявність стійких організаційних і нормативних проблем у сфері забезпечення такої взаємодії, серед яких слід виокремити: фрагментарність правового регулювання міжвідомчої співпраці; відсутність уніфікованих алгоритмів інформаційного обміну між правоохоронними органами та суб'єктами судової влади; формальний характер реагування на запити слідчого; невизначеність порядку взаємодії з технічними адміністраторами і відповідальними за кібербезпеку

особами; дублювання окремих повноважень; залежність ефективності співпраці від особистих комунікацій між посадовими особами. Сукупність цих чинників негативно позначається на оперативності, повноті та результативності досудового розслідування.

З огляду на викладене, вважаємо за необхідне прийняття спільного міжвідомчого нормативно-правового акта, а саме: «*Інструкції про організацію взаємодії слідчих з правоохоронними органами, органами та установами системи правосуддя, а також іншими суб'єктами під час розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя*», із таким змістовним наповненням:

Розділ І. Загальні положення: мета та завдання Інструкції; сфера застосування; коло суб'єктів взаємодії; основні терміни та їх визначення; принципи організації взаємодії; засади забезпечення незалежності правосуддя, конфіденційності та цілісності електронних даних.

Розділ ІІ. Суб'єкти взаємодії та їх повноваження: слідчий, прокурор, оперативні підрозділи; органи Національної поліції України, Служби безпеки України, Державного бюро розслідувань, НАБУ; Вища рада правосуддя; Державна судова адміністрація України; суди та інші установи системи правосуддя; фахівці із захисту інформації; експертні установи; оператори електронних комунікацій.

Розділ ІІІ. Форми та способи взаємодії: інформаційний обмін; невідкладне повідомлення про виявлення ознак втручання; виконання доручень; спільне планування слідчих (розшукових) дій; забезпечення доступу до технічної інфраструктури; участь спеціалістів та експертів; використання результатів службових перевірок, технічних аудитів та внутрішніх розслідувань; консультативна та аналітична допомога.

Розділ IV. Алгоритми взаємодії на окремих стадіях кримінального провадження: на стадії внесення відомостей до ЄРДР; на початковому етапі розслідування; під час проведення невідкладних слідчих (розшукових) дій; на подальших етапах досудового розслідування; під час завершення досудового

розслідування; у випадках виявлення ознак системного, повторного або зовнішнього втручання.

Розділ V. Порядок документування та фіксації результатів взаємодії: вимоги до оформлення запитів і відповідей; строки та способи надання інформації; порядок витребування та передачі журналів подій, резервних копій, лог-файлів, технічної документації; правила взаємодії під час вилучення цифрових носіїв та доступу до автоматизованих систем; використання електронних інформаційних систем для фіксації взаємодії.

Розділ VI. Забезпечення конфіденційності та захисту інформації: режим доступу до відомостей; порядок роботи з інформацією з обмеженим доступом; захист персональних даних; гарантії нерозголошення технічної інформації про архітектуру систем; відповідальність за порушення режиму конфіденційності.

Розділ VII. Контроль за дотриманням Інструкції та відповідальність: форми відомчого та міжвідомчого контролю; порядок реагування на порушення вимог Інструкції; відповідальність посадових осіб за ненадання, несвоєчасне надання або спотворення інформації; порядок усунення виявлених організаційних недоліків.

Реалізація запропонованої Інструкції покликана сприяти підвищенню ефективності досудового розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя й уніфікації алгоритмів міжвідомчої взаємодії, а також створити належні організаційно-правові передумови для повного, всебічного й об’єктивного встановлення обставин кримінального правопорушення.

Висновки до розділу 2

1. Встановлено, що під час розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя предмет першочергового пізнання та доказування зумовлюється специфікою механізму вчинення такого кримінального правопорушення, його цифровим середовищем, особливостями функціонування відповідних інформаційних систем, а також характером наслідків, які можуть настати для діяльності органів правосуддя. Констатовано, що для цієї категорії кримінальних проваджень особливого значення набуває своєчасне встановлення не лише загальних обставин, передбачених кримінальним процесуальним законом, а й спеціальних відомостей, пов'язаних із технічними параметрами функціонування автоматизованої системи, способом доступу до неї, змінами в інформаційному середовищі, слідами втручання, а також характером порушення встановленого порядку обробки, передавання, зберігання чи використання даних.

2. Наведено типовий перелік обставин, що підлягають встановленню в кримінальних провадженнях цієї категорії, а саме: 1) подія кримінального правопорушення, зокрема час, місце, обстановка, спосіб і конкретна форма незаконного втручання в роботу автоматизованої системи, характер змін, що були внесені до інформації чи програмного середовища, а також особливості функціонування органу або установи системи правосуддя, в межах яких відбулося відповідне втручання; 2) обставини, що характеризують автоматизовану систему як об'єкт незаконного впливу, зокрема її функціональне призначення, режим доступу, коло користувачів, порядок адміністрування, наявність засобів захисту інформації, технічні та програмні характеристики, а також види даних, щодо яких було здійснено протиправний вплив; 3) особа, яка вчинила кримінальне правопорушення, форма її вини, мотив, мета, наявність спеціальних знань, службового чи іншого доступу до системи, а також зв'язок такої особи з органом або установою системи правосуддя чи з іншими особами, які могли сприяти вчиненню втручання; 4) наслідки незаконного втручання,

зокрема вид і обсяг завданої шкоди, характер порушення нормального функціонування автоматизованої системи, можливе блокування, підроблення, знищення, модифікація, копіювання або витік інформації, а також вплив таких наслідків на здійснення судочинства, документообіг, розподіл справ, доступ до інформації чи реалізацію процесуальних прав учасників проваджень; 5) обставини, які впливають на ступінь тяжкості вчиненого кримінального правопорушення, характеризують особу підозрюваного чи обвинуваченого, обтяжують або пом'якшують покарання, свідчать про наявність групового способу вчинення, повторності, використання службового становища, спеціальних технічних засобів або інших кваліфікуючих ознак, а також виключають кримінальну відповідальність чи є підставою для закриття кримінального провадження; 6) обставини, що підтверджують використання технічних пристроїв, програмних засобів, облікових записів, серверного обладнання, носіїв інформації або інших засобів як знаряддя чи засобів учинення кримінального правопорушення, а також можливість їх вилучення, арешту, спеціальної конфіскації чи використання для подальшого експертного дослідження; 7) обставини, що свідчать про наявність підстав для застосування до юридичних осіб заходів кримінально-правового характеру, якщо незаконне втручання було вчинене в їх інтересах, від їх імені або уповноваженими особами з використанням їх організаційних, технічних чи фінансових можливостей.

3. Ефективність досудового розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя значною мірою залежить від належної організації взаємодії слідчого з іншими суб'єктами, залученими до фіксації, збереження, дослідження та процесуального використання джерел доказів. Обґрунтовано, що таку взаємодію доцільно розуміти як організовану відповідно до вимог чинного законодавства, погоджену за метою, завданнями, часом, місцем, межами компетенції та послідовністю реалізації систему взаємопов'язаних і взаємодоповнюючих дій слідчого, прокурора, оперативних підрозділів, спеціалістів, експертів, органів та установ системи правосуддя, суб'єктів технічного адміністрування, а в окремих випадках – інших осіб (зокрема адвокатів), спрямовану на своєчасне виявлення, фіксацію,

збереження, дослідження та належне процесуальне використання слідів, що відображають факт, механізм і суб'єктний склад незаконного втручання в роботу відповідних автоматизованих систем.

4. Найбільш значущими напрямами взаємодії є взаємодія слідчого з прокурором, оперативними підрозділами, спеціалістами та експертами у сфері комп'ютерної техніки, захисту інформації й телекомунікацій, а також з органами та установами системи правосуддя, суб'єктами технічного адміністрування, операторами електронних комунікацій та іншими особами, які можуть володіти інформацією, необхідною для встановлення обставин кримінального правопорушення.

5. Належно організована взаємодія є однією з ключових організаційних умов ефективного доказування у кримінальних провадженнях цієї категорії, оскільки встановлення обставин незаконного втручання потребує поєднання процесуальних можливостей слідчого з оперативними, технічними, інформаційно-аналітичними та експертними ресурсами інших суб'єктів. Відтак взаємодія має здійснюватися не епізодично, а як цілісна, системно організована діяльність, зорієнтована на отримання, збереження та належне використання доказової інформації, насамперед цифрових слідів.

6. Практичну значущість мають узгоджені дії слідчого з прокурором, оперативними підрозділами, спеціалістами й експертами у сфері комп'ютерної техніки та захисту інформації, а також з органами й установами системи правосуддя та суб'єктами технічного адміністрування відповідних систем. Водночас ефективність такої взаємодії істотно знижується під впливом нормативних, організаційних, кадрових і матеріально-технічних чинників, серед яких визначальними є недостатній рівень технічного забезпечення та низька ініціативність окремих учасників взаємодії, що свідчить про невідповідність існуючих механізмів співпраці складності завдань досудового розслідування. З огляду на це обґрунтовано необхідність нормативного впорядкування такої діяльності шляхом ухвалення спеціальної міжвідомчої Інструкції, яка б уніфікувала суб'єктний склад взаємодії, її форми, алгоритми спільних дій, порядок фіксації отриманих результатів та вимоги до захисту інформації.

РОЗДІЛ 3.
ТАКТИКА ПРОВЕДЕННЯ ОКРЕМИХ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ ПІД ЧАС РОЗСЛІДУВАННЯ НЕЗАКОННОГО ВТРУЧАННЯ В РОБОТУ АВТОМАТИЗОВАНИХ СИСТЕМ В ОРГАНАХ ТА УСТАНОВАХ СИСТЕМИ ПРАВОСУДДЯ

3.1. Огляд

Досудове розслідування кримінальних правопорушень, пов’язаних із незаконним втручанням у роботу автоматизованих систем в органах та установах системи правосуддя, передбачає проведення комплексу слідчих (розшукових) дій, спрямованих на отримання, перевірку та належну процесуальну фіксацію доказів у кримінальному провадженні. Прийняття діючого КПК України стало важливим етапом реформування кримінального процесуального законодавства, оскільки законодавець вперше системно визначив правову природу та процесуальний порядок проведення слідчих дій. Підтвердженням цього стало запровадження в КПК України окремої глави 20 «Слідчі (розшукові) дії», що встановлює загальні правила їх проведення, а також визначає їх процесуальне значення у механізмі доказування [72]. Відповідно до положень ст. 223 КПК України слідчі (розшукові) дії – це передбачені законом процесуальні заходи, здійснення яких спрямоване на виявлення, отримання, перевірку, фіксацію доказової інформації. Дотримання встановленого законом порядку їх проведення забезпечує законність і обґрунтованість процесу доказування, досягнення мети кримінального провадження та реалізацію його основних завдань [69, с. 368].

Аналіз практики розслідування кримінальних правопорушень, пов’язаних із незаконним втручанням у роботу автоматизованих систем органів та установ системи правосуддя, свідчить, що з метою встановлення обставин кримінального правопорушення слідчі найчастіше проводять огляд місця події (місцевості),

огляд приміщень (службових кабінетів суддів, працівників апарату суду, адміністраторів інформаційних систем), огляд комп'ютерної техніки, серверного обладнання, електронних носіїв інформації, а також огляд документів та цифрових даних, що можуть містити відомості про несанкціоновані зміни в інформаційних системах. Разом із тим у слідчій практиці існують різні підходи до визначення та організації початкових слідчих дій під час розслідування незаконного втручання у роботу автоматизованих систем. На вибір відповідної тактики можуть впливати як суб'єктивні чинники (позиція прокурора чи слідчого судді), так і об'єктивні обставини, зокрема обмеженість часу для підготовки до проведення слідчих (розшукових) дій, а також складність технічної структури інформаційних систем.

Огляд місця події, службових приміщень, технічних пристроїв і цифрових носіїв інформації під час розслідування кримінальних правопорушень цієї категорії має низку специфічних особливостей. До загальних тактичних положень проведення огляду, на які звертає увагу Н. І. Клименко, належать: своєчасність, невідкладність, об'єктивність, повнота, активність, методичність і послідовність дій слідчого, а також забезпечення єдиного керівництва проведенням огляду [101, с. 5–6]. Безпосередньо перед початком огляду слідчий або залучений спеціаліст повинні провести інструктаж усіх учасників слідчої дії щодо дотримання правил безпеки та порядку поводження з об'єктами, що підлягають дослідженню. Зокрема, такі рекомендації мають враховувати технічний стан обладнання, особливості комп'ютерних систем та можливість втрати або зміни електронної інформації. Наприклад, спеціаліст може надати інструкції щодо правильного відключення комп'ютерної техніки, вилучення електронних носіїв інформації, недопущення зміни цифрових слідів або знищення даних, що містяться на носіях [114, с. 139].

Для огляду території або приміщення місця події можуть застосовуватися різні тактичні способи організації роботи: рух по концентричних колах різного радіуса; рух від центру до периферії або навпаки; а також лінійний (фронтальний або маршрутний) спосіб огляду відповідно до конкретної обстановки [5, с. 107].

Вибір конкретного способу здійснюється слідчим безпосередньо на місці події з урахуванням характеру приміщення, розташування технічного обладнання та можливих місць локалізації цифрових слідів кримінального правопорушення. При цьому предмети та технічні пристрої, що перебувають на місці події, не повинні переміщуватися без попередньої фіксації їхнього положення та стану. У ході огляду слідчі або оперативні працівники можуть здійснювати відеофіксацію процесу проведення слідчої дії, а спеціалісти застосовують технічні засоби для виявлення цифрових слідів втручання в інформаційні системи. Зокрема, можуть аналізуватися лог-файли, параметри доступу до системи, історія авторизацій користувачів й інші дані, що відображають функціонування автоматизованої системи. Такі відомості мають важливе значення для встановлення способу несанкціонованого доступу та ідентифікації осіб, причетних до вчинення кримінального правопорушення.

Фіксація результатів огляду місця події відповідно до вимог КПК України передбачає складання протоколу з дотриманням вимог ст. 104 КПК України. У протоколі повинні бути відображені всі дії слідчого та інших учасників огляду у тій послідовності, у якій вони здійснювалися, а також описані всі вилучені предмети, документи та електронні носії інформації у тому вигляді, в якому вони були виявлені [72]. Під час проведення огляду допускається вилучення лише тих речей і документів, які мають значення для кримінального провадження або вилучені з цивільного обігу. Усі вилучені предмети та документи підлягають негайному опечатуванню із засвідченням підписами осіб, які брали участь у проведенні огляду. У випадках, коли огляд речей чи документів на місці події є неможливим або пов’язаний із значними труднощами, вони тимчасово опечатуються та зберігаються в такому вигляді до моменту проведення їх остаточного огляду (ч. 5 ст. 237 КПК України) [72].

На відміну від огляду місця події, огляд житла чи іншого володіння особи відповідно до ч. 7 ст. 223 КПК України проводиться з обов’язковою участю не менше двох понятих незалежно від застосування технічних засобів фіксації. Понятими не можуть бути потерпілий, родичі підозрюваного або

обвинуваченого, працівники правоохоронних органів, а також інші особи, зацікавлені у результатах кримінального провадження. Під час проведення огляду житла чи іншого володіння особи нерідко виникає необхідність здійснення огляду документів. Значна кількість інформації про обставини незаконного втручання у роботу автоматизованих систем може міститися у службовій документації, технічних журналах, інструкціях із використання інформаційних систем, а також у документах, що відображають діяльність працівників установи. У свою чергу, огляд документів є різновидом слідчої (розшукової) дії, що проводиться з метою виявлення та фіксації відомостей про обставини кримінального правопорушення. Він полягає у вивченні змісту документів, перевірці їх форми, реквізитів та інших ознак, які можуть свідчити про їх доказове значення у кримінальному провадженні [65]. Під час розслідування незаконного втручання в роботу автоматизованих систем об’єктами огляду можуть бути різноманітні види документів: письмові службові документи, фото- та відеоматеріали, електронні файли, а також інші носії інформації. Враховуючи те, що особи, які вчинили кримінальне правопорушення, можуть намагатися знищити або підробити компрометуючі документи, слідчий повинен проводити відповідні слідчі дії без зволікання.

Перед початком огляду документів слідчий повинен визначити їх загальний характер і призначення, вивчити їхній зовнішній вигляд, стан та зміст, а також вжити заходів щодо виявлення можливих ознак підроблення. Під час огляду документів особливу увагу слід звертати на зміст документів, відповідність встановленій формі, наявність усіх реквізитів, а також правильність їх оформлення [4, с. 649]. Специфіку у таких кримінальних провадженнях має огляд електронних документів. Під час огляду електронних документів слідчий повинен зафіксувати наявність усіх реквізитів документа, зокрема електронного підпису автора, дату та час створення документа, його змінення та передачі іншим користувачам. У випадку надсилання електронного документа кільком адресатам або зберігання його на кількох електронних носіях кожен із таких примірників може вважатися оригіналом електронного

документа. Якщо ж автор створює ідентичний за змістом документ у паперовій та електронній формі, кожен із них має однакову юридичну силу. До проведення огляду електронних документів доцільно залучати спеціалістів у галузі інформаційних технологій або комп'ютерної техніки.

Таким чином, огляд місця події, приміщень, документів, комп'ютерної техніки та електронних даних є однією з основних слідчих (розшукових) дій під час розслідування незаконного втручання у роботу автоматизованих систем органів та установ системи правосуддя.

3.2. Обшук

Відповідно до ст. 234 КПК України, обшук проводиться з метою виявлення та фіксації відомостей про обставини вчинення кримінального правопорушення, відшукання знаряддя кримінального правопорушення або майна, здобутого внаслідок його вчинення, а також установлення місцезнаходження розшукуваних осіб [72].

Фактичними підставами для проведення обшуку є наявність достатніх даних вважати, що: 1) було вчинено або готується кримінальне правопорушення, пов'язане з незаконним втручанням у роботу автоматизованих систем органів та установ системи правосуддя; 2) речі, документи, електронні носії інформації чи програмно-технічні засоби, які планується відшукати, мають значення для досудового розслідування; 3) відомості, що містяться у таких об'єктах, можуть бути використані як докази під час судового розгляду; 4) відшукувані речі, документи, електронні дані або розшукувані особи перебувають у зазначеному в клопотанні житлі чи іншому володінні особи [71, с. 187]. У провадженнях цієї категорії йдеться не лише про звичайні документи чи речі, а насамперед про комп'ютерну техніку, серверне обладнання, зовнішні накопичувачі, мобільні телефони, токени, засоби криптографічного захисту, маршрутизатори, блокноти

з паролями, схеми доступу до систем, а також внутрішню документацію, яка відображає порядок адміністрування та використання автоматизованих систем.

Як зазначають Антощук А.О., Степанова Г.М., Замула Б.А. тактичне забезпечення розслідування зазначеної категорії кримінальних правопорушень має зосереджуватися насамперед на допиті, обшуку та призначенні судових експертиз, що й зумовлює структуру подальшого дослідження [6, с. 2910].

Перед визначенням організаційних і тактичних прийомів проведення цієї слідчої (розшукової) дії слідчому необхідно вирішити низку взаємопов'язаних завдань, зокрема: встановити об'єкти, в межах яких слід проводити обшук; окреслити коло предметів, документів і цифрових носіїв, які підлягають відшуканню та вилученню; визначити послідовність проведення кожного окремого обшуку; вирішити питання про залучення спеціалістів у сфері комп'ютерної техніки, телекомунікацій, захисту інформації або цифрової криміналістики. Зазначені завдання вирішуються на підставі аналізу матеріалів кримінального провадження. Необхідною умовою ефективного проведення обшуку є наявність якісної вихідної інформації, яка може містити дані про місце знаходження комп'ютерної техніки, серверів, носіїв інформації, резервних копій, записників із паролями, віддалених засобів доступу, а також про час появи таких об'єктів у приміщенні, їх переміщення, технічні характеристики, упаковку, маркування та інші індивідуалізуючі ознаки [206, с. 293].

Примусовий характер обшуку полягає в тому, що законодавство допускає його проведення незалежно від згоди особи, у володінні якої такий обшук здійснюється. У цьому аспекті для розслідування незаконного втручання в роботу автоматизованих систем особливого значення набуває положення про те, що слідчий і прокурор під час проведення обшуку мають право відкривати закриті приміщення, сховища, речі, а також долати системи логічного захисту, якщо особа, присутня під час обшуку, відмовляється їх відкрити, надати засоби доступу, повідомити пароль або деактивувати відповідну систему захисту, чи якщо обшук проводиться за відсутності осіб, визначених ч. 3 ст. 236 КПК України. Водночас вчинення таких примусових дій можливе виключно за

наявності вмотивованої ухвали слідчого судді про надання дозволу на обшук житла або іншого володіння особи, що узгоджується зі ст. 30 Конституції України [52], а також ч. 2 ст. 234 КПК України [75, с. 578]. З урахуванням специфіки цієї категорії кримінальних проваджень, йдеться, зокрема, про доступ до захищених комп'ютерних систем, локальних мереж, облікових записів користувачів, засобів багатофакторної автентифікації, шифрованих архівів або хмарних сервісів, у яких можуть міститися відомості, що мають доказове значення.

Окремо слід звернути увагу на правову позицію Верховного Суду щодо неможливості передоручення виконання ухвали про дозвіл на обшук житла чи іншого володіння особи. Так, Верховний Суд у складі колегії суддів Другої судової палати Касаційного кримінального суду у справі № 466/896/17 від 29 січня 2019 року вказав, що за змістом ч. 1 ст. 236 КПК України виконання ухвали слідчого судді про дозвіл на обшук житла чи іншого володіння особи покладається особисто на слідчого або прокурора і не може бути доручене в порядку п. 3 ч. 2 ст. 40 КПК України відповідним оперативним підрозділам. Для вирішення питань, що потребують спеціальних знань, слідчий або прокурор мають право залучати спеціалістів, однак це не звільняє їх від обов'язку особисто проводити обшук. Якщо ж обшук фактично здійснюють інші особи, а не слідчий чи прокурор, таке порушення слід визнавати істотним, а одержані результати – такими, що не можуть бути використані при прийнятті процесуальних рішень і не можуть покладатися судом в основу обвинувального вироку відповідно до вимог ст. 86, 87 КПК України [112]. Для розслідування незаконного втручання у роботу автоматизованих систем ця правова позиція має особливу вагу, оскільки на практиці участь спеціалістів з комп'ютерної техніки є майже обов'язковою, проте їхня участь не підміняє процесуальну роль слідчого чи прокурора як суб'єктів проведення обшуку.

З урахуванням законодавчої регламентації обшуку, а також сучасної слідчо-судової практики, доцільно виокремити три основні ситуації, за наявності яких слід розрізняти і мету проведення обшуку у кримінальних провадженнях

про незаконне втручання в роботу автоматизованих систем органів та установ системи правосуддя: 1) несанкціоноване втручання вже відбувається на момент проведення слідчої дії, тобто має місце активний доступ до системи, зміна інформації, втручання в алгоритм функціонування програмного забезпечення, знищення чи блокування даних (мета обшуку – припинити кримінальне правопорушення та зберегти цифрові сліди); 2) факт незаконного втручання мав місце в минулому і завданням обшуку є своєчасне виявлення та вилучення технічних засобів, електронних слідів, документації та інших об'єктів, які підтверджують вже вчинене діяння; 3) у розпорядженні сторони обвинувачення є дані про підготовку до майбутнього втручання в роботу автоматизованої системи, наприклад створення шкідливого програмного забезпечення, незаконне отримання облікових даних, підготовку віддаленого доступу чи зміну конфігурації обладнання, а тому метою обшуку є завчасне запобігання кримінальному правопорушенню та недопущення його реалізації.

Стосовно перших двох випадків істотних процесуальних проблем при проведенні обшуку, не повинно виникати, оскільки його мета пов'язана з відшуканням об'єктів, що підтверджують факт уже вчиненого або триваючого незаконного втручання. Йдеться про вилучення комп'ютерної техніки, зовнішніх накопичувачів, мобільних пристроїв, записів із паролями, мережевого обладнання, носіїв резервного копіювання, службової документації, а також доступ до цифрових слідів, що збереглися в системі або на пристроях. Водночас за наявності відомостей про підготовку до майбутнього втручання застосування положень про обшук у документуванні такої діяльності, з одного боку, є необхідним, оскільки дозволяє своєчасно нейтралізувати загрозу для функціонування автоматизованих систем правосуддя, а з іншого – пов'язане з певними труднощами, оскільки вимагає особливо ретельного обґрунтування зв'язку між передбачуваними діями особи та ризиком майбутнього несанкціонованого втручання.

Щодо цифрових доказів, то цікава думка науковців, які у свої статті запропонували алгоритм роботи із цифровими слідами. Запропонований

алгоритм створює методологічне підґрунтя для стандартизації практик перевірки доказів та сприяє процесуальному узгодженню національних етапів верифікації з міжнародними стандартами, зокрема рекомендаціями European Public Prosecutor's Office (EPPO Guidelines), посібником United Nations Office on Drugs and Crime щодо цифрових доказів, стандартом International Organization for Standardization ISO/IEC 27001 та тестом пропорційності European Court of Human Rights [205, с. 192].

Аналіз практичної діяльності органів досудового розслідування свідчить, що типовими помилками, яких припускаються слідчі ще на етапі звернення до слідчих суддів із клопотаннями про проведення обшуку у кримінальних провадженнях щодо незаконного втручання в роботу автоматизованих систем органів та установ системи правосуддя, є такі:

– копії документів та інших матеріалів кримінального провадження, доданих до клопотання, а також копія витягу з ЄРДР щодо відповідного кримінального провадження не засвідчуються належним чином, а інколи є такими, що їх зміст неможливо повноцінно прочитати або ідентифікувати;

– у клопотанні про проведення обшуку відсутня конкретна вказівка на те, в якому саме приміщенні, службовому кабінеті, житлі, дата-центрі, серверній кімнаті чи іншому володінні слід проводити обшук, а також хто є власником або фактичним користувачем відповідного приміщення;

– у клопотанні не зазначаються індивідуальні або родові ознаки предметів, документів, технічних засобів та електронних носіїв інформації, які планується відшукати, зокрема не конкретизуються види комп’ютерної техніки, маркування серверів, носіїв інформації, токенів, засобів автентифікації, логінів, записників із паролями, службової документації чи інших об’єктів, які можуть містити дані про несанкціоноване втручання.

Однак, у разі постановлення слідчим суддею ухвали про надання дозволу на проведення обшуку наступним етапом є прибуття на місце його проведення та проникнення до приміщення, житла, службового кабінету, серверної, дата-центру чи іншого володіння, де такий обшук має відбуватися. У цьому контексті

доцільно враховувати і сформовану практику Верховного Суду, який неодноразово наголошував на неприпустимості підміни обшуку оглядом місця події. Зокрема, у постановах від 07 червня 2018 р. (справа № 740/5066/15-к), від 26 лютого 2019 р. (справа № 266/4000/14-к), від 19 березня 2019 р. (справа № 380/157/14-к) Верховний Суд виходив із того, що проведення фактичного обшуку під виглядом огляду місця події нівелює вимоги судового контролю, передбачені ст. 223, ч. 2 ст. 234 КПК України. Якщо прокурор або слідчий не зверталися до слідчого судді з клопотанням про проведення обшуку, а проникнення до житла чи іншого володіння особи відбулося під виглядом іншої слідчої дії, отримані внаслідок цього докази визнаються недопустимими і не можуть бути використані судом під час ухвалення рішення. Сам по собі запис у протоколі про те, що огляд нібито проведено на підставі заяви власника приміщення, без належного документального підтвердження такої згоди, не може розглядатися як достатня правова підстава для проникнення до житла чи іншого володіння особи без ухвали слідчого судді. Як уже зазначав Верховний Суд у своїх попередніх рішеннях (постанови від 26 лютого 2019 р. у справі № 266/4000/14-к, від 12 вересня 2019 р. у справі № 159/451/16-к), при вирішенні питання про допустимість доказів, отриманих у ході огляду житла чи іншого володіння особи, якщо сторона ставить під сумнів сам факт надання згоди або її добровільність, суд повинен виходити із сукупності всіх обставин, що супроводжували проведення відповідної слідчої дії, враховуючи, хоча і не обмежуючись цим, наявність письмового підтвердження такої згоди [99, с. 410].

У кримінальних провадженнях щодо незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя обшук найчастіше проводиться за місцем роботи підозрюваних осіб, у службових кабінетах працівників апарату суду, адміністраторів систем, технічного персоналу, за місцем проживання таких осіб, а також у приміщеннях, що можуть використовуватися їхніми родичами, знайомими, посередниками або іншими особами, залученими до реалізації протиправного механізму. Окремими об’єктами обшуку можуть бути серверні приміщення, архівні кімнати,

приміщення, де зберігаються резервні копії, мережеве обладнання, робочі станції, ноутбуки, мобільні телефони, зовнішні носії інформації, маршрутизатори, токени доступу, засоби електронного підпису, документація з адміністрування системи, а також записи, що містять логіни, паролі чи інші облікові дані. Основна мета таких обшуків полягає у відшуканні технічних засобів, за допомогою яких могло бути здійснено несанкціонований доступ до автоматизованої системи; документів і електронних даних, що свідчать про факт, механізм, спосіб, час та наслідки втручання; відомостей про інших учасників протиправної діяльності, характер їх взаємозв'язків; слідів підготовки, вчинення та приховування кримінального правопорушення; а також майна, що може підлягати арешту, спеціальній конфіскації або використовуватися для забезпечення відшкодування шкоди [174, с. 50–51].

На нашу думку, для досягнення завдань обшуку в такій категорії кримінальних проваджень обов'язковим є залучення спеціалістів. Як слушно зазначає К. О. Чаплинський, фахівці (спеціалісти) надають керівнику операції та керівникам окремих пошукових груп консультації і рекомендації науково-технічного характеру, зокрема щодо підготовки слідчої дії, вибору прийомів, методів і технічних засобів, які доцільно застосовувати для виявлення, фіксації, вилучення та попереднього дослідження доказів. Крім того, спеціалісти можуть надавати допомогу у використанні криміналістичної техніки, пошукових приладів, цифрових засобів копіювання інформації, а також у складанні схем, планів, креслень або відображенні архітектури інформаційної системи [185, с. 85]. У провадженнях про незаконне втручання в роботу автоматизованих систем така допомога має особливе значення, оскільки без фахового супроводу існує високий ризик втрати електронної інформації, порушення цілісності цифрових слідів або неправильного поводження з технічними пристроями, що унеможливить їх подальше експертне дослідження. Залучаючи спеціаліста до проведення обшуку у кримінальному провадженні щодо незаконного втручання в роботу автоматизованих систем органів та установ системи правосуддя, слід враховувати низку обставин.

По-перше, має значення вид обшуку: житла, службового приміщення, серверної кімнати, дата-центру, транспортного засобу чи особи. По-друге, необхідно чітко визначити предмети пошуку: комп'ютерну техніку, мобільні термінали, електронні носії інформації, ключі доступу, документацію з адміністрування систем, резервні копії, записники з паролями, засоби віддаленого доступу, шкідливе програмне забезпечення, засоби обходу систем захисту, а також інші речі й документи, що мають значення для встановлення істини у справі. По-третє, слід мати дані про суб'єкта, щодо якого проводиться обшук: його посаду, функціональні обов'язки, рівень технічної підготовки, обсяг доступу до інформаційних систем, можливість активної протидії обшуку, наявність навичок швидкого видалення, шифрування або приховування цифрових даних. По-четверте, важливе значення має мета обшуку, оскільки від цього залежить вибір конкретного спеціаліста або групи спеціалістів: фахівця у сфері комп'ютерної техніки, мережевої інфраструктури, цифрової криміналістики, захисту інформації, програмування чи адміністрування баз даних. По-п'яте, має враховуватися конкретна слідча ситуація, а також час проведення обшуку, оскільки в окремих випадках доцільним є проведення тактичної операції, пов'язаної з одночасним «груповим обшуком» у кількох співучасників на різних об'єктах [174, с. 50]. Саме такий підхід уможливлює одночасне блокування потенційних каналів зв'язку між причетними особами, запобігає синхронному знищенню доказів і забезпечує ефективність документування діяльності всього механізму незаконного втручання.

Для того щоб проведення обшуку було раптовим, а підозрювані особи не мали можливості знищити або приховати сліди кримінального правопорушення, необхідно забезпечити швидке та несподіване проникнення до приміщення, житла чи іншого володіння, де проводиться обшук, а також негайний контроль за всіма потенційними шляхами виходу та передачі інформації. У справах цієї категорії це означає не лише фізичне спостереження за вікнами, дверима, запасними виходами чи прибудовами, але й за можливістю – блокування засобів дистанційного зв'язку, відключення зовнішніх каналів доступу до мережі,

унеможливлення віддаленого знищення інформації, перезапуску серверів, активації програм автоматичного стирання або передачі шкідливих команд на інші пристрої. Одночасно необхідно виключити ситуацію, за якої хтось із присутніх зможе залишити приміщення, передати носії інформації іншій особі, викинути мобільний пристрій, знищити записники з паролями, активувати функцію шифрування чи фізично пошкодити обладнання [1, с. 67]. Усе це потребує ретельної координації між членами слідчо-оперативної групи та належної попередньої підготовки.

Отже, на наш погляд, організація обшуку у кримінальних провадженнях щодо незаконного втручання в роботу автоматизованих систем органів та установ системи правосуддя включає складання детального плану його проведення з урахуванням таких тактичних рекомендацій:

– проведення комплексу підготовчих заходів, спрямованих на встановлення місць можливого зберігання комп'ютерної техніки, серверного обладнання, зовнішніх носіїв інформації, документів, засобів доступу до інформаційної системи, резервних копій, мобільних пристроїв та інших об'єктів, які можуть містити інформацію, що цікавить слідство, а також встановлення місцезнаходження особи, яка буде присутня під час проведення обшуку;

– підготовка процесуальних документів для проведення обшуку, визначення складу слідчо-оперативної групи, добір співробітників правоохоронних органів і спеціалістів відповідного профілю, формування за необхідності кількох груп, а також вирішення питань технічного забезпечення: відеофіксації, засобів зв'язку, носіїв для копіювання інформації, пристроїв для екранування сигналу, пакувальних матеріалів, засобів маркування і збереження речових доказів;

– проведення перед обшуком загального інструктажу всіх груп із доведенням до кожної з них переліку предметів, документів, технічних засобів і цифрових носіїв, що підлягають виявленню та вилученню, орієнтовних місць їх можливого знаходження, визначенням порядку дій у разі виявлення увімкненого

обладнання, захищених носіїв, зашифрованих файлів, систем віддаленого доступу чи інших технічно складних об’єктів;

– здійснення розстановки сил за об’єктами проведення обшуків, встановлення постійного зв’язку між керівниками груп і слідчим, який здійснює досудове розслідування, для координації дій, визначення періодичності виходу на зв’язок, повідомлення про виявлення шуканих предметів, технічних пристроїв чи документів, а також коригування пошукової роботи, що дозволяє своєчасно вирішувати питання щодо вилучення «сумнівних» об’єктів, їх зв’язку з подією кримінального правопорушення та доцільності призначення подальших експертних досліджень [7, с. 11].

Невідкладними діями слідчого після проникнення до місця проведення обшуку є: пред’явлення службового посвідчення, ознайомлення присутніх з ухвалою слідчого судді про дозвіл на обшук, роз’яснення особам, які перебувають у приміщенні, їхніх прав та обов’язків, а також правил поведінки під час проведення цієї слідчої (розшукової) дії; надання доручення членам слідчої групи обстежити об’єкт з метою встановлення кола осіб, які на ньому перебувають, і недопущення приховування, пошкодження чи знищення речей та відомостей, що мають значення для кримінального провадження. У кримінальних провадженнях щодо незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя особливо важливо негайно заборонити особам, які перебувають на об’єкті обшуку, торкатися працюючих комп’ютерів, серверів, ноутбуків, мобільних пристроїв, а також вчиняти будь-які дії з комп’ютерною технікою, якщо їх наслідки наперед не є визначеними та контрольованими. У разі необхідності персонал або інших осіб доцільно ізолювати в окремому приміщенні, щоб унеможливити віддалене видалення даних, зміну конфігурації обладнання, передачу команд іншим співучасникам чи приховування засобів доступу [105, с. 198].

Доцільним є застосування під час обшуку таких тактичних прийомів:

– послідовне та вибіркове обстеження (дослідження мають проводитися ретельно, з усіх боків, із перевіркою частин об’єкта, прихованих від

безпосереднього спостереження слідчого; при цьому кожен предмет, пристрій, носій інформації, елемент мережевої інфраструктури, технічна документація чи робоче місце оглядаються окремо) [192, с. 142];

– паралельне і зустрічне обстеження (паралельне обстеження доцільне під час обшуку великих службових приміщень, серверних кімнат, архівів, дата-центрів або офісів із кількома робочими зонами. Під час зустрічного обстеження одна особа, що проводить обшук, рухається праворуч від входу, інша – ліворуч, після чого вони, зустрівшись, спільно досліджують центральну частину приміщення, вузли комутації, серверні шафи, технічні меблі та інші осередки можливого зберігання цифрових носіїв або супровідної документації);

– поєднання одиночного та групового обшуків (якщо учасники недостатньо підготовлені до проведення обшуку у складному цифровому середовищі, пошук здійснює переважно керівник групи або спеціаліст під його контролем; якщо ж учасники мають достатній рівень підготовки, доцільним є груповий пошук, коли окремі підгрупи одночасно працюють із технікою, документацією, носіями інформації, системами відеоспостереження, резервними копіями й іншими об’єктами);

– відволікаючі прийоми (навмисне зосередження уваги на другорядних об’єктах, демонстративне дослідження окремих приміщень або секцій для виявлення реакції обшукуваної особи, особливо у випадках, коли є дані про поінформованість такої особи щодо предмета пошуку або місця його приховування) [183, с. 89];

– спостереження за реакціями та поведінкою обшукуваних осіб (створення певних умов з метою викриття приховуваних об’єктів, зокрема тих, на які особа реагує хвилюванням, зміною тону голосу, тремтінням рук, спробами відволікти увагу, перевести огляд в іншу частину приміщення, наблизитися до техніки чи документів, що мають для неї особливе значення);

– постійний обмін інформацією між учасниками обшуку про виявлені технічні засоби, носії, документи, способи приховання цифрових слідів, а також прийоми їх виявлення;

– постійний зв’язок між групами [7, с. 16].

Зазвичай під час проведення обшуку у кримінальних провадженнях щодо незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя виявленню та вилученню підлягають:

– документи, що відображають законодавчі, організаційно-розпорядчі та відомчі положення, які регламентують функціонування автоматизованих систем, порядок доступу до них, правила адміністрування, резервного копіювання, інформаційної безпеки, технічного обслуговування, авторизації користувачів та дій у системі;

– посадові інструкції, накази про призначення на посаду, розпорядження про надання чи зміну рівня доступу до інформаційних систем, документи щодо визначення адміністраторів, відповідальних осіб за технічний супровід, кіберзахист або облік електронних ключів;

– установчі, організаційні та службові документи установи чи органу, де функціонує відповідна автоматизована система, а також внутрішні регламенти, положення про порядок роботи автоматизованої системи документообігу суду, системи автоматизованого розподілу справ, локальні акти з технічного захисту інформації, схеми мережевої інфраструктури, акти інсталяції, модернізації або оновлення програмного забезпечення;

– матеріали службових розслідувань, пов’язані з порушенням порядку функціонування автоматизованих систем або доступу до них;

– грошові кошти, електронні пристрої чи інше майно, яке могло бути використане як засіб вчинення кримінального правопорушення, отримане внаслідок такого втручання або пов’язане з оплатою несанкціонованих послуг, придбанням шкідливого програмного забезпечення;

– предмети й документи, які мають інше значення для кримінального провадження, зокрема чорнові записи, блокноти, мобільні телефони, SIM-картки, смарт-картки, ключі електронного підпису, пластикові картки доступу до приміщень чи систем, платіжні квитанції, договори з постачальниками

програмного забезпечення, дані про акаунти в хмарних сервісах, месенджерах та електронній пошті;

– комп'ютери, сервери, ноутбуки, периферійні пристрої, засоби зберігання інформації, маршрутизатори, комутатори, точки доступу, зовнішні накопичувачі, флеш-носії, карти пам'яті, оптичні диски, технічні модулі, резервні носії та інші електронні пристрої, що можуть містити дані про незаконне втручання.

Разом із тим під час обшуку можуть бути вилучені речі, дозвіл на відшукання та вилучення яких прямо не передбачений ухвалою слідчого судді, однак які були виявлені в процесі проведення цієї слідчої дії та мають очевидне значення для кримінального провадження або вилучені з цивільного обігу. У кримінальних провадженнях цієї категорії такими об'єктами можуть виявитися не задекларовані облікові записи, приховані носії інформації, шифровані архіви, спеціальні засоби для обходу систем захисту, сторонні засоби віддаленого адміністрування, а також грошові кошти чи матеріальні цінності, походження яких викликає обґрунтовані сумніви. У подальшому підозрювані або обвинувачені можуть надавати пояснення щодо джерела походження таких речей, технічних засобів чи документів, посилатися на їх законне походження, побутове призначення або випадкове зберігання. Однак така інформація та подані документи потребують ретельної перевірки, оскільки в окремих випадках пояснення є неправдивими, а документи – підробленими або створеними вже після проведення обшуку з метою ускладнення доказування [189, с. 170–171].

Успіх розслідування у цій категорії кримінальних проваджень значною мірою залежить від правильності фіксації та вилучення виявлених слідів кримінального правопорушення як у процесуальному, так і в криміналістичному аспектах. Оскільки процесуальний закон основним способом фіксації слідчих (розшукових) дій визначає протокол, слідчий повинен детально відобразити в ньому фізичні, технічні та інші характеристики вилучених об'єктів: модель, тип, серійний номер апаратури, зовнішній стан пристроїв, наявні пошкодження, підключення до мережі, розташування кабелів, ідентифікаційні ознаки носіїв

інформації, характер пакування, а також інші видимі індивідуальні ознаки. Усі вилучені предмети, носії інформації, документи, а за потреби – зліпки, копії, відбитки, цифрові образи чи контрольні хеш-значення за допомогою спеціаліста упаковуються, опечатуються відповідно до встановлених вимог, передаються слідчому і долучаються до протоколу обшуку [72].

Другий примірник протоколу обшуку разом із доданим до нього описом вилучених документів і тимчасово вилучених речей (за їх наявності) вручається особі, у якої проведено обшук, а в разі її відсутності – повнолітньому члену її сім'ї або представникові. Якщо обшук проводився на підприємстві, в установі чи організації, другий примірник протоколу вручається керівнику або представникові відповідної установи, організації чи підприємства (ч. 9, 10 ст. 236 КПК України) [72]. У справах про незаконне втручання в роботу автоматизованих систем це правило має особливе значення, оскільки опис вилучених технічних засобів, носіїв та документації має бути максимально точним, щоб унеможливити спори щодо складу вилученого майна, його ідентичності, цілісності та умов зберігання. Необхідно також зазначити, що після затримання в приміщенні, де проводиться обшук, особи, яка може бути причетною до незаконного втручання в автоматизовану систему, може бути проведений її особистий обшук із дотриманням правил, передбачених ч. 3 ст. 208, ч. 7 ст. 223 та ч. 5 ст. 236 КПК України [72]. Крім того, обшук особи в таких кримінальних провадженнях нерідко має самостійне значення, оскільки саме при особі можуть знаходитися мобільні пристрої, флеш-накопичувачі, службові посвідчення, чорнові записи або інші об'єкти, які безпосередньо підтверджують її роль у механізмі втручання. У зв'язку з цим при проведенні обшуку особи доцільно дотримуватися таких рекомендацій:

– фізичне затримання має бути сплановане та проведене в місці, яке унеможливлює втечу особи, використання нею засобів зв'язку, швидке видалення електронної інформації, активацію функцій шифрування, знищення карт пам'яті, токенів чи інших носіїв, а також вчинення дій, спрямованих на позбавлення від предметів і слідів кримінального правопорушення;

– під час затримання бажаною є присутність понятих для безпосереднього візуального сприйняття події, що в подальшому дозволить засвідчити обставини спроб особи позбутися мобільного пристрою, носія інформації, засобу доступу чи іншого предмета, який має доказове значення;

– з метою забезпечення неупередженості кримінального провадження не слід залучати як понятих осіб, які брали участь у підготовчих заходах з документування кримінального правопорушення, мали контакт із предметами, що можуть бути вилучені, або іншим чином пов'язані з діяльністю правоохоронних органів у цьому провадженні. При цьому необхідно дотримуватися загальних вимог закону щодо участі понятих під час обшуку особи;

– для належної фіксації проведення слідчої дії за допомогою технічних засобів доцільно залучити спеціаліста, який здійснюватиме відеозапис затримання, обшуку особи та вилучення предметів. За можливості слід забезпечити відеофіксацію з двох різних ракурсів, що дозволяє повніше відобразити поведінку особи, місце виявлення відповідних предметів, їх стан і послідовність процесуальних дій [201, с. 121–122].

Варто додати, що збройна агресія російської федерації проти України зумовила внесення низки змін до чинного законодавства, спрямованих на адаптацію кримінального процесу до викликів воєнного стану. Серед іншого, зміни торкнулися режиму досудового розслідування та судового розгляду кримінальних проваджень в умовах воєнного стану. Очевидно, що такі законодавчі новації були покликані врахувати та вирішити ризики і суперечливі ситуації, які можуть виникати на різних стадіях кримінального провадження в умовах особливого правового режиму [75, с. 579].

Так, відповідно до абз. 2 п. 1 та п. 2 ч. 1 ст. 615 КПК України обшук житла чи іншого володіння особи, а також обшук особи без надання відповідного дозволу слідчого судді допускається у випадку, коли відсутня можливість виконання слідчим суддею своїх повноважень, передбачених ст. ст. 140, 163, 164, 170, 173, 206, 219, 232, 233, 234, 235, 245–248, 250, 294 КПК України. У такому

разі відповідні повноваження здійснює керівник відповідного органу прокуратури за клопотанням прокурора або за клопотанням слідчого, погодженим із прокурором. Отже, у наведеній ситуації керівник відповідного органу прокуратури отримує право без ухвали слідчого судді самостійно приймати рішення та надавати дозвіл на проведення обшуку житла чи іншого володіння особи відповідно до вимог ст. ст. 234, 235 КПК України. Згідно з абз. 1 п. 2 ч. 1 ст. 615 КПК України рішення керівника органу прокуратури приймається у формі постанови та має містити обґрунтування правомірності здійснення ним повноважень слідчого судді у конкретному випадку [72]. У кримінальних провадженнях щодо незаконного втручання в роботу автоматизованих систем така процедура може набувати особливої актуальності, зокрема у випадках, коли зволікання з проведенням обшуку створює ризик втрати електронних доказів, дистанційного знищення даних, компрометації функціонування критично важливих інформаційних ресурсів системи правосуддя або подальшого незаконного втручання в їх роботу.

Поряд із цим, в умовах воєнного стану проведення обшуку або огляду житла чи іншого володіння особи у кримінальних провадженнях щодо незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя має здійснюватися з урахуванням спеціальних процесуальних правил, обумовлених дією особливого правового режиму. Зокрема, якщо залучення понятих є об’єктивно неможливим або пов’язане з реальною чи потенційною небезпекою для їхнього життя чи здоров’я, відповідні слідчі (розшукові) дії можуть проводитися без їх участі. Такий підхід зумовлений як безпековими ризиками, характерними для територій, де ведуться бойові дії або існує загроза їх виникнення, так і необхідністю невідкладного реагування для збереження доказової інформації, яка в умовах розслідування кіберзалежних кримінальних правопорушень може бути втрачена, знищена, зашифрована або змінена протягом дуже короткого проміжку часу. Як слушно зазначає Г. К. Тетерятник, загалом два основні фактори виступають детермінантами законодавчих змін щодо участі понятих при проведенні слідчих (розшукових)

дій у кримінальних провадженнях в умовах надзвичайних правових режимів: фактор небезпеки, який ставить під сумнів саму можливість участі понятих у процесуальних діях, та фактор швидкої змінюваності обстановки, що вказує на невідкладність проведення таких дій з метою збереження доказової інформації [164, с. 196]. Для кримінальних проваджень щодо незаконного втручання в роботу автоматизованих систем цей другий фактор має особливе значення, оскільки йдеться не лише про матеріальні сліди, а й про цифрову інформацію, яка може бути дистанційно видалена, пошкоджена або прихована внаслідок зволікання з проведенням обшуку. У такому випадку хід і результати проведення обшуку або огляду житла чи іншого володіння особи, а також обшуку особи в обов'язковому порядку мають фіксуватися доступними технічними засобами шляхом здійснення безперервного відеозапису [102]. Саме така форма фіксації у зазначених умовах набуває особливої доказової ваги, оскільки дозволяє компенсувати відсутність понятих, зафіксувати послідовність дій учасників обшуку, місце виявлення технічних засобів, носіїв інформації, документації, а також поведінку осіб, які перебували на об'єкті. Ще однією особливістю проведення обшуку в умовах воєнного стану є зміна часових меж його допустимого проведення. Йдеться про можливість здійснення обшуку та інших слідчих (розшукових) дій цілодобово, зокрема і в нічний час. Таким чином, відповідно до змін, внесених до ч. 4 ст. 223 КПК України, в умовах воєнного стану дозволяється проводити слідчі (розшукові) дії, у тому числі обшук, у нічний період, тобто з 22 години вечора до 6 години ранку, без необхідності окремого обґрунтування причин проведення такої дії саме у цей час [72].

Отже, під час досудового розслідування кримінальних правопорушень, пов'язаних із незаконним втручанням у роботу автоматизованих систем в органах та установах системи правосуддя, обшук повинен мати невідкладний характер, оскільки фіксація таких діянь часто супроводжується протидією з боку осіб, які мають спеціальні технічні знання, доступ до інформаційних систем, можливість оперативного знищення або спотворення цифрових слідів, а іноді й підтримку інших осіб, залучених до технічного чи організаційного забезпечення

функціонування відповідних систем. Водночас такий обшук повинен мати і «груповий» характер, тобто за потреби проводитися комплексно та одночасно у кількох місцях: за місцем роботи, проживання, у приміщеннях, де знаходяться сервери, а також у володінні інших осіб, причетних до вчинення кримінального правопорушення. Не менш важливою є і його пропорційність, адже не всі виявлені під час обшуку предмети, документи чи окремі технічні пристрої мають значення для конкретного кримінального провадження, а тому вилучення повинно здійснюватися вибірково, обґрунтовано та з дотриманням загальних засад кримінального провадження. Саме за таких умов обшук виступає не лише ефективним засобом збирання доказів, а й забезпечує баланс між інтересами кримінального провадження, необхідністю збереження доказової інформації та дотриманням прав осіб, щодо яких така слідча дія проводиться.

3.3. Допит

Допит є однією з найпоширеніших слідчих (розшукових) дій, зміст якої полягає в одержанні та процесуальному закріпленні у встановленій кримінальним процесуальним законом формі показань підозрюваного, свідка, потерпілого, експерта та інших учасників кримінального провадження, яким можуть бути відомі обставини, що мають значення для встановлення істини. Процесуальний порядок проведення допиту визначено положеннями ст. ст. 65, 95–97, 133, 223–226, 232, 256 КПК України [72].

Як зауважує С. Ю. Карпушин, допит фактично виступає необхідною й обов’язковою слідчою дією у кожному кримінальному провадженні, оскільки саме він є єдиним процесуальним засобом формування такого самостійного джерела доказів, як показання. Саме тому практично жодне кримінальне провадження не обходиться без проведення допитів, насамперед на стадії досудового розслідування [44, с. 82].

Відповідно до ст. 95 КПК України показаннями є відомості, які надаються в усній або письмовій формі під час допиту підозрюваним, обвинуваченим,

свідком, потерпілим, експертом щодо відомих їм обставин кримінального провадження, що мають значення для цього провадження [72]. Виклик учасника провадження для участі в допиті становить систему дій, спрямованих на його належне інформування про необхідність явки до слідчого, дізнавача чи прокурора із зазначенням процесуального статусу викликаної особи, дати, часу та місця прибуття, слідчої (розшукової) дії, для участі в якій її викликають, а також можливих правових наслідків неприбуття. Фактичними підставами для виклику особи на допит є: 1) наявність у слідчого достатніх підстав вважати, що особа може надати показання, які мають значення для кримінального провадження; 2) необхідність її особистої участі у проведенні допиту [41].

Як свідчить аналіз слідчо-прокурорської практики, початок досудового розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя зазвичай зумовлює необхідність першочергового отримання пояснювальної та доказової інформації від особи, яка повідомила про виявлені ознаки такого кримінального правопорушення. З огляду на положення ч. 1 ст. 60 КПК України, заявником є фізична або юридична особа, яка звернулася із заявою чи повідомленням про кримінальне правопорушення до органу уповноваженого розпочати досудове провадження, і не є потерпілим. Водночас КПК України не передбачає самостійного процесуального різновиду допиту заявника. Тому залежно від конкретних обставин кримінального провадження така особа може бути допитана або як свідок, або як потерпілий, якщо незаконним втручанням у роботу автоматизованої системи їй завдано відповідної шкоди [196, с. 220; 197, с .23].

Під час допиту заявника у кримінальному провадженні цієї категорії обов’язково слід з’ясувати: з яких джерел йому стало відомо про факт або ознаки незаконного втручання в роботу автоматизованої системи; чи спостерігав він особисто збої, несанкціоновані зміни в системі, втрату або блокування інформації, порушення автоматизованого розподілу справ, несанкціоновані входи до системи, зникнення електронних документів, зміну черговості реєстрації матеріалів або інші аномальні прояви; у який час, у якому місці та за

яких обставин це відбулося; які саме автоматизовані системи або їх модулі були задіяні; чи відомо заявникові, хто мав доступ до відповідної системи в момент події; які документи, скріншоти, службові листи, акти технічної перевірки або інші носії інформації можуть підтвердити повідомлені ним факти; коли, за яких умов і з ким саме він обговорював виявлені порушення; чи звертався раніше до керівництва суду, працівників апарату, служби підтримки, ДСА України, органів суддівського врядування чи правоохоронних органів; чи фіксувались відповідні події у будь-яких внутрішніх документах, службових записках, електронних зверненнях або повідомленнях; хто ще, окрім заявника, володіє інформацією про виявлені обставини; якими є характеристики осіб, які могли бути причетними до втручання; чи мали місце подібні випадки раніше; кому ще заявник повідомляв про зазначені факти і коли саме це відбулося; чи відомі йому мотиви можливого незаконного втручання; що спонукало його повідомити про відповідні обставини орган досудового розслідування. Якщо заявник повідомляє про конкретний факт несанкціонованого доступу до автоматизованої системи, зміну її параметрів, модифікацію електронних документів, порушення алгоритму розподілу справ, видалення або блокування інформації, додатково необхідно з’ясувати: за яких саме обставин було виявлено втручання; які технічні або організаційні ознаки це підтверджують; у чому саме проявився збій чи несанкціонована зміна; які дані, на думку заявника, були змінені, видалені, заблоковані або штучно внесені; чи є у нього відомості про конкретну особу або коло осіб, які могли мати фізичний чи логічний доступ до системи; чи використовувались під час виявлення події технічні засоби фіксації, зокрема скріншоти, фото-, відеозапис, резервні копії, автоматичні повідомлення системи, засоби моніторингу або аудиту; якими доказами заявник може підтвердити факт незаконного втручання тощо.

Загалом складність допиту визначається не лише тим, що слідчому нерідко протистоїть особа, яка не бажає надавати правдиві показання, але й тим, що навіть добросовісний допитуваний може помилятися, неповно чи перекручено сприймати події [147, с. 34], неправильно інтерпретувати технічні процеси або відтворювати інформацію з урахуванням власних суб’єктивних уявлень. Усе це

потребує від слідчого вміння вчасно виявити неточності, викривлення чи припущення і врахувати їх у процесі встановлення об’єктивних обставин кримінального провадження [60, с. 352–353]. Тому під час допиту, зокрема свідків, у кримінальних провадженнях про незаконне втручання в роботу автоматизованих систем можуть виникати такі типові ситуації підвищеної складності: а) допитувана особа володіє необхідною інформацією, однак свідомо її приховує; б) допитувана особа має значущі відомості, але навмисне викладає їх у спотвореному вигляді; в) допитувана особа добросовісно повідомляє певні відомості, проте вони не повністю відповідають дійсності через помилки сприйняття, недостатню технічну обізнаність чи викривлення пам’яті; г) допитувана особа взагалі не володіє інформацією, яка цікавить слідство [51; 21, с. 160].

У зв’язку з цим на початковому етапі проведення допиту доцільно використовувати такі тактичні прийоми, як встановлення психологічного контакту, з’ясування анкетних і біографічних даних, вільна бесіда. Після заповнення анкетної частини протоколу допитуваній особі спочатку доцільно запропонувати у формі вільної розповіді викласти все, що їй відомо про обставини, які цікавлять орган досудового розслідування. Надалі слідчий повинен ставити уточнювальні запитання, які допомагають деталізувати показання, перевірити їх послідовність, виявити можливі суперечності та спонукати особу до подальшої розповіді. При цьому запитання мають відповідати таким критеріям: бути конкретними, чіткими, лаконічними і не допускати подвійного тлумачення; не містити у своєму формулюванні підказки або фактичної відповіді на поставлене запитання; бути логічно пов’язаними між собою та послідовними, без безпідставного переходу з одного предмета на інший. Вирішення питання про місце проведення допиту залежить від конкретної слідчої ситуації. У кримінальних провадженнях щодо незаконного втручання в роботу автоматизованих систем допити, як правило, проводяться або за місцем здійснення розслідування, або за місцем перебування допитуваної особи, якщо це зумовлено її станом, службовим становищем, умовами безпеки

або потребою забезпечити таємницю досудового розслідування. Водночас у будь-якому разі слідчий повинен прагнути до того, щоб місце проведення допиту відповідало вимогам, що висуваються до обстановки цієї слідчої дії: було зручним, не створювало додаткового психологічного тиску, сприяло встановленню контакту з допитуваним, забезпечувало його зосередженість на предметі допиту та виключало сторонній вплив на зміст показань.

З урахуванням результатів вивчення слідчої практики вважаємо за доцільне запропонувати певну градацію типових свідків у кримінальних провадженнях про незаконне втручання в роботу автоматизованих систем в органах та установах системи правосуддя, а саме:

Працівники органів та установ системи правосуддя, які безпосередньо працюють із відповідною автоматизованою системою або мають стосунок до її функціонування. До них можуть належати судді, працівники апарату суду, секретарі судових засідань, помічники суддів, працівники канцелярії, підрозділів технічного забезпечення, особи, відповідальні за електронний документообіг чи автоматизований розподіл справ. Їх допитують насамперед щодо того, чи відомі їм обставини втручання, які саме дії з системою здійснювалися, хто мав доступ до відповідних модулів, чи спостерігалися порушення в розподілі справ, зникнення документів або інші явища.

Керівники, колеги по роботі, підпорядковані та інші особи, які перебували у службових або професійних зв’язках із підозрюваним. Вони можуть повідомити відомості про його службове становище, функціональні обов’язки, обсяг доступу до автоматизованих систем, рівень технічної обізнаності, поведінку до і після події, взаємини з іншими працівниками, коло спілкування, наявність конфліктів, інтерес до конкретних справ або документів, а також можливі мотиви втручання.

Члени сім’ї, близькі родичі, друзі, знайомі підозрюваного. Насамперед вони можуть надати інформацію про спосіб життя цієї особи, коло її контактів, користування технічними пристроями, наявність спеціальних знань у сфері інформаційних технологій, використання додаткових комп’ютерів, носіїв

інформації, мобільних пристроїв, а також обставини придбання чи зберігання відповідного обладнання. Разом із тим члени сім'ї та близькі родичі, посилаючись на ст. 63 Конституції України, у певних випадках відмовляються давати показання чи пояснення щодо себе, членів сім'ї або близьких родичів, коло яких визначене законом.

Інші особи, які володіють інформацією і можуть бути дотичними до окремих епізодів події кримінального правопорушення. Ними можуть бути працівники служби технічної підтримки, працівники судової адміністрації, адвокати, фахівці із захисту інформації, особи, які обслуговували техніку, встановлювали програмні продукти, надавали консультації, ремонтували обладнання, або іншим чином мали стосунок до функціонування системи. Крім того, до цієї групи можуть належати особи, які були очевидцями певних дій, пов'язаних із використанням комп'ютерної техніки, входом до службових приміщень, перенесенням носіїв інформації чи обговоренням планів незаконного доступу.

Приймаючи рішення щодо часу проведення допиту зазначених категорій осіб, слідчий, як правило, виходить із конкретної ситуації, що склалася під час розслідування. Крім того, час допиту визначається з урахуванням важливості показань, якими, на думку слідчого, володіє допитуваний, зв'язку його показань з іншими доказами, кола осіб, яких ще належить допитати, а також необхідності збереження таємниці досудового розслідування. На вирішення цього питання впливають також обрана слідчим послідовність допиту тих чи інших осіб, ризик узгодження ними позицій, можливість втрати електронних доказів, службова залежність одних свідків від інших, а також психоемоційний стан допитуваної особи. Не рекомендується проводити допит осіб, які перебувають у стані сильного хвилювання, пригніченості, неуважності чи виявляють очевидні ознаки виснаження, до моменту їх повернення у більш стабільний стан, за винятком випадків, коли такий допит є невідкладним [7, с. 144–145].

У випадку зібрання достатнього обсягу доказів першому допиту підозрюваного у кримінальному провадженні щодо незаконного втручання в

роботу автоматизованих систем в органах та установах системи правосуддя передує процедура вручення письмового повідомлення про підозру у вчиненні кримінального правопорушення та роз'яснення прав підозрюваного згідно зі ст.42, 276–278 КПК України. Відповідно до ст. 42 КПК України підозрюваним є особа, якій у порядку, передбаченому ст. 276–279 цього Кодексу, повідомлено про підозру; особа, затримана за підозрою у вчиненні кримінального правопорушення; а також особа, щодо якої складено повідомлення про підозру, однак його не вручено внаслідок невстановлення місцезнаходження такої особи, за умови, що вжито заходів для вручення повідомлення у спосіб, передбачений кримінальним процесуальним законом [72].

У протоколі допиту мають бути повно і послідовно відображені всі відомості, повідомлені допитуваним, а також інформація про виявлені порушення порядку функціонування автоматизованої системи, режиму доступу до неї, правил користування обліковими записами, адміністрування, електронного документообігу, автоматизованого розподілу справ чи інших пов'язаних процесів із посиланням на конкретні документи. Під час допиту підозрюваного може виникнути необхідність участі спеціаліста. Такий спеціаліст, з дозволу сторони кримінального провадження, яка його залучила, має право ставити запитання допитуваному, користуватися технічними засобами, звертати увагу сторони кримінального провадження або суду на характерні обставини чи особливості речей, документів, електронних носіїв інформації, технічних пристроїв, програмних продуктів, параметрів доступу, інформаційних слідів або інших об'єктів.

Водночас вважаємо за необхідне навести типові властивості поведінки підозрюваних у вчиненні незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя під час допиту, які можуть перешкоджати ефективному проведенню цієї слідчої (розшукової) дії. Зокрема, до них належать: 1) штучність формально-логічної структури показань, коли відповіді підозрюваного є надмірно стриманими, «сухими», мають характер навмисно офіційного пояснення, не виходять за межі мінімально безпечної для

нього інформації та не містять природних деталей, які властиві реальному сприйняттю події; 2) «відхід» від теми, коли допитуваний уникає прямих відповідей на конкретні запитання щодо доступу до автоматизованої системи, своїх дій у ній, використання технічних засобів, присутності на робочому місці в певний час, зберігання ключів доступу, налаштування обладнання чи взаємодії з іншими особами, посилаючись на необізнаність, забудькуватість, відсутність технічної компетентності або формальний характер своїх повноважень. У разі невизнання вини, зокрема шляхом надання неправдивих показань, доцільно застосовувати тактичні прийоми, напрацьовані криміналістикою для подібних ситуацій. Це можуть бути прийоми емоційного впливу, логічного впливу, а також тактичні комбінації.

До прийомів емоційного впливу на підозрюваного, які виокремлюються в криміналістиці та можуть застосовуватися у кримінальних провадженнях цієї категорії, належать:

– спонукання до каяття і правдивих показань шляхом роз’яснення як негативних наслідків неправди, так і можливих сприятливих наслідків визнання своєї ролі, щирого сприяння слідству;

– використання фактору раптовості шляхом постановки несподіваних запитань у момент, коли підозрюваний не очікує переходу до конкретних технічних аспектів справи, почувається внутрішньо захищеним через нібито безпечний, на його погляд, напрям допиту, і тому втрачає контроль над заздалегідь підготовленою моделлю поведінки [60, с. 359–362].

Прийоми логічного впливу полягають у демонстрації невідповідності показань допитуваного фактичним обставинам і наявним доказам. До їх числа належать:

– пред’явлення доказів, що спростовують показання підозрюваного: а) від менш вагомих до більш вагомих; б) шляхом негайного пред’явлення найбільш переконливого доказу, наприклад журналу подій системи, відомостей про авторизацію з конкретного облікового запису, даних із сервера, інформації про час входу до системи, історії змін електронного документа, переписки щодо

отримання доступу або виявлених збігів між діями підозрюваного та технічними слідами;

– логічний аналіз суперечностей, що містяться в показаннях підозрюваного, зокрема між його твердженнями про відсутність доступу до системи і наявними даними про використання його облікових даних, між поясненнями про випадковість змін і їх технічно складним характером, між посиланням на необізнаність і фактичним рівнем його службових або технічних повноважень;

– доведення безглуздості обраної позиції, коли підозрюваному послідовно демонструється, що його версія подій не узгоджується з установленою логікою функціонування системи, послідовністю технічних дій, цифровими слідами, показаннями свідків чи наявними документами [60, с. 359–362].

Під тактичною комбінацією під час допиту слід розуміти створення такої ситуації, яка розрахована на неправильну оцінку її допитуваним і внаслідок цього об’єктивно призводить до його викриття. У межах тактичних комбінацій можуть застосовуватися:

– прийоми, спрямовані на приховування від допитуваного реального обсягу поінформованості слідчого щодо технічного механізму втручання, послідовності дій у системі, або використаних пристроїв;

– метод непрямого допиту, який полягає у постановці питань, що з точки зору допитуваного мають другорядний характер, але фактично маскують головне питання. Наприклад, якщо слідству відомо, що в певний час підозрюваний здійснював доступ до автоматизованої системи з конкретного робочого місця або пристрою, спочатку з’ясовуються обставини його перебування у відповідному приміщенні, режим користування службовим комп’ютером, порядок отримання ключів доступу, що надалі виключає можливість стверджувати, ніби відповідні цифрові сліди виникли раніше, пізніше або були залишені іншою особою;

– прийоми, спрямовані на створення ситуації, за якої допитуваний обмовляється, розкриває технічні деталі, відомі лише безпосередньому

виконавцю, або суперечить сам собі щодо обставин користування системою, послідовності дій, місця перебування, доступу до пристроїв чи характеру взаємодії з іншими учасниками [60, с. 359–562].

Отже, тактика допиту підозрюваного під час досудового розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя полягає в такому: 1) ґрунтовна підготовка до допиту; 2) складання плану допиту з визначенням переліку обставин і питань, які необхідно з'ясувати; 3) підготовка всіх необхідних матеріалів кримінального провадження для можливого пред'явлення допитуваному – протоколів огляду, висновків спеціалістів, лог-файлів, електронних документів, скріншотів, відомостей із серверів, внутрішніх актів, службового листування та інших доказів; 4) за наявності кількох підозрюваних доцільно розпочинати допити з другорядних учасників протиправної діяльності або осіб, роль яких є менш захищеною та більш залежною від інших співучасників; 5) спочатку одержати показання щодо окремих обставин, а вже потім, за потреби, пред'являти докази як підтвердження чи спростування сказаного; 6) пред'являти докази у порядку зростання їх переконливості – від менш значних до найбільш вагомих; 7) у разі вчинення кримінального правопорушення групою осіб виявляти та використовувати під час допиту суперечності інтересів між її учасниками. Зокрема, під час допиту особи, яка виконувала технічну, допоміжну або посередницьку роль у реалізації незаконного доступу, доцільно відразу з'ясувати: хто і за яких обставин залучив її до відповідних дій; чи не була вона сама ініціатором використання певних технічних рішень або способів обходу захисту; яку вигоду, перевагу, обіцянку або іншу форму заохочення їй було запропоновано і що вона фактично одержала; коли, де і за яких умов вона контактувала з безпосереднім виконавцем втручання, користувачем системи, працівником апарату суду, адміністратором або іншими причетними особами; хто може це підтвердити; які засоби зв'язку або технічні пристрої використовувались. При цьому, науковці єдині у поглядах щодо доцільності застосування у ході допиту звуко- та відеозапису з метою мінімізації ризику

подальшої зміни підозрюваним або обвинуваченим раніше наданих показань чи відмови від них. Звуко- та відеозапис мають важливе значення і для фіксації емоційного забарвлення висловлювань, інтонацій, реакцій на окремі запитання, а також вживаних спеціальних технічних термінів [172, с. 55–56].

Слід звернути увагу і на те, що у кримінальних провадженнях цієї категорії може виникнути потреба в проведенні одночасного допиту двох чи більше вже допитаних осіб, зокрема свідків, підозрюваних. Означувана слідча (розшукова) дія, що полягає в почерговому допиті в присутності один одного двох чи більше вже допитаних осіб щодо спільних обставин кримінального провадження, у безперервному аналізі, порівнянні та зіставленні їхніх показань з метою з'ясування причин наявних розбіжностей і перевірки вже отриманої доказової інформації [4, с. 658–659]. Необхідно наголосити на важливості складання плану відповідної слідчої (розшукової) дії, що є запорукою її належної організації. План має включати: 1) завдання одночасного допиту та перелік розбіжностей, причини яких належить з'ясувати; 2) коло питань, які необхідно поставити кожній із допитуваних осіб; 3) час і місце проведення цієї слідчої дії; 4) орієнтири щодо наявних доказів, які дозволяють поставити під сумнів помилкові чи неправдиві показання та підтверджують правдиві; 5) перелік технічних засобів, необхідних для проведення допиту; 6) дії, які мають бути здійснені одразу після завершення одночасного допиту, причому бажано розробити кілька варіантів – на випадок, якщо допит досягне своєї мети, і на випадок, якщо він не дасть очікуваного результату [32, с. 305].

На початку такого допиту встановлюють, чи знають особи одна одну і в яких відносинах вони перебувають. Свідків попереджають про кримінальну відповідальність за відмову від давання показань та за завідомо неправдиві показання, а потерпілих – за завідомо неправдиві показання. Після цього викликаним особам почергово пропонують дати показання щодо тих обставин кримінального провадження, для з'ясування яких проводиться одночасний допит, а вже потім слідчий чи прокурор ставить уточнювальні запитання. Особи, які беруть участь у допиті, а також їхні захисники чи представники мають право

ставити одна одній запитання, що стосуються предмета допиту. Оголошення показань, наданих учасниками на попередніх допитах, допускається лише після того, як вони вже надали показання в ході цієї слідчої дії. Пізнавальна сутність одночасного допиту полягає в безперервному аналізі та порівнянні повідомлюваних відомостей між собою та з іншими матеріалами досудового розслідування. Тактика одночасного допиту двох чи більше вже допитаних осіб ґрунтується на таких пізнавальних прийомах, як: розповідь, розпитування, аналіз міміки та жестів, логічне порівняння і зіставлення.

Основними прийомами підвищення ефективності одночасного допиту у кримінальних провадженнях, розпочатих за фактом незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя, є: надання учасникам одночасного допиту можливості більш ініціативно висловитися щодо тих питань, з приводу яких виникли суперечності; розгляд спірних обставин у зворотній послідовності розвитку подій; пред'явлення доказів для актуалізації асоціативних зв'язків пам'яті; поділ предмета одночасного допиту на окремі смислові блоки; загострення суперечностей у показаннях допитуваних щодо менш значущих обставин з подальшим переходом до основних епізодів; припинення неправдивої версії одного з учасників із акцентуванням уваги на послідовності та правдоподібності показань іншого; уповільнений темп допиту; зміна черговості постановки запитань. Необхідно пам'ятати і про доцільність залучення до проведення цієї процесуальної дії спеціаліста з метою розширення можливостей слідчого чи прокурора в одержанні, перевірці та правильному тлумаченні доказової інформації, особливо якщо суперечності стосуються технічних аспектів автоматизованої системи, параметрів доступу чи специфіки програмного забезпечення.

3.4. Використання спеціальних знань та призначення судових експертиз

Сучасний етап розвитку криміналістики, судової експертології та цифрових технологій характеризується активною інтеграцією знань із суміжних галузей, а також упровадженням новітніх методів і засобів для вирішення завдань, що виникають у процесі розслідування кримінальних правопорушень. За нинішніх умов досудове розслідування фактично неможливо уявити без системного використання досягнень науково-технічного прогресу та залучення обізнаних осіб, здатних забезпечити належне виявлення, фіксацію, вилучення, збереження й дослідження доказової інформації. Особливої актуальності це набуває у кримінальних провадженнях щодо незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя, де переважна більшість відомостей про подію кримінального правопорушення має цифрову природу, а механізм посягання нерідко є прихованим, технічно складним і багаторівневим [80, с. 151; 195, с. 89].

Як зазначає В. В. Тищенко, пізнання під час розслідування здійснюється у формі доказування, тобто діяльності, що відбувається у встановленому законом порядку шляхом збирання, дослідження та оцінки доказів [167, с. 158]. У провадженнях, пов’язаних із незаконним втручанням у роботу автоматизованих систем в органах та установах системи правосуддя, доказова база здебільшого формується навколо електронних документів, журналів подій, лог-файлів, метаданих, відомостей про авторизацію користувачів, мережеву активність, параметри доступу до інформаційних ресурсів, конфігурацію програмного забезпечення, резервні копії, дані серверного обладнання та інших цифрових слідів. За таких обставин повне, всебічне й об’єктивне встановлення фактичних даних вимагає поєднання правової компетентності слідчого і прокурора з фаховими можливостями спеціалістів та експертів, які володіють знаннями у сфері комп’ютерної техніки, телекомунікацій, програмування, кібербезпеки,

захисту інформації, системного адміністрування, цифрової криміналістики, електронного документообігу та технічного супроводу інформаційних систем.

Відповідно до ст. 71 КПК України спеціалістом у кримінальному провадженні є особа, яка володіє спеціальними знаннями та навичками. Водночас процесуальний закон не містить легального визначення поняття «спеціальні знання», що зумовило існування різних підходів у науці. Так, В. Ю. Шепітько визначає спеціальні знання як сукупність знань в окремій галузі науки, техніки, мистецтва чи ремесла [199, с. 207]. В. Г. Гончаренко пов'язує їх з основою спеціальностей і спеціалізацій та наголошує на кримінально-процесуальному значенні таких знань як засобу одержання доказової інформації спеціально підготовленими особами [29, с. 5]. На думку М. Г. Щербаковського, спеціальні знання охоплюють як результати навчання, так і практичні навички, набуті у професійній діяльності, хоча автор переважно акцентує на їх реалізації у формі судової експертизи [161, с. 3]. Узагальнення наведених підходів дає підстави стверджувати, що у кримінальному провадженні спеціальні знання не зводяться виключно до експертного дослідження, а використовуються значно ширше – як у процесуальних, так і в організаційно-тактичних формах, забезпечуючи результативність слідчих (розшукових) дій, правильне виявлення цифрових слідів та коректну інтерпретацію технічних даних.

Для належного розуміння сутності спеціальних знань доцільно виокремити їх основні ознаки: 1) загальна спрямованість на сприяння виконанню завдань кримінального провадження, передусім – швидке і повне встановлення фактичних обставин події; 2) опора на сучасні досягнення науки, техніки та інформаційних технологій; 3) поєднання теоретичних відомостей із практичними вміннями і навичками; 4) набуття шляхом спеціальної підготовки або професійного досвіду [184, с. 40]. Ці ознаки мають принципове значення саме для розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя, де доказування безпосередньо пов'язане з виявленням несанкціонованого доступу, аналізом технічної архітектури системи, встановленням способу модифікації електронних даних,

відновленням видаленої або зміненої інформації, дослідженням алгоритмів функціонування програмного забезпечення, визначенням ролей користувачів і технічних наслідків втручання.

У кримінальному провадженні спеціальні знання можуть бути класифіковані за різними критеріями, зокрема: 1) за суб'єктом застосування – спеціаліст або експерт; 2) за етапом розслідування – використання на стадії виявлення ознак кримінального правопорушення, під час огляду місця події, проведення обшуку, тимчасового доступу до речей і документів, огляду комп'ютерної техніки, зняття інформації з електронних інформаційних систем, призначення та проведення експертиз; 3) за предметом і сферою спеціальних знань – технічні знання у сфері комп'ютерних систем, знання у сфері захисту інформації, адміністрування автоматизованих систем, програмної інженерії, телекомунікацій, електронного документообігу, криптографічного захисту, цифрової ідентифікації користувачів тощо [166, с. 84]. З огляду на постійний розвиток інформаційних технологій перелік необхідних компетенцій фактично не є вичерпним, адже зі зміною програмних платформ, архітектури інформаційних систем, способів зберігання даних та механізмів автентифікації розширюється і коло спеціальних знань, необхідних для належного доказування.

Емпіричні дані, отримані у межах проведеного дослідження, свідчать, що допомога спеціалістів у кримінальних провадженнях зазначеної категорії використовується у переважній більшості випадків у різних формах – як процесуальних, так і непроцесуальних: спеціалісти залучалися до проведення слідчих (розшукових) дій (52%); надавали консультації щодо виявлення, фіксації та вилучення цифрових слідів (45%); надавали пояснення як спеціалісти у суді відповідно до ст. ст. 357, 358 КПК України (31%) (додаток В).

Для досудового розслідування незаконного втручання в роботу автоматизованих систем така тенденція є закономірною, оскільки значна частина доказової інформації «міститься» не у традиційних матеріальних носіях, а в електронному середовищі, що потребує фахового аналізу вже на початкових етапах провадження. Зокрема, у провадженнях щодо незаконного втручання в

роботу автоматизованих систем в органах та установах системи правосуддя участь спеціаліста під час огляду місця події, огляду комп'ютерної техніки, серверного обладнання, мережевих ресурсів або електронних носіїв інформації, обшуку, тимчасового доступу до речей і документів тощо дозволяє: визначити оптимальний перелік технічних пристроїв, облікових записів, файлів, журналів подій і баз даних, що підлягають вилученню чи копіюванню; встановити можливі місця зберігання доказової інформації, у тому числі у віддалених сховищах, резервних копіях, мережевих архівах, хмарних сервісах або на віртуальних серверах; швидко інтерпретувати зміст технічних параметрів, налаштувань доступу, часових міток, системних помилок, мережевих з'єднань і змін у структурі електронних документів; виявити ознаки несанкціонованого доступу, модифікації, видалення або блокування інформації, а також типові сліди стороннього втручання у функціонування програмного забезпечення. У підсумку це створює передумови для якісного призначення судових експертиз і суттєво зменшує ризик втрати, пошкодження або процесуально неправильного вилучення цифрових доказів.

Доцільно розмежовувати й основні види консультацій спеціаліста, що є найбільш затребуваними у провадженнях цієї категорії: 1) консультації загального, орієнтуючого характеру – для розуміння принципів функціонування конкретної автоматизованої системи, її архітектури, ролей користувачів, порядку документообігу, механізмів фіксації подій та основних вузлів накопичення доказової інформації на етапі планування і проведення первинних невідкладних слідчих (розшукових) дій; 2) консультації з конкретних спеціальних питань – під час підготовки та проведення окремих процесуальних дій, коли необхідно вирішити питання щодо способу копіювання даних, забезпечення цілісності електронної інформації, відновлення видалених файлів, фіксації структури цифрового середовища, ідентифікації користувачів або визначення доцільності призначення певного виду судової експертизи [50, с. 46; 22, с. 53]. Наприклад, участь спеціаліста під час огляду технічного обладнання чи інформаційної системи дає можливість слідчому своєчасно зорієнтуватися у конфігурації

програмного середовища, виявити критично важливі цифрові сліди, правильно описати спосіб функціонування системи та зафіксувати ознаки стороннього втручання [65, с. 32].

Водночас слід визнати, що проведення огляду комп'ютерної техніки, електронних носіїв або автоматизованих систем без залучення спеціаліста нерідко перетворюється на типову організаційно-тактичну помилку, наслідком якої є неповнота виявлення цифрових слідів, порушення порядку фіксації технічної обстановки, неналежне копіювання інформації, втрата метаданих, неправильне тлумачення функціонального призначення системи або навіть пошкодження доказово значущих даних. У справах цієї категорії така помилка має особливо негативні наслідки, оскільки будь-яке необережне втручання у програмне чи апаратне середовище може призвести до зміни стану системи, автоматичного видалення інформації, втрати журналів подій або неможливості подальшого експертного дослідження.

Обираючи спеціаліста, необхідно враховувати обставини, що визначають можливість його участі у кримінальному провадженні, оскільки порушення порядку залучення обізнаних осіб може негативно вплинути на оцінку доказів у суді. Доцільним є попереднє з'ясування: 1) відсутності особистої зацікавленості у результатах провадження та будь-яких зв'язків із відповідним органом, установою системи правосуддя, адміністратором системи чи конкретними користувачами, дії яких перевіряються; 2) відсутності участі особи у провадженні в іншому процесуальному статусі; 3) наявності документів, що підтверджують кваліфікацію і компетентність у відповідній технічній сфері (дипломи, сертифікати, свідоцтва, підтвердження права на адміністрування або обслуговування відповідних систем, досвід роботи з комп'ютерною технікою, мережами, системами захисту інформації тощо) [165, с. 54].

Серед основних напрямів використання спеціальних знань під час розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя особливе місце посідає призначення та проведення судової експертизи. Для цієї категорії кримінальних проваджень

характерними є значні масиви електронних даних, складна технічна архітектура інформаційних систем, багаторівнева структура доступу користувачів, необхідність аналізу мережевої активності, журналів подій, цифрових слідів зміни чи знищення інформації, а також встановлення способу несанкціонованого впливу на функціонування програмно-апаратного комплексу. За таких умов лише професійне дослідження з використанням спеціальних знань дає змогу встановити технічний механізм втручання, його наслідки, засоби реалізації, джерело походження змін та інші фактичні обставини, що мають значення для кримінального провадження.

У практичній діяльності та наукових джерелах поняття «експертиза» є багатозначним. Так, Н. В. Тутецька наголошує, що експертизу слід розуміти як інститут доказового й процесуального права, систему процесуальних відносин, форму використання спеціальних знань, різновид слідчої діяльності, процедуру дослідження та документ, оформлений за результатами її проведення, – висновок експерта [173, с. 357]. Подібної позиції дотримується і В. Ю. Шепітько, підкреслюючи, що судова експертиза є процесуальною дією, яка полягає в дослідженні експертом за завданням слідчого або суду речових доказів та інших матеріалів із метою встановлення фактичних даних і обставин, що мають значення для правильного вирішення справи [57, с. 257].

Нормативне визначення судово-експертної діяльності міститься у ст. 1 Закону України «Про судову експертизу», де вона розкривається як дослідження на основі спеціальних знань у галузі науки, техніки, мистецтва, ремесла тощо об’єктів, явищ і процесів з метою надання висновку з питань, що є або будуть предметом судового розгляду [137]. У кримінальному провадженні експертом визнається особа, яка володіє науковими, технічними або іншими спеціальними знаннями, має право відповідно до Закону України «Про судову експертизу» на проведення експертизи і якій доручено здійснити дослідження об’єктів, явищ і процесів, що містять відомості про обставини вчинення кримінального правопорушення, та надати висновок з питань, що виникають під час провадження і належать до сфери її знань (ч. 1 ст. 69 КПК України).

Процесуальні права, обов'язки та відповідальність експерта визначені у ст. 69–70 КПК України, а висновок експерта відповідно до положень глави 4 КПК України належить до процесуальних джерел доказів [72].

Зіставлення наведених положень дозволяє дійти висновку, що спеціаліст і експерт мають спільні риси: обидва володіють спеціальними знаннями, залучаються до кримінального провадження та не повинні бути заінтересованими в його результатах. Водночас їх процесуальні статуси не є тотожними. Відмінність полягає, по-перше, у характері завдань, які перед ними ставляться: експерт здійснює самостійне дослідження та формує доказово значущий висновок, тоді як спеціаліст переважно надає технічну допомогу, консультації, роз'яснення та сприяє проведенню процесуальних дій; по-друге, у наявності кримінальної відповідальності експерта за завідомо неправдивий висновок або безпідставну відмову від виконання покладених на нього обов'язків (ст. ст. 384–385 КК України); по-третє, у відмінностях процесуального оформлення результатів їх діяльності та доказовому значенні відповідних документів [72; 93, с. 61].

Судово-експертну діяльність здійснюють спеціалізовані установи, їх територіальні підрозділи, а також судові експерти, які не є працівниками таких установ, та інші фахівці з відповідних галузей знань [137]. Для кримінальних проваджень щодо незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя найбільш типовими є комп'ютерно-технічні експертизи, телекомунікаційні дослідження, експертизи у сфері технічного захисту інформації, дослідження програмних продуктів, а також, залежно від способу втручання та характеру змінених даних, технічні експертизи документів, почеркознавчі експертизи (якщо посягання супроводжувалося використанням паперових документів чи підробкою супровідної документації), а в окремих випадках – комплексні експертизи, що поєднують цифровий, документальний і телекомунікаційний компоненти.

Практика свідчить, що у цій категорії справ найчастіше виникає потреба у вирішенні таких експертних завдань: встановлення факту несанкціонованого

доступу до автоматизованої системи або її окремих модулів; визначення способу проникнення до системи; встановлення ознак внесення змін до електронних документів, реєстраційних форм, журналів подій чи баз даних; виявлення фактів знищення, блокування, копіювання або підміни інформації; ідентифікація технічних пристроїв, з яких здійснювався доступ; аналіз часу, послідовності та технічних параметрів дій користувача; встановлення можливості відновлення видалених даних; визначення цілісності та автентичності електронної інформації; з'ясування, чи могли певні технічні зміни виникнути внаслідок штатного функціонування системи, чи вони є результатом стороннього втручання.

Ефективність експертного дослідження прямо залежить від узгодженості дій слідчого (прокурора) та експерта: своєчасного визначення предмета і меж дослідження, правильного відбору й фіксації об'єктів, коректного формулювання питань, а також повного і репрезентативного надання матеріалів, необхідних для дослідження. У науковій літературі обґрунтовано підкреслюється, що попереднє обговорення завдань експертизи й належна організація доказового забезпечення з боку слідства мінімізують ризики повернення матеріалів або необхідності призначення повторних чи додаткових досліджень [5, с. 107]. За організаційно-процесуальними підставами судові експертизи традиційно поділяють за послідовністю на первинні та повторні, за обсягом – на основні й додаткові, за чисельністю і складом експертів – на одноособові та комісійні [182, с. 47]. Водночас саме у провадженнях щодо незаконного втручання в роботу автоматизованих систем особливої ваги набуває також поділ на однорідні та комплексні експертизи, оскільки дослідження часто потребує одночасного використання знань у кількох технічних сферах.

Аналіз слідчої та судової практики дає підстави виокремити низку типових проблем, які знижують доказову цінність експертних висновків або штучно збільшують строки досудового розслідування. До таких недоліків належать: нечітке уявлення про предмет експертизи і межі компетенції експерта; непризначення експертизи у випадках, коли без неї неможливо встановити

ключові обставини механізму втручання; постановка звуженого, неточного або помилкового кола запитань, яке не враховує складності цифрового середовища; ненадання експерту повного комплексу вихідних даних (журналів подій, резервних копій, технічної документації, зразків електронних документів, відомостей про користувачів, конфігурацій системи); порушення правил вилучення або копіювання цифрової інформації, що ускладнює або унеможливлює подальше експертне дослідження. Як слушно зазначається в літературі, причинами таких помилок є як суб'єктивні чинники (недостатній практичний досвід слідчих і недостатня поінформованість про можливості відповідних видів експертиз), так і об'єктивні (відсутність системного узагальнення слідчо-експертної практики, прогалини професійної підготовки та недосконаліть окремих аспектів законодавчої регламентації взаємодії слідчого й експерта) [82, с. 17].

З метою забезпечення єдиного підходу до призначення та проведення судових експертиз і підвищення якості експертних досліджень Міністерством юстиції України на виконання вимог Закону України «Про судову експертизу» наказом від 08 жовтня 1998 р. № 53/5 затверджено Інструкцію про призначення та проведення судових експертиз та експертних досліджень і Науково-методичні рекомендації з питань підготовки та призначення судових експертиз та експертних досліджень [124]. Для розслідування незаконного втручання в роботу автоматизованих систем практична цінність цих актів полягає насамперед у тому, що вони орієнтують слідчого на правильне визначення об'єктів дослідження, меж компетенції експерта та загальних вимог до формулювання питань. У цій категорії проваджень перед експертом доцільно ставити не абстрактні питання про «злам системи» чи «незаконність дій», а конкретні технічні запитання, наприклад: чи містить наданий носій або серверне середовище сліди стороннього втручання; чи вносилися зміни до електронних документів, реєстраційних записів або журналів подій; чи є можливим встановити обліковий запис, з якого здійснювалися певні дії; чи могли виявлені зміни виникнути внаслідок штатного функціонування системи; чи були видалені

певні відомості та чи підлягають вони відновленню; з якого технічного засобу або мережевого сегмента було ініційовано доступ; чи відповідає наявний стан системи її нормативно визначеному режиму функціонування.

Практика підтверджує, що специфіка досліджуваної категорії кримінальних правопорушень майже завжди потребує комплексного підходу: у межах одного кримінального провадження можуть послідовно або паралельно призначатися кілька експертиз різного профілю. Наприклад, комп'ютерно-технічна експертиза може встановлювати спосіб доступу до системи та характер змін у цифровому середовищі, тоді як технічна експертиза документів – підтверджувати наявність змін у друкованих формах документів, сформованих із системи, а телекомунікаційне дослідження – встановлювати параметри мережевої взаємодії та джерело підключення. Однією з найбільш проблемних ділянок залишається формулювання питань експерту: слідчі інколи або виходять за межі його компетенції, пропонуючи встановити вину особи, кваліфікувати дії або оцінити умисел, або, навпаки, ставлять надто загальні питання, що не дозволяють отримати доказово значущий результат. Саме тому найбільш раціональним є поєднання використання Науково-методичних рекомендацій із залученням спеціаліста відповідної технічної галузі на стадії підготовки постанови про призначення експертизи – для правильного визначення об'єктів, меж дослідження та логіки запитань.

Окремо необхідно зауважити, що у кримінальних провадженнях цієї категорії на практиці можуть залучатися як експерти державних спеціалізованих установ, так і експерти недержавного сектору або приватні фахівці, за умови наявності в них належної кваліфікації та процесуальних підстав для участі у провадженні. Зазвичай це зумовлено або надмірним завантаженням державних експертних установ, або необхідністю проведення вузькоспеціалізованих досліджень, пов'язаних із конкретними програмними продуктами, складними конфігураціями мережевої інфраструктури, спеціалізованими засобами захисту інформації чи нестандартними способами цифрового втручання [26, с. 132]. Водночас у кожному випадку має бути забезпечене безумовне дотримання вимог

щодо належності, допустимості та процесуальної прозорості залучення такого експерта.

Проведення експертизи як складова судово-експертної діяльності фактично розпочинається з моменту надходження до експертної установи або експерта процесуального документа про її призначення та матеріалів, що додаються, і передачі їх відповідному підрозділу чи конкретному виконавцю для організації дослідження. Якщо ж надані матеріали є неповними, цифрові носії упаковані неналежним чином, не забезпечено збереження їх цілісності, не зафіксовано умови копіювання інформації, відсутні відомості про спосіб вилучення електронних даних, не надано необхідних паролів, ключів доступу, опису конфігурації системи або технічної документації, що унеможливлює проведення повноцінного дослідження, такі матеріали підлягають поверненню ініціаторові для усунення недоліків. У разі надходження матеріалів поштою чи кур'єром ініціатора повідомляють про виявлені недоліки, складається відповідна довідка, а матеріали повертаються для приведення у належний стан [166, с. 251].

Один із найскладніших напрямів використання спеціальних знань під час розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя пов'язаний із дослідженням цифрових носіїв інформації, тобто із призначенням *комп'ютерно-технічної* експертизи. Комп'ютери, ноутбуки, сервери, робочі станції, мобільні телефони, планшети, зовнішні накопичувачі, мережеве обладнання, SIM-картки, картки пам'яті, токени доступу, ключі електронного підпису, а також віртуальні середовища, резервні копії та хмарні сховища нерідко містять сліди підготовки, реалізації або приховування несанкціонованого втручання. Саме у таких об'єктах можуть зберігатися файли конфігурації системи, журнали авторизації, дані про підключення до віддалених ресурсів, історія змін у електронних документах, сліди використання спеціалізованого програмного забезпечення, метадані файлів, інформація про облікові записи користувачів, часові мітки виконання окремих дій, а також інші цифрові сліди, що мають значення для встановлення механізму посягання [166, с. 328–329].

Водночас практика свідчить, що ініціатори експертиз не завжди коректно визначають коло об’єктів дослідження, забезпечують належне вилучення та правильно формулюють запитання, що ускладнює або затягує процес експертного дослідження. До найбільш типових проблем належать: неповне вилучення цифрових носіїв, які фактично містять сліди втручання; порушення правил фіксації, копіювання, зберігання і транспортування електронної інформації; направлення на дослідження об’єктів, які не мають доказового значення або технічно непридатні для повноцінного аналізу; поєднання в одній постанові надмірної кількості різнорідних технічних завдань, що фактично потребують окремих або комплексних досліджень.

З огляду на проведений аналіз кримінальних проваджень та матеріалів судових справ, орієнтовний перелік запитань до експерта у межах комп’ютерно-технічної експертизи може бути таким:

– які саме дані (системні журнали, лог-файли, електронні документи, бази даних, резервні копії, файли конфігурації, відомості про облікові записи, мережеві журнали) містяться на наданому носії або в наданому програмно-апаратному середовищі та в якому форматі вони зберігаються;

– чи містить досліджуваний об’єкт відомості про несанкціонований доступ до автоматизованої системи, її окремих модулів або пов’язаних із нею інформаційних ресурсів;

– чи виявлено на носії електронні документи, журнали подій або інші файли, пов’язані з функціонуванням автоматизованої системи, та які їх метадані (час створення, відкриття, редагування, копіювання, переміщення, видалення, автор, обліковий запис, шлях збереження);

– чи здійснювалося видалення, зміна або блокування інформації; чи можливо її відновити; які саме дані були змінені або видалені та коли це відбулося;

– чи створювалися конкретні файли або електронні документи на цьому пристрої, чи вони були перенесені з інших джерел; якщо так, то яким способом

(через зовнішній носій, локальну мережу, віддалений доступ, месенджер, електронну пошту або хмарний сервіс);

– яка послідовність роботи з конкретним файлом, обліковим записом, модулем системи або базою даних;

– чи є відомості про підключення зовнішніх носіїв, використання засобів віддаленого адміністрування, зміну конфігурації системи, синхронізацію з віддаленими сховищами або використання каналів несанкціонованого обміну даними;

– чи встановлено на пристрої спеціалізоване програмне забезпечення, зокрема засоби віддаленого доступу, адміністрування, шифрування, відновлення або знищення даних, і які сліди його використання містяться у системі;

– чи наявні технічні несправності, що впливають на можливість зчитування або дослідження інформації, та які умови необхідні для коректного вилучення цифрових даних [145, с. 25].

Для розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя істотне значення можуть мати не лише комп’ютерно-технічні експертизи, а й експертні дослідження у сфері *телекомунікацій*, спрямовані на встановлення параметрів мережевої взаємодії, джерел віддаленого доступу, маршрутів передавання даних та інших обставин функціонування каналів електронного зв’язку. Їх необхідність зумовлена тим, що втручання в автоматизовані системи нерідко реалізується не лише шляхом безпосереднього впливу на окремий технічний пристрій чи носій інформації, а й через використання локальних мереж, зовнішніх каналів зв’язку, засобів віддаленого адміністрування, мобільного інтернету, VPN-з’єднань, проксі-серверів, хмарної інфраструктури або інших телекомунікаційних механізмів, які забезпечують передачу даних між користувачем і відповідною системою. У таких випадках без спеціального дослідження мережевої інфраструктури, параметрів підключення та послідовності обміну даними неможливо повноцінно встановити технічний механізм посягання, час, спосіб і джерело доступу до автоматизованої системи [55, с. 93].

Практичне значення експертних досліджень у сфері телекомунікацій полягає в тому, що вони дають можливість встановити, чи здійснювалося підключення до автоматизованої системи ззовні, з якого саме мережевого сегмента або вузла ініційовано доступ, які технічні засоби забезпечували передавання інформації, чи використовувалися засоби приховування або зміни реального джерела мережевої активності, а також чи відбувалася передача інформації на сторонні інформаційні ресурси. У межах такого дослідження можуть аналізуватися мережеві журнали, конфігурація маршрутизаторів і комутаторів, інформація про IP-адресацію, параметри сесій зв'язку, дані операторів електронних комунікацій, журнали VPN-підключень, DHCP-логи, NAT-трансляції, DNS-запити, записи проксі-серверів, відомості про MAC-адреси пристроїв, а також інші технічні дані, що відображають рух інформації мережею. Особливого значення такі дослідження набувають у випадках, коли незаконне втручання здійснюється шляхом використання легітимних облікових даних, але з нетипового місця підключення, у незвичний час або через незвичайний маршрут мережевої взаємодії. У подібних ситуаціях саме аналіз телекомунікаційних параметрів дозволяє відмежувати звичайну службову активність користувача від несанкціонованого доступу, встановити аномальні сеанси зв'язку, виявити ознаки підміни мережевої ідентифікації, використання віддалених серверів або спеціальних засобів маскування. Крім того, результати такого дослідження можуть мати істотне значення для перевірки версій щодо інсайдерського втручання, зовнішньої атаки, використання скомпрометованих облікових записів чи організації колективного доступу до системи з різних технічних вузлів [28].

З огляду на типові слідчі ситуації, у межах експертних досліджень у сфері телекомунікацій можуть вирішуватися, зокрема, такі питання: чи здійснювалося в певний проміжок часу підключення до автоматизованої системи або пов'язаного з нею серверного середовища з конкретної IP-адреси, мережевого сегмента або пристрою; чи використовувалися канали віддаленого доступу, VPN, проксі або інші засоби приховування реального місцезнаходження

користувача; яким був маршрут передавання даних від джерела ініціювання до об’єкта доступу; чи фіксуються ознаки перенаправлення, дублювання або несанкціонованого виведення інформації за межі інформаційної інфраструктури органу чи установи системи правосуддя; чи перебували конкретні технічні пристрої у стані мережевої взаємодії між собою; чи могли певні технічні умови функціонування каналу зв’язку забезпечити виконання конкретних дій у системі в заданий проміжок часу.

Якщо незаконне втручання в роботу автоматизованої системи поєднується з використанням засобів прихованої комунікації, координацією дій між кількома особами або передачею незаконних вказівок, актуалізується потреба у призначенні експертизи *відео-* та *звукозапису*. У таких кримінальних провадженнях органи досудового розслідування можуть вилучати записи розмов, відеофайли з камер спостереження, службових пристроїв або мобільних телефонів, дані, отримані в ході негласних слідчих (розшукових) дій, а також технічні засоби, за допомогою яких здійснювалася фіксація. Відповідно, експертиза відео- та звукозапису використовується для встановлення технічних параметрів і умов створення запису, перевірки його цілісності та автентичності, виключення ознак монтажу, визначення джерела звуку, послідовності фіксації подій, а за наявності належних зразків – для ідентифікації голосу та мовлення конкретних осіб [166, с. 129].

У такій ситуації запитання до експерта мають стосуватися виключно технічних і спеціальних аспектів, без виходу на правову оцінку змісту події. Орієнтовний перелік питань може бути таким: чи зафіксовано на наданому носії відповідну фонограму або відеофонограму; чи здійснювався запис одним чи кількома технічними засобами; чи є наданий запис оригіналом або копією; чи містить він ознаки переривання, дублювання, вирізання, склеювання, перекодування або іншого стороннього втручання; чи здійснювався запис безперервно; чи змінювалися цифрові параметри файлу, що може свідчити про обробку; чи синхронні між собою звукова доріжка та відеоряд; у якому середовищі проводився запис; скільки осіб бере участь у розмові; чи можливо

розмежувати їхні репліки; чи можлива текстова розшифровка мовленнєвих фрагментів із часовими мітками; чи брали конкретні особи участь у розмові, за наявності належних зразків голосу та мовлення. Для повного й обґрунтованого дослідження на експертизу доцільно надавати не лише сам запис, а й первинний носій або пристрій фіксації, інформацію про спосіб отримання файлу, ланцюг його збереження, умови копіювання та належні зразки голосу осіб, щодо яких ставляться ідентифікаційні питання.

Самостійне доказове значення у провадженнях досліджуваної категорії може мати і експертиза *матеріалів, речовин та виробів*, хоча її призначення є ситуативним і залежить від конкретного способу втручання. Така експертиза може бути необхідною, коли незаконне втручання супроводжувалося вчиненням корупційних діянь. У подібних випадках може виникати потреба дослідити речовини чи нашарування на готівкових коштах, корпусах технічних пристроїв, рукавичках або інших предметах, що контактували з відповідними об’єктами. Практичне значення такого дослідження полягає у можливості встановити природу речовини, факт контактної взаємодії між об’єктами, походження окремих нашарувань тощо [30].

Поряд із цим, у провадженнях щодо незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя значну роль може відігравати *почеркознавча* експертиза, якщо цифрове втручання супроводжувалося використанням паперових документів, службових записок, заявок на доступ, журналів реєстрації, розпоряджень, актів передачі носіїв інформації, супровідної технічної документації або інших документів, що містять підписи та рукописні записи. У таких випадках виникає потреба встановити виконавця підписів чи записів, з’ясувати, хто саме оформляв або посвідчував документи, пов’язані з наданням доступу до системи, обігом технічних засобів, передачею паролів, ключів, носіїв інформації або організацією технічного обслуговування [182, с. 89].

Експертне дослідження у такій ситуації спрямовується не на оцінку правомірності дій посадових осіб, а на встановлення факту виконання підпису

чи рукописного запису конкретною особою, виявлення ознак підроблення або імітації письма, а також визначення умов виконання записів. Методика почеркознавчої експертизи традиційно охоплює чотири взаємопов'язані стадії: попереднє ознайомлення з матеріалами, роздільне дослідження, порівняльне дослідження та оцінку результатів із формулюванням висновку. У справах цієї категорії особливу увагу слід приділяти належності об'єктів дослідження до юридично значущих документів, оскільки саме через них нерідко маскується використання чужого імені, підставного виконавця або неуповноваженого доступу до окремих сегментів інформаційної системи.

З урахуванням типових слідчих ситуацій орієнтовний перелік запитань до експерта-почеркознавця може включати: чи виконано підпис або рукописний запис у конкретному документі певною особою; чи виконано кілька підписів однією чи різними особами; чи виконано підпис шляхом наслідування підпису іншої особи або зі свідомою зміною письма; чи виконано рукописні записи в кількох документах однією особою; чи виконано підпис або запис в умовах, що ускладнювали письмово-рухові навички.

У цій категорії проваджень почеркознавчу експертизу доцільно поєднувати з техніко-криміналістичним дослідженням документів, оскільки паперові носії можуть містити не лише рукописні реквізити, а й друкований текст, відбитки печаток, факсиміле, ознаки монтажу, внесення виправлень, заміни аркушів або виготовлення документа не тим способом, який декларується його формою. Технічне дослідження документів у таких випадках охоплює перевірку справжності бланків і реквізитів, встановлення способу нанесення підпису, аналіз відбитків печаток і штампів, виявлення дописок, підчисток, травлення, вклейок, визначення способу виготовлення друкованого тексту та, за наявності технічних умов, ідентифікацію відповідних засобів друку. Наприклад, така експертиза є необхідною, коли існують підстави вважати, що документ, який формально підтверджує законність доступу до системи або передачу технічного носія, був виготовлений шляхом комп'ютерного монтажу, копіювання або комбінування фрагментів із різних джерел [166, с. 149].

Комплексне призначення судово-почеркознавчої та технічної експертизи документів дає змогу одночасно вирішити два принципово важливі блоки питань: хто саме виконав підпис або рукописний запис і яким способом був виготовлений документ та його реквізити. Такий підхід підвищує доказову цінність висновку, зменшує ризик фрагментарного дослідження та дозволяє пов'язати встановлені експертним шляхом обставини з ролями посадових осіб, порядком документообігу, режимом доступу до автоматизованої системи та механізмом реалізації незаконного втручання.

Висновок експерта є підсумковим процесуальним документом, у якому мають бути відображені хід і послідовність проведеного дослідження, використані методи, встановлені ознаки, отримані результати та висновки. Його доказова цінність безпосередньо залежить від того, наскільки повно, прозоро й відтворювано викладено перебіг дослідження, а також від того, чи є зрозумілою інтерпретація результатів для учасників кримінального провадження, які не володіють відповідними фаховими знаннями. Саме тому в практично орієнтованому аспекті доцільно, щоб у висновку експерта технічні терміни супроводжувалися короткими поясненнями, складні цифрові процеси – логічно структурованим описом, а у випадках дослідження електронної інформації, мережевої взаємодії, аудіо- чи відеозаписів використовувалися таблиці, схеми, часові маркери, ілюстративні фрагменти журналів подій, стоп-кадри або інші засоби наочного обґрунтування [15, с. 243;124].

Узагальнюючи вищевикладене, необхідно наголосити, що у кримінальних провадженнях, розпочатих за фактом вчинення незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя, експертні дослідження мають плануватися як продовження слідчих (розшукових) і процесуальних дій – огляду місця події, огляду техніки й цифрових носіїв, обшуку, тимчасового доступу до речей і документів тощо. Встановлено, що для цієї категорії кримінальних проваджень особливо значущими є такі види судових експертиз: комп'ютерно-технічна (для виявлення цифрових слідів втручання, встановлення параметрів створення, зміни, копіювання чи видалення

електронної інформації, відновлення втрачених даних та аналізу дій користувачів у системі); експертні дослідження у сфері телекомунікацій (для встановлення параметрів мережевої взаємодії, джерел віддаленого доступу, маршрутів передавання даних та інших обставин функціонування каналів електронного зв'язку); експертиза відео- та звукозапису (коли необхідно перевірити цілісність і автентичність записів, встановити умови їх створення, ознаки монтажу чи ідентифікувати учасників розмови); почеркознавча та технічна експертиза документів (у випадках, коли втручання супроводжувалося використанням паперових документів, підписів, печаток, службових записок або інших матеріальних носіїв інформації); експертиза матеріалів, речовин і виробів (у ситуаціях корупційного характеру, коли необхідно дослідити нашарування, спеціальні речовини на помічених купюрах чи інші матеріальні сліди). Комплексне та своєчасне використання зазначених видів експертиз істотно підвищує ефективність розслідування, оскільки дозволяє встановити не лише сам факт втручання, а й спосіб його реалізації, часові межі, технічні умови, характер змін в автоматизованій системі та доказово значущий зв'язок між подією кримінального правопорушення і конкретними особами.

Висновки до розділу 3

1. Огляд у кримінальних провадженнях щодо незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя має визначальне значення для первинного виявлення, локалізації та збереження слідів кримінального правопорушення. На відміну від традиційних проваджень, його предметом є не лише матеріальні об'єкти, а й електронне середовище: стан автоматизованої системи, конфігурація технічних засобів, наявні сесії користувачів, журнали подій, мережеві з'єднання, електронні документи та інші дані, які можуть бути змінені або втрачені за короткий проміжок часу. На цій підставі запропоновано науково-практичні рекомендації для слідчих, прокурорів

і спеціалістів щодо алгоритму проведення огляду, який охоплює: визначення меж цифрового середовища огляду; фіксацію стану системи на момент виявлення ознак втручання; розмежування об’єктів, які підлягають візуальному, технічному та процесуальному дослідженню; забезпечення збереження даних; а також правильне документування виявлених цифрових слідів для їх подальшого використання у доказуванні. Доведено, що саме якість і повнота огляду значною мірою визначають можливість подальшого встановлення способу втручання, часових меж події та кола причетних осіб.

2. Обґрунтовано, що обшук повинен розглядатися як цілеспрямована пошуково-фіксаційна дія, спрямована не лише на виявлення окремих речей чи документів, а на відшукання всього арсеналу щодо підготовки, вчинення та приховування кримінального правопорушення. Практичне значення мають не тільки комп’ютери, мобільні телефони, флеш-накопичувачі чи серверне обладнання, а й засоби автентифікації, записані паролі, чорнові записи, службові документи, засоби зв’язку між співучасниками, а у разі корупційної складової – також предмети й документи, що підтверджують передачу неправомірної вигоди. У зв’язку з цим розроблено тактичні рекомендації щодо підготовки та проведення обшуку, які передбачають: визначення кола шуканих об’єктів із урахуванням механізму втручання; забезпечення раптовості; блокування можливості дистанційного знищення інформації; ізоляцію присутніх осіб від технічних пристроїв; правильну послідовність вилучення цифрових носіїв; а також обов’язкове залучення спеціаліста у випадках, коли існує ризик втрати або спотворення електронних доказів. Встановлено, що ефективність обшуку в цій категорії проваджень залежить передусім від здатності слідчого виявити записи, приховані технічні та інформаційні об’єкти, які зовні можуть не мати очевидного доказового значення, але фактично відображають підготовку, реалізацію або приховування незаконного втручання.

3. Допит у кримінальних провадженнях про незаконне втручання в роботу автоматизованих систем є однією з найбільш складних у тактичному відношенні слідчих дій, оскільки поєднує необхідність встановлення юридично значущих фактів із з’ясуванням спеціальних технічних, службових та організаційних

обставин функціонування відповідних систем. Його результативність залежить не стільки від кількості поставлених запитань, скільки від правильної побудови предмета допиту з урахуванням ролі допитуваної особи у механізмі події, рівня її обізнаності з роботою системи та характеру вже зібраних цифрових доказів. На цій основі запропоновано практичні рекомендації для працівників органів досудового розслідування щодо тактики допиту різних категорій осіб: свідків, заявників, підозрюваних та інших учасників кримінального провадження. Рекомендовано структурувати допит за блоками, що стосуються порядку доступу до системи, правил використання облікових записів, факту і часу виявлення збоїв, характеру внесених змін, службових повноважень конкретних осіб, технічних умов функціонування системи та можливого зовнішнього чи внутрішнього впливу на неї. Доведено, що у кримінальних провадженнях цієї категорії показання набувають найбільшої доказової цінності лише за умови їх зіставлення з даними огляду, обшуку та висновками експертів, що дозволяє перевірити достовірність пояснень, викрити неправдиві версії та встановити реальний механізм кримінального правопорушення.

4. Наголошено на тому, що в кримінальних провадженнях, розпочатих за фактом незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя, використання спеціальних знань і призначення судових експертиз повинно розглядатися як логічне продовження проведених слідчих (розшукових) і процесуальних дій, зокрема огляду місця події, огляду комп’ютерної техніки та цифрових носіїв, обшуку, допиту та тимчасового доступу до речей і документів. Визначено, що для цієї категорії кримінальних проваджень найбільше значення мають комп’ютерно-технічна експертиза, дослідження у сфері телекомунікацій, експертиза відео- та звукозапису, почеркознавча і технічна експертиза документів, а також експертиза матеріалів, речовин і виробів. Обґрунтовано, що їх своєчасне і комплексне використання дає змогу встановити факт і спосіб незаконного втручання, часові межі та технічні умови його реалізації, характер змін в автоматизованій системі, наявність цифрових і матеріальних слідів, а також доказово значущий зв’язок між подією кримінального правопорушення та конкретними особами.

ВИСНОВКИ

У **дисертації,** з урахуванням сучасного стану кримінального процесуального законодавства та практики діяльності органів кримінальної юстиції, розроблена криміналістична методика розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя, з визначенням пропозицій та рекомендацій, що набувають праксеологічного значення. Найсуттєвішими з них є такі:

1. Електронне судочинство в Україні є закономірним результатом цифрової трансформації судової влади та одним із пріоритетних напрямів модернізації механізму здійснення правосуддя. Його сутність полягає не лише у впровадженні окремих інформаційно-комунікаційних технологій у діяльність суду, а також у формуванні цілісного, нормативно врегульованого організаційно-правового механізму здійснення судочинства, в межах якого електронні засоби та автоматизовані системи забезпечують створення, передавання, обробку, зберігання й використання процесуально значущої інформації, електронну взаємодію суду з учасниками процесу, рух процесуальних документів, доступ до судової інформації, а також реалізацію принципів доступності, гласності, відкритості, безпеки та процесуальної надійності правосуддя.

Функціональне призначення електронного судочинства в Україні охоплює організаційно-управлінську, документообігову, комунікаційну, ідентифікаційну, інформаційну, аналітичну, гарантійну функції, а також функції відкритості та підзвітності й захисту даних, що в сукупності свідчить про багаторівневий характер правового механізму, спрямованого не лише на технічне вдосконалення судової діяльності, а й на підвищення ефективності, прозорості, доступності, стабільності та безпечності правосуддя.

2. До елементів криміналістичної характеристики незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя

віднесено: особу правопорушника; предмет посягання; способи підготовки, вчинення та приховування; обстановку вчинення; слідову картину.

Осіб, які незаконно втручаються в роботу автоматизованих систем в органах та установах системи правосуддя розподілено на: 1) осіб, які безпосередньо здійснюють професійну діяльність у межах органів та установ системи правосуддя та мають легітимний або службово зумовлений доступ до відповідних автоматизованих інформаційних ресурсів (58%); 2) осіб, які не є безпосередніми працівниками органів та установ системи правосуддя, однак можуть отримувати доступ до таких систем у зв'язку з виконанням професійних, технічних, сервісних чи інших функцій або шляхом використання технічних засобів, спеціальних програм чи наявних вразливостей інформаційного середовища (42%).

Предмет незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя має комплексний характер і охоплює ресурси, які забезпечують функціонування судового адміністрування, рух справ, автоматизований розподіл, електронний документообіг, службову діяльність органів системи правосуддя, обробку персональних даних та фіксацію технічних параметрів роботи відповідних систем.

Незаконне втручання має попередньо підготовлений характер (72%); здійснюється з використанням службових повноважень або наданого у зв'язку із займаною посадою доступу до автоматизованої системи (64%); поєднується з іншими кримінальними правопорушеннями (48%); вчиняється за участю кількох осіб (36%). Найбільш поширеними способами безпосереднього вчинення цього кримінального правопорушення є несанкціоновані дії з інформацією, що міститься в автоматизованих системах, або інше незаконне втручання в їх роботу (69%), а також внесення неправдивих відомостей чи несвоєчасне внесення інформації до відповідних систем (57%). Приховування незаконного втручання найчастіше здійснюється шляхом внесення до системи недостовірних або змінених даних (62%), використання чужих облікових записів (51%), видалення чи модифікації електронних записів (46%), що свідчить про високий рівень

адаптації способів протиправної поведінки до особливостей цифрового середовища.

Обстановка незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя формується під впливом сукупності організаційних, службових, технічних та інформаційних умов, які створюють сприятливе середовище для реалізації злочинного наміру. Найбільш істотними серед них є: наявність у особи доступу до автоматизованої системи (62,8%), недоліки внутрішнього контролю за засобами авторизації (48,6%), обізнаність із порядком функціонування системи чи її окремих модулів (44,1%), а також неналежний рівень технічного аудиту, журналювання подій і моніторингу змін в інформаційному середовищі (33,4%).

Найтиповішими матеріальними проявами незаконного втручання є: електронні записи про входи до системи та факти авторизації користувачів (61,8%), журнали подій і лог-файли (57,6%), зміни в базах даних автоматизованої системи (48,9%), сліди видалення, блокування, модифікації чи копіювання інформації (43,2%), використання чужих облікових записів чи засобів автентифікації (39,5%), а також зміни облікових даних або параметрів доступу (34,7%). У 29,4% випадків виявляються також додаткові технічні ознаки, пов’язані зі зміною конфігурації програмного забезпечення, нехарактерною мережевою активністю чи появою сторонніх файлів і програмних компонентів. У разі поєднання незаконного втручання з корупційними проявами структура слідової картини розширюється за рахунок документів, що підтверджують домовленості або одержання неправомірної вигоди (31,8%), грошових коштів (21,6%), а також слідів спеціальних хімічних речовин на предметах чи руках причетних осіб (18,3%). Важливу роль відіграють й ідеальні сліди, носіями яких найчастіше виступають працівники органів та установ системи правосуддя, зокрема, працівники, які безпосередньо або опосередковано спостерігали використання автоматизованих систем (28,7%), особи, які виявили ознаки незаконного втручання чи повідомили про них (24,5%), а також особи, які

здійснювали технічне обслуговування або налаштування програмного забезпечення (15,2%).

3. Під час розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя підлягають встановленню не лише загальні обставини, передбачені кримінальним процесуальним законом, а й спеціальні відомості, пов'язані з технічними параметрами функціонування автоматизованої системи, режимом і способом доступу до неї, особливостями інформаційного середовища, слідами несанкціонованого впливу, характером змін у програмному забезпеченні або даних, а також із порушенням установленого порядку обробки, передавання, зберігання чи використання інформації, а саме: подія кримінального правопорушення, включаючи час, місце, спосіб, обстановку й конкретну форму втручання; характеристики автоматизованої системи як об'єкта протиправного впливу; дані про особу правопорушника, форму вини, мотив, мету, наявність спеціальних знань чи відповідного доступу; наслідки незаконного втручання у вигляді порушення функціонування системи, блокування, модифікації, знищення, копіювання або витоку інформації та заподіяної шкоди; обставини, що впливають на ступінь тяжкості кримінального правопорушення й індивідуалізацію відповідальності; відомості про використані технічні пристрої, програмні засоби, облікові записи, серверне обладнання чи інші засоби як знаряддя вчинення кримінального правопорушення; а також підстави для застосування до юридичних осіб заходів кримінально-правового характеру. Встановлення таких обставин має здійснюватися комплексно, із поєднанням кримінального процесуального, криміналістичного та інформаційно-технічного підходів, що забезпечує ефективність досудового розслідування.

4. Повноцінному здійсненню взаємодії під час розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя перешкоджають: низький рівень матеріально-технічного забезпечення діяльності, пов'язаної з фіксацією, збереженням та дослідженням інформації (46%); відсутність зацікавленості або належної ініціативності з боку

окремих суб'єктів, які повинні бути залучені до взаємодії (32%); нерозуміння окремими учасниками змісту, завдань і меж взаємодії (17%); недосконаліть нормативного регулювання міжвідомчої та внутрішньо-системної взаємодії (15%). Наведені дані свідчать, що на практиці проблеми взаємодії мають не лише нормативний, а й організаційний, кадровий та ресурсний характер, що істотно ускладнює отримання технічної інформації, забезпечення її збереження та подальше використання у доказуванні. У зв'язку з цим обґрунтовано необхідність прийняття спільного міжвідомчого нормативно-правового акта – *Інструкції про організацію взаємодії слідчих з правоохоронними органами, органами та установами системи правосуддя, а також іншими суб'єктами під час розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя*. Запропоновано, щоб її структура охоплювала загальні положення, визначення суб'єктів взаємодії та їх повноважень, форми і способи взаємодії, алгоритми спільних дій на окремих стадіях кримінального провадження, порядок фіксації результатів взаємодії, правила забезпечення конфіденційності та захисту інформації, а також механізми контролю за дотриманням вимог такої Інструкції й відповідальність за їх порушення.

5. Доведено, що огляд у кримінальних провадженнях про незаконне втручання в роботу автоматизованих систем в органах та установах системи правосуддя є не просто початковою слідчою дією, а одним із основних способів своєчасного виявлення та збереження слідів кримінального правопорушення. Саме на цьому етапі формується первинне уявлення про механізм втручання, обсяг змін в інформаційному середовищі, характер використаних технічних засобів і коло можливих причетних осіб. У зв'язку з цим розроблено науково-практичні рекомендації для слідчих, прокурорів та працівників оперативних підрозділів щодо підготовки й проведення огляду місця події, комп'ютерної техніки (78%), серверного обладнання (54%), автоматизованих робочих місць (71%), цифрових носіїв (67%), мережевої інфраструктури (49%) та системних журналів (74%). Запропоновано послідовність дій, яка дає змогу не лише

зафіксувати зовнішню обстановку, а й зберегти динамічні електронні дані, не допустити їх пошкодження або зміни, правильно визначити об’єкти, що мають доказове значення, та забезпечити їх придатність для подальшого експертного дослідження.

6. Встановлено, що обшук у провадженнях зазначеної категорії має пошуково-тактичний характер, оскільки спрямований на виявлення не лише очевидних матеріальних об’єктів, а насамперед прихованих цифрових носіїв, засобів доступу, технічних пристроїв, чорнових записів, службових документів і предметів, які відображають підготовку, реалізацію або приховування незаконного втручання. На цій підставі розроблено тактичні рекомендації з урахуванням ризику швидкого знищення або дистанційного видалення інформації (61%), необхідності забезпечення раптовості (56%), одночасного контролю за поведінкою присутніх осіб (48%) та своєчасного виявлення об’єктів, що зовні можуть не сприйматися як джерела доказів (52%). Запропоновано практичні підходи до локалізації цифрового середовища обшуку, блокування несанкціонованих дій із пристроями, виявлення засобів автентифікації, правильного вилучення та пакування електронних носіїв, а також до залучення спеціаліста для розпізнавання технічно значущих об’єктів і мінімізації ризику втрати електронних доказів.

7. Обґрунтовано, що допит у кримінальних провадженнях про незаконне втручання в роботу автоматизованих систем в органах та установах системи правосуддя пов’язаний із необхідністю з’ясування не лише юридично значущих фактів, а й технічних, службових та поведінкових аспектів події. Ефективність такої слідчої дії залежить від здатності слідчого поєднати відомості про функціонування автоматизованої системи, порядок доступу до неї, технічні параметри втручання та службовий статус допитуваної особи. У зв’язку з цим розроблено науково-практичні рекомендації щодо тактики допиту підозрюваних (36%), свідків із числа працівників органів та установ системи правосуддя (64%), системних адміністраторів і технічних спеціалістів (42%) та інших осіб, які можуть володіти інформацією про обставини кримінального правопорушення.

Запропоновано орієнтовні блоки запитань для різних категорій допитуваних, визначено типові тактичні ситуації допиту та окреслено підходи до подолання заперечення причетності, посилань на технічну необізнаність, перекладання відповідальності на інших осіб або пояснення втручання випадковими збоями в роботі системи.

8. Проаналізовано особливості використання спеціальних знань під час розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя та розроблено практичні рекомендації щодо залучення спеціалістів, вибору виду судової експертизи та формулювання запитань експерту. Встановлено, що у провадженнях цієї категорії найбільше значення мають комп'ютерно-технічна експертиза (76%), експертиза телекомунікаційних систем і засобів (51%), експертиза у сфері технічного захисту інформації (43%), почеркознавча й технічна експертиза документів (34%), а в разі поєднання незаконного втручання з корупційними проявами – також економічна (22%), фоноскопічна (17%) та інші види експертиз залежно від слідчої ситуації. Обґрунтовано, що застосування спеціальних знань дає змогу встановити спосіб доступу до автоматизованої системи, факт і характер змін даних, наявність слідів використання конкретного пристрою чи облікового запису, механізм видалення або модифікації інформації, а також зв'язок між технічними діями і конкретною особою. У зв'язку з цим сформульовано орієнтовний перелік питань, які доцільно ставити експерту, зокрема щодо факту втручання в систему, способу його реалізації, часу внесення змін, використаних технічних засобів, можливості відновлення видаленої інформації, наявності слідів стороннього програмного впливу та ідентифікації користувача, який виконував відповідні дії.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Абламський С. Є., Юхно О. О., Лук'яненко Ю. В. Взаємодія слідчого з іншими органами і підрозділами при розкритті та розслідуванні кримінальних правопорушень: навч. посіб. Харків, 2017 152 с.

2. Аленін Ю. П. Початок досудового розслідування за КПК 2012 року. *Юридичний часопис Національної академії внутрішніх справ*. № 1. 2013. С. 198–203.

3. Англійсько-український словник термінів і понять з державного управління / Уклали: Г. Райт та ін.; Пер. В. Івашко. Київ : Основи, 1996. 128 с

4. Антикорупційний менеджмент: підручник. Київ : Нац. акад. внутр. справ, 2020. 680 с.

5. Антонюк Ю. В., Удовенко Ж. В. Поняття та суть взаємодії слідчого з працівниками експертної служби. *Теорія і практика судової експертизи*: зб. матеріалів кругл. ст. Київ: Нац. акад. внутр. справ, 2016. С. 107–108.

6. Антощук А.О., Степанова Г.М., Замула Б.А. Тактичні особливості проведення слідчих (розшукових) дій при розслідуванні незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя. *Наукові інновації та передові технології*. № 4 (56). 2026. С. 2905–2916. https://doi.org/10.52058/2786-5274-2026-4(56)-2905-2916

7. Балонь А. Б. Методика розслідування злочинів, вчинених з використанням службовою особою своїх повноважень: автореф. дис. …канд. юрид. наук: 12.00.09. Київ, 2015. 20 с.

8. Барназюк О. О. Поняття та особливості електронного судочинства в Україні. URL: http://pravoisuspilstvo.org.ua/archive/2019/3_2019/part_2/5.pdf

9. Баулін О. В. Обставини, що підлягають встановленню під час досудового розслідування терористичного акту. *Науковий часопис Національної академії прокуратури України.* 2015. № 4. С. 28–37.

10. Білоус В. В. Інформатизація судочинства як гарантія конституційного права на доступ до правосуддя. *Конституція України – основа розбудови*

правової демократичної соціальної держави та формування правової системи : матеріали Всеукр. наук.-практ. конф., Харків, 2011. С. 289–295.

11. Бринцев О. В. «Електронний суд» в Україні. Досвід та перспективи: монографія. Харків: Право, 2016. 72 с.

12. Бруссо К. М. Розслідування корупційних кримінальних правопорушень, які вчиняються в сфері житлового будівництва: дис. …канд. юрид. наук: 12.00.09. Маріуполь. 2021. 242 с.

13. Вакулік О. А. Реформування кримінального процесуального законодавства в частині регламентації початку досудового розслідування. *Науковий вісник Національної академії внутрішніх справ*. 2013. № 4 (89). С. 160–167.

14. Вапнярчук В. В. Характеристика обставин предмету доказування, які підтверджують наявність головного факту. *Науковий вісник Ужгородського національного університету*. Серія Право, 2013. Вип. 22. Частина ІІ. Том 3. С. 93–97.

15. Велика українська юридична енциклопедія : у 20 т. Харків : Право, 2016 Т. 20 Криміналістика, судова експертиза, юридична психологія / редкол. В. Ю. Шепітько (голова) та ін.; Нац. акад. прав. Наук України; Інт держави і права ім. В. М. Корецького НАН України; Нац. юрид. ун.т ім. Ярослава Мудрого, 2018. 952 с.

16. Великий тлумачний словник української мови / уклад. і голов. ред. В. Т. Бусел. Київ, Ірпінь: Перун, 2009. 1440 с.

17. Вирок Апеляційного суду Черкаської області від 29 серп. 2018 р. Провадження № 11-кп/793/589/18. Справа № 696/1199/17. URL: http://reyestr.court.gov.ua/Review/76124521.

18. Вирок Святошинського районного суду м. Києва від 10 серп. 2022 р. № 759/9998/19. URL: https://reyestr.court.gov.ua/Review/105689723

19. Вирок Бабушкінського районного суду м. Дніпра від 01 берез. 2024 р. Справа № 932/5166/21. URL: https://reyestr.court.gov.ua/Review/117364050

20. Волобуєв А. Ф. Проблеми методики розслідування розкрадань майна в сфері підприємництва. Харків : Ун-т внутр. справ, 2000. 336 с.

21. Воробей О. В. Особливості проведення допиту у кримінальних провадженнях щодо діяльності конвертаційних центрів. *Юридичний науковий електронний журнал.* 2017. № 1. С. 159–162.

22. Галаган В. І. Проблеми вдосконалення кримінально-процесуальної діяльності органів внутрішніх справ України: монографія. Київ: Нац. акад. внутр. справ України, 2002. 300 с.

23. Грохольський В., Грохольська Л. Удосконалення нормативно-правового забезпечення управління органами внутрішніх справ України. *Вісник Академії управління МВС*. 2007. № 2–3. С. 12–20.

24. Дарбінян С. Цифрове судочинство. URL: https://rublacklist.net/13307/

25. Дикий О. В. Житлова нерухомість як предмет злочинів проти власності. Серія Право. Випуск 27. Том 3. *Науковий вісник Ужгородського національного університету*, 2014. С. 26–29.

26. Діденко В. Л. Використання спеціальних знань при розслідуванні кримінальних правопорушень у бюджетній сфері: дис. …канд. юрид. наук: 12.00.09. Дніпро, 2024. 236 с.

27. Дуда А. В. Особа злочинця як елемент криміналістичної характеристики корупційних злочинів. *Реалізація державної антикорупційної політики в міжнародному вимірі*: матеріали ІІІ Міжнар. наук.-практ. конф. (Київ, 7 груд. 2018 р.): у 2 ч. Київ: Нац. акад. внутр. справ, Ч. 2. 2018. С. 84–87.

28. Експертиза телекомунікаційних систем (обладнання) та засобів. URL: https://kndise.gov.ua/expertise/telecommunication-examination

29. Експертизи у судовій практиці: підручник / за заг. ред. В. Г. Гончаренка. Київ: Юрінком Інтер, 2004. 388 с.

30. Експертизи у судочинстві України. URL: https://pidru4niki.com/74873/pravo/ekspertizi_u_sudochinstvi_ukrayini.

31. Електронне судочинство: плюси і мінуси для адвоката URL: https://radako.com.ua/news/elektronne-sudochinstvo-plyusi-i-minusi-dlya-advokata

32. Жалдак І. А. Актуальні питання тактики одночасного допиту двох чи більше вже допитаних осіб. *Науковий вісник публічного та приватного п*рава. 2019. Вип. 1. С. 304–311.

33. Зав'ялов С. М. Спосіб вчинення злочину: окремі проблеми вивчення та використання у боротьбі зі злочинністю: автореф. дис. … канд. юрид. наук: 12.00.09. Київ, 2005. 21 с.

34. Задорожний О. С. Криміналістична характеристика ухилень від сплати податків, зборів, інших обов'язкових платежів та основні положення їх розслідування : дис. … канд. юрид. наук : 12.00.09. Харків, 2005. 212 с.

35. Заплотинський Б. А. Електронне судочинство. Конспект лекцій. Кафедра менеджменту та інформаційних технологій КІІВтаП НУ «ОЮА», 2018. 84 с.

36. Зарубей В. В., Моісеєв М. Г. Тактика проведення огляду під час розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя. *Право.UA*. № 1. 2026. С. 274–278. DOI: https://doi.org/10.71404/LAW.UA.2026.1.36

37. Затенацький Д. В. Ідеальні сліди в криміналістиці (техніко-криміналістичні та тактичні прийоми їх актуалізації): автореф. дис. … канд. юрид. наук: 12.00.09. Харків. 2008. 20 с.

38. Звіт Офісу Генерального прокурора про зареєстровані кримінальні правопорушення та результати їх досудового розслідування за 2017–2023 рр. *Офіс Генерального прокурора*. URL**:** https://www.gp.gov.ua/ua/posts/2013-2024-roki-pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya

39. Іванов О. В. Адміністративно-правовий статус Національного агентства з питань запобігання корупції : дис. … канд. юрид. наук : 12.00.07. Київ, 2019. 304 с.

40. Іванов О. В. Криміналістична характеристика суб'єкта незаконного збагачення. *Реалізація державної антикорупційної політики в міжнародному*

вимірі: матеріали Міжнарод. наук.-практ. конф. (Київ, 9 груд. 2016 р.). Київ: Нац. акад. внутр. справ, 2016. С. 200–203.

41. Іващенко О. В. Підстави і процесуальний порядок виклику учасників кримінального провадження для участі у слідчих(розшукових) діях. *Часопис Національного університету «Острозька академія»*. Серія : Право. Острог, 2013. № 1 (7). URL: http://lj.oa.edu.ua/articles/2013/n1/13iovsrd.pdf.

42. Іноземцева К. О. Організаційно-правові засади кадрового забезпечення судової системи України: дис. …докт. філософ. 081. Суми. 2021. 248 с.

43. Іноземцева К. О. Сучасні проблеми кадрового забезпечення судової системи України. *Приватне та публічне право*. 2020. № 1. С. 71–76.

44. Карпушин С. В. Проведення слідчих (розшукових) дій: дис. … канд. юрид. наук: 12.00.09. Київ, 2016. 210 с.

45. Кирилюк Р. І. Кримінальна відповідальність за незаконне втручання в роботу автоматизованої системи документообігу суду: проблеми теорії та практики. URL: https://ivpz.kh.ua/wpcontent/uploads/2019/02/zbirnik_konf_2013.pdf

46. Клюєв О. М. Проблеми розмежування понять «координація» і «взаємодія» в управлінській науці та практичній діяльності органів внутрішніх справ. *Право і Безпека*. 2011. № 3. С. 76–80.

47. Козак В.А. Кримінальна відповідальність за незаконне втручання в роботу автоматизованої системи документообігу суду: аналіз основного складу злочину. *Проблеми законності*. 2013. С. 151–158

48. Козяр Р. Я. Класифікація видів втручання у професійну діяльність судді: методологічний аспект. Наукові *записки Львівського університету бізнесу і права*. Серія економічна. Юридична серія. Випуск 31. 2021. С. 77–86.

49. Колодій А. М. Принципи права: генеза, поняття, класифікація та реалізація. *Альманах права*. 2012. Вип. 3. С. 42–46.

50. Коновалова В. О. Допит: тактика і психологія: навч. посіб. Харків: Консум, 1999. 157 с.

51. Конспект лекцій з дисципліни «Юридична психологія» / укл. С. Г. Головко. Київ, 2016. URL: http://divovo.in.ua/konspekt-lekcij-z-disciplini-yuridichna-psihologiya.html?page=6.

52. Конституція України : Основний Закон України від 28 черв. 1996 р. № 254к/96-ВР. *Верховна рада України*. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

53. Концепція розвитку електронного урядування в Україні: розпорядження Кабінету Міністрів України від 20 вересня 2017 р. номер 649-р. URL: http://zakon2.rada.gov.ua/laws/show/649-2017-%D1%80

54. Корнієнко В. В. Криміналістична характеристика особи злочинця та злочинних груп у сфері банківської діяльності. *Право і безпека*. 2015. № 2 (57). С. 98–102.

55. Коршенко В. А. Сучасні проблеми судової телекомунікаційної експертизи. *Актуальні проблеми сучасної науки в дослідженнях молодих учених*. Харків, 2017. С. 92–97.

56. Косович В. М. Нормативне закріплення принципів права як чинник досконалості нормативно-правових актів. *Науковий інформаційний вісник*. 2013. № 7. С. 40–50.

57. Криміналістика : підручник. Вид. 4-е перероб. і доп. / за ред. проф. В. Ю. Шепітька. Харків : Право, 2008. 464 с.

58. Криміналістика. Академічний курс: підручник / Т. В. Варфоломеєв, В. Г. Гончаренко, В. І. Бояров, С. В. Гончаренко, В. О. Попелюшко. Київ: ЮрІнком Інтер, 2011. 495 с.

59. Криміналістика: навч. посіб. / Р. І. Благута, Р. І. Сибірна, В. М. Бараняк та ін.; за заг. ред. Є. В. Пряхіна. Київ: Атіка, 2012. 496 с.

60. Криміналістика: підручник / В. В. Пясковський, Ю. М. Чорноус, А. В. Іщенко, О. О. Алєксєєв та ін. Київ: «Центр учбової літератури», 2015. 544 с.

61. Криміналістика: підручник / В. Ю. Шепітько, В. О. Коновалова, В. А. Журавель та ін.; за ред. проф. В. Ю. Шепітька. 4-е вид., перероб. і доп. Харків: Право, 2008. 462 с.

62. Криміналістика: підручник / Р. І. Благута, О. І. Герасимів, О. М. Дуфенюк та ін.; за заг. ред. Є. В. Пряхіна. 3 вид., переробл. та допов. Львів: ЛьвДУВС, 2016. 948 с.

63. Криміналістика: підручник: у 2 т. Т. 2. / В. Ю. Шепітько, В. А. Журавель, В. О. Коновалова та ін.; за ред. В.Ю. Шепітька. Харків: Право, 2019. 328 с.

64. Криміналістична тактика і методика розслідування окремих видів злочинів: навч. посіб. / В. П. Бахін, В. К. Весельський, В. С. Кузьмічов та ін.; за ред. О. М. Джужі. Київ.: Нац. акад. внутр. справ, 2010. 524 с.

65. Криміналістичне забезпечення розслідування кримінальних правопорушень щодо підроблення документів, які подаються для проведення державної реєстрації юридичної особи та фізичних осіб-підприємців: метод. реком. Саковський А. А., Мировська А. В., Нечеснюк М. В. та ін. Київ : Нац. акад. внутр. справ, 2023. 57 с.

66. Кримінальне право (Особлива частина) : підруч. / за ред. О. О. Дудорова, Є. О. Письменського. Т. 2. Луганськ : Елтон-2, 2012. 780 с.

67. Кримінальне право України. Загальна частина / за редакцією професорів М. І. Бажанова, В. В. Сташиса, В. Я. Тація. Київ : Юрінком Інтер. Право, 2001. 236 с.

68. Кримінальний кодекс України: Закон України від 5 квіт. 2001 р. № 2341-III. *Верховна рада України*. URL: http://zakon2.rada.gov.ua/laws/show/2341-14/

69. Кримінальний процес: підручник / Ю. М. Грошевий, В. Я. Тацій та ін.; за ред. В. Я. Тація, Ю. М. Грошевого, О. В. Капліної, О. Г. Шило. Харків: Право, 2013. 824 с.

70. Кримінальний процес України : підручник / авт. кол.: М. М. Михеєнко, В. Т. Нор, В. П. Шибіко. Київ, 1999. 639 с.

71. Кримінальний процес: альбом схем (загальна та особливі частини) : навч. посіб. / Л. Д. Удалова, В. В. Рожнова, Д. П. Письменний та ін. 2-ге вид., випр. та доповн. Київ : Центр учб. літ., 2016. 406 с.

72. Кримінальний процесуальний кодекс України : Закон України від 13 квіт. 2012 р. № 4651-VI. *Верховна рада України*. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text

73. Кузьмічов В. С. Слідча діяльність: характеристика та напрями удосконалення: монограф. Київ : Нічлава, 2005. 446 с.

74. Кузьмічов В. С., Прокопенко Г. І. Криміналістика : навч. посіб. / за заг. ред. В. Г. Гончаренка та Є. М. Мойсеєва. Київ: Юрінком Інтер, 2001. 368 с.

75. Кухарчук А. В., Ткаченко О. Р. Особливості проведення обшуку в умовах воєнного стану. *Юридичний науковий електронний журнал.* № 4/2023. С. 578–580. URL: http://www.lsej.org.ua/4_2023/138.pdf

76. Кушакова-Костицька Н. В. Розвиток електронного судочинства в Україні: проблемні питання. *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького.* 2013. номер 7. С. 139-145

77. Лапкін А. В. Судове право України : навч. посібник у схемах. Харків : Право, 2016. 148 с.

78. Лащук Є. Ф. Предмет злочину в кримінальному праві України : дис. канд. юрид. наук : 12.00.08. Київ, 2005. 262 с.

79. Логінова Н. І. Упровадження електронного правосуддя в систему судочинства. URL: www.apdp.in.ua/v72/61.pdf

80. Лойф О. Використання спеціальних знань у розкритті та розслідуванні злочинів у сфері наркобізнесу. *Підприємництво, господарство і право*. 2008. № 6. С. 151–153.

81. Мазур Л. А., Морозова Я. О. Напрямки взаємодії підрозділів карного розшуку з різними суб'єктами протидії злочинам. *Право і безпека*. 2012. № 5 (47). С. 181–185.

82. Марченко А. Б. Слідчі помилки та шляхи їх подолання : автореф. дис. ... канд. юрид. наук: 12.00.09. Київ, 2006. 22 с.

83. Мірошниченко С. С. Предмет державного експертного контролю як обов'язкова ознака кримінального правопорушення. *Науковий вісник публічного та приватного права*. № 2. 2020. С. 208–214

84. Мозоль С. А. Кримінологічна безпека в Україні: феномен та наукові засади забезпечення: дис. …докт. юрид. наук: 12.00.08. Харків. 2018. 481 с.

85. Моісеєв М. Г. Електронне судочинство в умовах воєнного стану. *Кримінальне судочинство: сучасний стан та перспективи розвитку* : міжвідом. наук.-практ. конф. (Київ, 28 квіт. 2023 р.). Київ : Нац. акад. внутр. справ, 2023. С. 174–177. URL : https://elar.navs.edu.ua/server/api/core/bitstreams/72b10f52-7185-4e4c-b36f-943b408c5f7b/content

86. Моісеєв М. Г. Можливості застосування міжнародного досвіду щодо удосконалення електронного судочинства в Україні при запровадженні воєнного стану. *Кримінальне процесуальне право на сучасному етапі розвитку України* : матеріали круглого столу, присвяч. 40-річчю кафедри кримінального процесу (Київ, 27 жовт. 2023 р.). Київ : Нац. акад. внутр. справ, 2023. С. 282–286. URL: https://elar.navs.edu.ua/server/api/core/bitstreams/ece9dd4d-8e55-4ed1-bfae-ebb66a98894e/content#page=283&zoom=100,72,481

87. Моісеєв М. Г. Основні засади електронного судочинства в праві Європейського союзу. *Кримінальне судочинство: права людини під час дії надзвичайного або воєнного стану* : міжнар. наук.-практ. конф. (Київ, 18 листоп. 2022 р.). Київ : Нац. акад. внутр. справ, 2022. С. 215–218. URL: https://elar.navs.edu.ua/server/api/core/bitstreams/0c56ce37-2df4-48cb-b8d8-1d5fe007a70a/content

88. Моісеєв М. Г. Особа правопорушника як елемент криміналістичної характеристики незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя. *Кримінологія і війна: екзистенційні виклики для України* : міжвідом. наук.-практ. круглого столу (Київ, 6 листоп. 2025 р.). Київ : Нац. акад. внутр. справ, 2025. С. 272–274.

89. Моісеєв М. Г. Криміналістична характеристика незаконного втручання в роботу автоматизованих систем в органах правосуддя. *Юридичний вісник*. № 3, 2023. С. 265–277. DOI: https://doi.org/10.32782/yuv.v3.2023.33

90. Моісеєв М. Г. Обшук під час розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя.

Наукові інновації та передові технології. № 4(56) 2026. С. 3331–3343. DOI: https://doi.org/10.52058/2786-5274-2026-4(56)-3331-3343

91. Моісеєв М. Г. Основні засади електронного судочинства у праві Європейського союзу та незалежній Україні: порівняльний аспект. *Публічне право*. 2022. № 4 (48). С. 167–174. DOI: https://doi.org/10.32782/2306-9082/2022-48-19

92. Моісеєв М. Г., Зарубей В. В. Криміналістична характеристика особи злочинця, що незаконно втручається в роботу автоматизованих систем в органах та установах системи правосуддя. *Knowledge, Education, Law, Management*. 2024 № 8 (68). С. 122–132. DOI: https://doi.org/10.51647/kelm.2024.8.17

93. Моїсєєв О. М. Висновок експерта в контексті взаємодії процесуальних суб'єктів : монографія. Донецьк : Норд-Прес-Дон НУДОН НДІСЕ МЮ України, 2007. 187 с.

94. Морквін Д. А., Гох І. М. Основні засади та принципи діяльності Національної гвардії України. *Юридичний науковий електронний журнал*. № 10/2023. URL: http://lsej.org.ua/10_2023/5.pdf

95. Музика А. А., Лащук Є. В. Предмет злочину: теоретичні основи пізнання: монографія. Київ: Паливода А. В., 2011. 191 с.

96. Мусієнко О. Л., Григоренко А. О. Особливості криміналістичної характеристики злочинів, вчинених службовими особами. *Прикарпатський юридичний вісник*. Випуск 3 (24), 2018. С. 187–191.

97. Науково-практичний коментар Кримінального кодексу України / Д. С. Азаров, В. К. Грищук, А. В. Савченко та ін.; за заг. ред. О. М. Джужі, А. В. Савченка, В. В. Чернєя. 2-ге вид., перероб. і допов. Київ: Юрінком Інтер, 2018. 1104 с.

98. Науково-практичний коментар Кримінального кодексу України / за ред. М. І. Мельника, М. І. Хавронюка. Київ: Юрид. думка, 2012. 1316 с.

99. Науково-практичний коментар Кримінального процесуального кодексу України / За редакцією С. В. Ківалова та С. І. Кравченко. Одеса: Фенікс. 2020. 924 с.

100. Никоненко М.Я., Степанова Г.М. Доказування у кримінальних провадженнях в умовах воєнного стану. *Наукові перспективи*. № 12(66). 2025. С. 1778–1790. DOI: https://doi.org/10.52058/2708-7530-2025-12(66)

101. Огляд місця події при розслідуванні окремих видів злочинів: наук.-практ. посібник / за ред. Н. І. Клименко. Київ: Юрінком Інтер, 2005. 216 с.

102. Особливості кримінального провадження у період воєнного стану. URL: https://syrota.com.ua/blog/osoblyvosti-kryminalnoho-provadzhennia-u-period-voiennoho-stanu/

103. Особливості розслідування прийняття пропозиції, обіцянки або одержання неправомірної вигоди службовою особою: метод. рек. / Чернявський С. С., Вакуленко О. Ф., Толочко О. М. та ін. Київ: Нац. акад. внутр. справ, 2014. 92 с.

104. Панов М. М. Кримінальна відповідальність за незаконні дії з документами на переказ; платіжними картками та іншими засобами доступу до банківських рахунків : монографія / наук. ред. В. І. Борисов. Харків : Право, 2009. 184 с.

105. Пашинська І. В. Теоретико-методологічні основи розслідування організованої злочинності у сфері господарської діяльності: дис. …докт. філос. 081 – Право. Харків. 2023. 296 с.

106. Податковий кодекс України: Закон України від 02 груд. 2010 р. № 2755-VI. *Верховна рада України*. URL: https://zakon.rada.gov.ua/laws/show/2755-17#Text

107. Положення про автоматизовану систему документообігу суду: затверджено рішенням Ради суддів України 11 лист. 2024 р. № 39. URL: https://court.gov.ua/sudova-vlada/969076/polozhenniapasds/

108. Положення про автоматизовану систему розподілу справ: Рішення Ради суддів України від 04 лют. 2015 р. № 25. *Верховна рада України*. URL: https://zakon.rada.gov.ua/rada/show/v0025414-15 #Текст

109. Положення про Державну судову адміністрацію України: Рішення Ради суддів України від 22 жовт. 2010 № 2. URL: https://zakon.rada.gov.ua/rada/show/vr012414-10#n9

110. Пономаренко В. А. Нове спрощене провадження: ера електронного правосуддя настала? *Арбітражний та цивільний процес*. 2013. № 3. С. 25–30. URL: https://center-bereg.ru/h244.html

111. Попелюшко В. О. Предмет доказування в кримінальному процесі (процесуально-правові та кримінально-правові аспекти). Острог : Нац. ун-т «Острозька академія», 2001. 231 с.

112. Постанова Верховного Суду від 29 січ. 2019 р., у справі № 466/896/17. URL: https://verdictum.ligazakon.net/document/79601140.

113. Прийма С. В. Поняття принципу в аспекті співвідношення з суміжними категоріями. *Державне будівництво та місцеве самоврядування*. Вип. 28. 2014. С. 46–55.

114. Приходько Ю. П. Техніко-криміналістичне забезпечення розслідування злочинів, пов'язаних із кримінальними вибухами: дис. … канд. юрид. наук. Київ. 2016. 300 с.

115. Про валюту і валютні операції: Закон України від 21 черв. 2018 р. № 2473-VIII. *Верховна рада України*. URL: https://zakon.rada.gov.ua/laws/show/2473-19/print

116. Про Вищу раду правосуддя: Закон України від 21 груд. 2016 р. № 1798-VIII. *Верховна рада України*. URL: https://zakon.rada.gov.ua/laws/show/1798-19/ed20210805/print

117. Про внесення змін до деяких законодавчих актів України щодо запровадження автоматизованої системи документообігу в адміністративних судах: Закон України від 5 черв. 2009 р. *Верховна рада України*. URL: https://zakon.rada.gov.ua/laws/ show/1475-17#

118. Про державне регулювання видобутку, виробництва і використання дорогоцінних металів і дорогоцінного каміння та контроль за операціями з ними:

Закон України від 18 лист. 1997 р. № 637/97-ВР. *Верховна рада України*. URL: https://zakon.rada.gov.ua/laws/show/637/97-%D0%B2%D1%80/print

119. Про доступ до судових рішень: Закон України від 22 груд. 2005 р. № 3262-IV. *Верховна рада України*. URL: https://zakon.rada.gov.ua/laws/show/3262-15/print

120. Про електронний цифровий підпис: Закон України від 22 трав. 2003 р. № 852-IV. *Верховна рада України*. URL: https://zakon.rada.gov.ua/laws/show/852-15#Text

121. Про електронні документи та електронний документообіг: Закон України від 22 трав. 2003 р. № 851-IV. *Верховна рада України*. URL: https://zakon.rada.gov.ua/laws/show/851-15/print

122. Про електронні комунікації: Закон України від 16 груд. 2020 р. № 1089-IX. *Верховна рада України*. URL: https://zakon.rada.gov.ua/laws/show/1089-20

123. Про запобігання корупції: Закон України від 14 жовт. 2014 р. № 1700-VII. *Верховна рада України*. URL: https://zakon2.rada.gov.ua/laws/show/1700-18.

124. Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень: наказ Міністерства юстиції України від 08 жовт. 1998 р. № 53/5. *Верховна рада України*. URL: https://zakon.rada.gov.ua/laws/show/z0705-98#Text

125. Про затвердження Національного положення (стандарту) бухгалтерського обліку 1 «Загальні вимоги до фінансової звітності» : наказ Міністерства фінансів України від 07 лют. 2013 р. № 73. *Верховна рада України*. URL: https://zakon.rada.gov.ua/laws/show/z0336-13#Text

126. Про затвердження Положення про Єдиний реєстр досудових розслідувань, порядок його формування та ведення: Наказ Офісу Генерального прокурора від 30 лип. 2020 р. № 298. *Верховна рада України*. URL: https://zakon.rada.gov.ua/laws/show/v0298905-20#Text

127. Про затвердження Положення про Національну поліцію : Постанова Кабінету Міністрів України від 28 жовт. 2015 р. № 877. *Верховна рада України*. URL: https://zakon.rada.gov.ua/laws/show/877-2015-%D0%BF#Text.

128. Про затвердження Положення про порядок функціонування окремих підсистем Єдиної судової інформаційно-телекомунікаційної системи: Рішення Вищої Ради Правосуддя від 17 серп. 2021 р. № 1845/0/15-21. *Верховна рада України*. URL: https://zakon.rada.gov.ua/rada/show/v1845910-21#Text

129. Про затвердження Порядку ведення Єдиного державного реєстру судових рішень: Рішення Вищої ради правосуддя від 19 квіт. 2018 р. № 1200/0/15-18. *Верховна рада України*. URL: https://zakon.rada.gov.ua/rada/show/v1200910-18#Text

130. Про електронну ідентифікацію та електронні довірчі послуги: Закон України від 5 жовт. 2017 р. № 2155-VIII. *Верховна рада України*. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text

131. Про інформацію: Закон України від 02 жовт. 1992 р. № 2657-XII. *Верховна рада України*. URL: https://zakon.rada.gov.ua/laws/show/2657-12

132. Про науково-технічну інформацію: Закон України від 25 черв. 1993 р. № 3322-XII. *Верховна рада України*. URL: https://zakon.rada.gov.ua/laws/show/3322-12

133. Про оперативно-розшукову діяльність : Закон України від 18 лют. 1992 р. № 2135-XII. *Верховна рада України*. URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text

134. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 9 січня 2007 р. № 537-V. *Верховна рада України*. URL: https://zakon.rada.gov.ua/laws/show/537-16#Text

135. Про прокуратуру : Закон України від 14 жовт. 2014 р. № 1697-VII. *Верховна рада України*. URL : http://zakon2.rada.gov.ua/ laws/show/1697-18.

136. Про Службу безпеки України : Закон України від 25 берез. 1992 р. № 2229-XII. *Верховна рада України*. URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text

137. Про судову експертизу: Закон України від 25 лют. 1994 р. № 4038-XII. *Верховна рада України*. URL: https://zakon.rada.gov.ua/laws/show/4038-12#Text

138. Про судоустрій і статус суддів: Закон України від 02 черв. 2016 р. № 1402-VIII. *Верховна рада України*. URL: https://zakon.rada.gov.ua/laws/show/1402-19#Text

139. Протидія кримінальним та іншим правопорушенням у сфері проведення операцій з об'єктами нерухомого майна: метод. рекомендації; кол. авт. Дніпро: ДДУВС, 2022, 40 с.

140. Пчеліна О. В. Особа злочинця як елемент криміналістичної характеристики злочинів у сфері службової діяльності. *Вісник Національної академії правових наук України*. 2017. № 2 (89). С. 145–156.

141. Пчеліна О. В. Теоретичні засади формування та реалізації методики розслідування злочинів у сфері службової діяльності: автореф. дис. ... докт. юрид. наук: 12.00.09. Харків, 2017. 40 с.

142. Решетняк В. І. Електронне правосуддя у цивільному процесі Сінгапуру. *Юридичний журнал*. 2012. Номер 2 (83). С. 75–80.

143. Рєзнік О. М., Андрійченко Н. С. Специфіка адміністративно-правового статусу СБУ як суб'єкта захисту фінансової системи держави. *Часопис Київського університету права*. 2016. № 3. С. 156–160.

144. Рішення Конституційного Суду України у справі за конституційним поданням Верховного Суду України щодо відповідності Конституції України (конституційності) положень статті 69 Кримінального кодексу України (справа про призначення судом більш м'якого покарання) : справа № 1-33/2004 від 02 лист. 2004 р. *Верховна рада України*. URL: https://zakon.rada.gov.ua/laws/show/v015p710-04#Text

145. Розслідування злочинів, учинених з використанням шкідливих програмних чи технічних засобів: метод. реком. / О. С. Тарасенко, О. Ф. Вакуленко, О. М. Стрільців та ін. Київ, 2016. 55 с.

146. Розслідування незаконного збагачення: метод. рек. / О. М. Стрільців, С. С. Чернявський, В. І. Василинчук та ін. Київ: Нац. акад. внутр.справ, 2018. 86 с.

147. Розслідування прийняття пропозиції, обіцянки або одержання неправомірної вигоди службовою особою: метод. рек. Чернявський С. С., Вознюк А. А., Дударець Р. М., Беленок В. П. та ін. Київ : Нац. акад. внутр. справ, 2016. 92 с.

148. Розшук незаконно отриманих активів: практичний посібник / Базельський інститут управління, Міжнародний центр з повернення активів. 2015. 146 с.

149. Романенкова С. В. Поняття електронного правосуддя, його генезис та впровадження у правозастосовну практику розвинених країн. *Арбітражний та цивільний процес*. 2013. номер 4. С. 26–31

150. Ромців О. І. Криміналістична характеристика злочинів у сфері службової діяльності. Zbiór raportów naukowych. С. 10–14. URL: http://xn--e1aajfpcds8ay4h.com.ua/files/txt/scientific_conference_34/zbornik_Lodz_34_4.pdf#page=10.

151. Ромців О. І. Особливості подолання протидії під час розслідування злочинів у сфері службової діяльності: дис. … канд. юрид. наук: 12.00.09. Львів. 2016. 226 с.

152. Салтевський М. В. Криміналістика (у сучасному викладі): підручник. Київ: Кондор, 2005. 588 с.

153. Салтевський М. В. Криміналістика: підручник: у 2-х ч. Ч. 2. Харків: Консум, 2001. 268 с.

154. Сердюк Л. Р. Електронне судочинство через призму верховенства права: окремі питання теорії й практики. *Науковий вісник Херсонського державного університету*. Серія : Юридичні науки. 2016. Вип. 1(4). С. 126–129. URL: http://nbuv.gov.ua/UJRN/Nvkhdu_jur_2016_1(4)__35

155. Сірий Є. В. Соціологія: загальна теорія та методологія, історія розвитку, спеціальні та галузеві теорії : навч. посіб. Київ: Атіка, 2009 р. 492 с.

156. Словник української мови : в 11 т. / АН Української РСР, Ін-т мовознав. ім. О. О. Потебні; ред. кол.: І. К. Білодід (голова) та ін. Київ : Наук. думка, 1970–1980.Т. 7. 723 с.

157. Стахівський С. М. Теорія і практика кримінально-процесуального доказування: монографія. Київ: Нац. академія внутр. справ України, 2005. 272 с.

158. Стратегія сталого розвитку «Україна – 2020: Указ Президента України від 12 січ. 2015 р. № 5/2015. URL: https://zakon.rada.gov.ua/laws/show/5/2015#Text

159. Суд – це не будівля, – це послуга: британський експерт про європейське розуміння ролі суду та онлайн-урегулювання суперечок. *Юридична практика*, 2017. номер 26 (1011). URL: http://pravo.ua/ news.php?id=0062445.

160. Судитимуть учасників організованої групи, які втручалися в автоматизовану систему та перереєстровували майно громадян. URL: https://gp.gov.ua/ua/posts/suditimut-ucasnikiv-organizovanoyi-grupi-yaki-vtrucalisya-v-avtomatizovanu-sistemu-ta-pererejestrovuvali-maino-gromadyan

161. Тактика проведення судових експертиз: лекція для усіх форм навчання: метод. реком. / укл. М. Г. Щербаковський. Харків: Нац. ун-т внутр. справ, 2004. 60 с.

162. Таран О.В., Чернявський С.С. Право на справедливий суд у нормах міжнародного гуманітарного права (міжнародний збройний конфлікт, кримінальне обвинувачення). *Наше право*. № 2. 2023. С.251–255. DOI: 10.32782/NP.2023.2.38

163. Татаров О. Ю. Досудове провадження в кримінальному процесі України: теоретико-правові та організаційні засади (за матеріалами МВС України): монограф. Донецьк: 2012. 640 с.

164. Тетерятник Г. К. Інститут понятих при проведенні слідчих (розшукових) дій в умовах надзвичайних правових режимів. *Держава та регіони*. Серія: Право. 2020. № 4 (70). С. 196.

165. Тимофєєва Н. В. Використання спеціальних знань при розслідуванні злочинів проти безпеки виробництва : дис. ... канд. юрид. наук: 12.00.09. Київ, 2018. 214 с.

166. Тимчишин А. М. Спеціальні знання у кримінальному процесі України : монографія. Одеса : «Юридика», 2023. 362 с.

167. Тищенко В. В. Корисливо-насильницькі злочини: криміналістичний аналіз: монографія. Одеса: Юрид. літ. 2002. 360 с.

168. Тіщенко В. В. Теоретичні і практичні основи методики розслідування злочинів: монографія. Одеса: Фенікс, 2007. 260 с.

169. Топорецька З. М. Криміналістична характеристика декларування недостовірної інформації. *Вісник кримінального судочинства*. № 2. 2018. С. 156–166.

170. Топчій В. В., Горбачевський В. Я. Взаємодія правоохоронних органів у запобіганні транснаціональній організованій злочинності в Україні. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2013. № 4. С. 121–129.

171. Трепак В. М. Теоретико-прикладні проблеми запобігання та протидії корупції в Україні : дис. … докт. юрид. наук : 12.00.08. Львів, 2020. С. 327–328.

172. Туркевич В. К. Деякі особливості допиту обвинувачених у справах про хабарництво. *Вісник Київського університету.* 1987. № 7. С. 53–57.

173. Тутецька Н. В. Судова експертиза як засіб доказування у кримінальному судочинстві *Теорія і практика судової експертизи і криміналістики* : матеріали всеукр. наук.-практ. конф. з нагоди 85-річчя доктора юридичних наук, професора Н. І. Клименко (Київ – Маріуполь, 27 лют. 2018 р.). Київ Маріуполь, 2018. С. 357–359.

174. Участь спеціаліста у проведенні слідчих (розшукових) дій під час розслідування корупційних злочинів: метод. рек. / Б. Б. Теплицький, О. М. Шрамко, В. В. Юсупов. Київ: Нац. акад. внутр. справ, 2019. 71 с.

175. Федорчук О. Предмет злочину, передбаченого ст. 376-1 КК України (незаконне втручання в роботу автоматизованої системи документообігу суду). *Підприємництво, господарство, право* : науково-практичний господарсько-правовий журнал. 2016. № 11. С. 186–190.

176. Фонова О. С. Упрощене електронне провадження – інноваційний розвиток господарського процесу. URL: http://lg.arbitr.gov.ua/sud5014/4673456/279646/

177. Хавронюк М. І. Стаття 376-1 Кримінального кодексу України: здобуток чи прорахунок? *Вісн. Верхов. Суду України*. 2009. № 10. С. 6–13.

178. Хахуцяк О.Ю., Антощук А.О. Процесуальні аспекти доказування підроблення документів у сфері державної реєстрації. *Наше право*. 1. 2026. С. 53–59. DOI: https://doi.org/10.71404/NP.2026.1.7

179. Христинченко Н. П. Принципи відкритості у діяльності органів виконавчої влади: проблеми реалізації. *Наше право*. 2013. № 7. С. 47–52. URL: http://nbuv.gov.ua/UJRN/Nashp_2013_7_10.

180. Хто і як втручався в автоматизовану систему документообігу суду? URL. https://dejure.foundation/library/khto-i-yak-vtruchavsia-v-avotomatyzovanusystemu-dokumentoobihu-sudu

181. Цивільний кодекс України: Закон України від 16 січ. 2003 р. № 435-IV. *Верховна рада України*. URL: https://zakon.rada.gov.ua/laws/show/435-15/print

182. Цимбал П. В., Антонюк А. Б., Кузьменко О. В., Омельчук Л. В., Тимошенко О. А. Судово-експертна діяльність в Україні: навчальний посібник. Київ: ПВНЗ «Європейський університет», 2024. 188 с.

183. Чаплинський К. О. Тактика проведення окремих слідчих дій : моногр. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2006. 308 с.

184. Чаплинський К. О. Наукові підходи щодо визначення поняття та сутності спеціальних знань у кримінальному судочинстві. *Актуальні питання теорії і практики криміналістичної науки*: зб. матер. Всеукр. наук.-практ. конф. (Київ, 23 січ. 2015). Київ : «Гельветика», 2015. С. 37–41.

185. Чаплинський К. О. Тактичне забезпечення проведення слідчих дій: монографія. Дніпропетр. держ. ун-т внутр. справ. Дніпро: Ліра ЛТД, 2011. 496 с.

186. Чередник К. О. Розслідування шахрайства на ринку нерухомості, вчиненого злочинними угрупованнями: дис. …канд. юрид. наук: 12.00.09. Київ. 2019. 270 с.

187. Черенков А. М. Криміналістична характеристика предметів декларування недостовірної інформації. *Науковий вісник Міжнародного гуманітарного університету*. Сер.: Юриспруденція. 2019 № 39. С. 154–157. DOI https://doi.org/10.32841/2307-1745.2019.39.35.

188. Черенков А. М. Криміналістична характеристика суб'єкта декларування недостовірної інформації. *Підприємництво, господарство і право*. 2019. № 7. С. 222–226. DOI https://doi.org/10.32849/2663-5313.2019.7.40

189. Черенков А. М. Розслідування декларування недостовірної інформації: дис. …канд. юрид. наук. Київ, 2020. 270 с.

190. Черепненко О. Я. Взаємодія підрозділів ОВС з іншими силовими структурами, державними та громадськими організаціями при ліквідації масових заворушень. *Форум права*. 2011. № 2. С. 958–962.

191. Чернявський С. С. Методика розслідування злочинів у сфері банківського кредитування: дис. ...канд. юрид. наук: 12.00.09. Київ, 2002. 240 с.

192. Чичиркіна С. П. Організація і тактика розслідування службових підроблень : дис. ... канд. юрид. наук : 12.00.09. Київ, 2012. 222 с.

193. Чичиркіна С. П. Способи приховування злочинів у сфері службової діяльності. *Юридичний часопис НАВС*. Київ., 2011. № 1 (1). С. 151–158.

194. Чорноус Ю. М. Актуальні питання реалізації міжнародного співробітництва під час розслідування злочинів. *Протидія злочинності*: теорія та практика: матер. VII Всеукр. наук.-практ. конф. (Київ, 19 жовтня 2016 р.). Київ: Нац. академ. прокур. України, 2016. С. 581–585.

195. Шевченко О. В. Використання спеціальних товарознавчих знань під час досудового розслідування: дис… канд. юрид. наук: 12.00.09. Київ, 2017. 317 с.

196. Шевчишен А. В. Проблеми доказування стороною обвинувачення у досудовому розслідуванні корупційних злочинів у сфері службової діяльності та професійної діяльності, пов'язаної з наданням публічних послуг: дис. …докт. юрид. наук: 12.00.09. Київ, 2019. 624 с.

197. Шевчишен А. В. Проблеми доказування стороною обвинувачення у досудовому розслідуванні корупційних злочинів у сфері службової діяльності та професійної діяльності, пов'язаної з наданням публічних послуг: автореф. дис. …докт. юрид. наук: 12.00.09. Київ, 2019. 43 с.

198. Шепітько М. В. Повторність та сукупність злочинів за кримінальним правом України. *Використання сучасних досягнень криміналістики у боротьбі зі злочинністю* : матеріали наук.-практ. конф. (Донецьк, 14 квіт. 2006). Донецьк : Донец. юрид. ін-т ЛДУВС, 2007. С. 301–304.

199. Шепітько В. Ю. Криміналістика. Енциклопедичний словник (українсько-російський і російсько-український) / за ред. акад. В. Я. Тація. Харків: Право, 2001. 560 с.

200. Шеремет А. П. Криміналістика: навч. посіб. Київ: ЦУЛ, 2005 472 с.

201. Шумейко Д. О. Розслідування прийняття пропозиції, обіцянки або одержання неправомірної вигоди службовою особою: дис. …канд. юрид. наук: 12.00.09. Київ, 2015. 240 с.

202. Щербіна А. В. Кримінальна відповідальність за незаконне втручання в роботу автоматизованої системи документообігу суду: дис. …канд. юрид. наук: 12.00.08. Маріуполь, 2021. 219 с.

203. Юсупов В. А. Структура адміністративно-правового статусу правоохоронних органів України. *Науковий вісник Ужгородського національного університету*. Серія Право, 2014. Випуск 29. Частина 2 Том 4/2, С. 136–140.

204. Як працює електронне судочинство, або «Встати! Суд на зв'язку». URL: https://www.ukrinform.ua/rubric-society/3016937-ak-pracue-elektronne-sudocinstvo-abo-vstati-sud-na-zvazku.html

205. Andrii Antoshchuk, Olha Dobrova, Olena Volobuieva, Vladas Tumalavičius, Oksana Bryskovska Forensic approaches to verifying the evidence reliability in the process of collecting and evaluating information during pre-trial investigations. (2026) *Cadernos de Dereito Actual*, (31), pp. 176–195. Available at: https://www.cadernosdedereitoactual.es/index.php/cadernos/article/view/1435

206. Ivan Kubariev, Yevgen Barash, Valeri Pcholkin, Olena Pluzhnik. Assessingthe Contemporary Issuesof Countering Transnational Crime. *JURNAL CITA HUKUM – INDONESIAN LAW JOURNAL*. Vol. 9. No. 2 (2021), P. 291-304.

207. Ndulo M. Review of the Anti-Corruption Legal Framework in Zambia. Southern African Institute for Policy and Research. 2014. URL: http://saipar.org/wp-content/uploads/2013/09/Ndulo_Review-of-the-Anti-corruption-Legal-Framework1.pdf.

208. Petro Rekotov, Andriy Antoshchuk, Iryna Dubivka, Yulia Tereshchenko, Volodymyr Bondar, Viacheslav Kuliush Countering Financial Cybercrime: Pre-Trial Investigation Standards, Digital Forensics Tools, and International Coordination. *Journal of Zhengzhou University-Natural Science*. VOL 57 : ISSUE 1 – 2026. P. 73–80. DOI: 10.5996/jzund.2025.v57i1.233551

209. Theodore W. Ruger, Pauline T. Kim, Andrew D. Martin, Kevin M. Quinn. The Supreme Court forecasting project: legal and political science approaches to predicting Supreme Court decisionmaking. URL: https://www.law.upenn.edu/cf/faculty/truger/workingpapers/104ColumLR1150.pdf

210. U.S. Department of Labor E-Government Strategic Plan. URL: http://www.dol.gov/_sec/e_government_plan/p41-43_appendixe.htm

ДОДАТКИ

Додаток А

Результативність досудового розслідування кримінальних правопорушень, передбачених ст. 376-1 КК України (2020–2026 рр.)

Рік	Внесено до ЄРДР кримінальних проваджень	Повідомлено про підозру	Направлено до суду з обвинувальним актом	Частка направлених до суду, %
2020	30	0	0	0 %
2021	32	2	2	6,2 %
2022	46	0	0	0 %
2023	65	19	19	29,2 %
2024	42	9	9	21,4 %
2025	35	3	3	8,5 %
2026 (4 міс.)	17	1	1	2,8 %

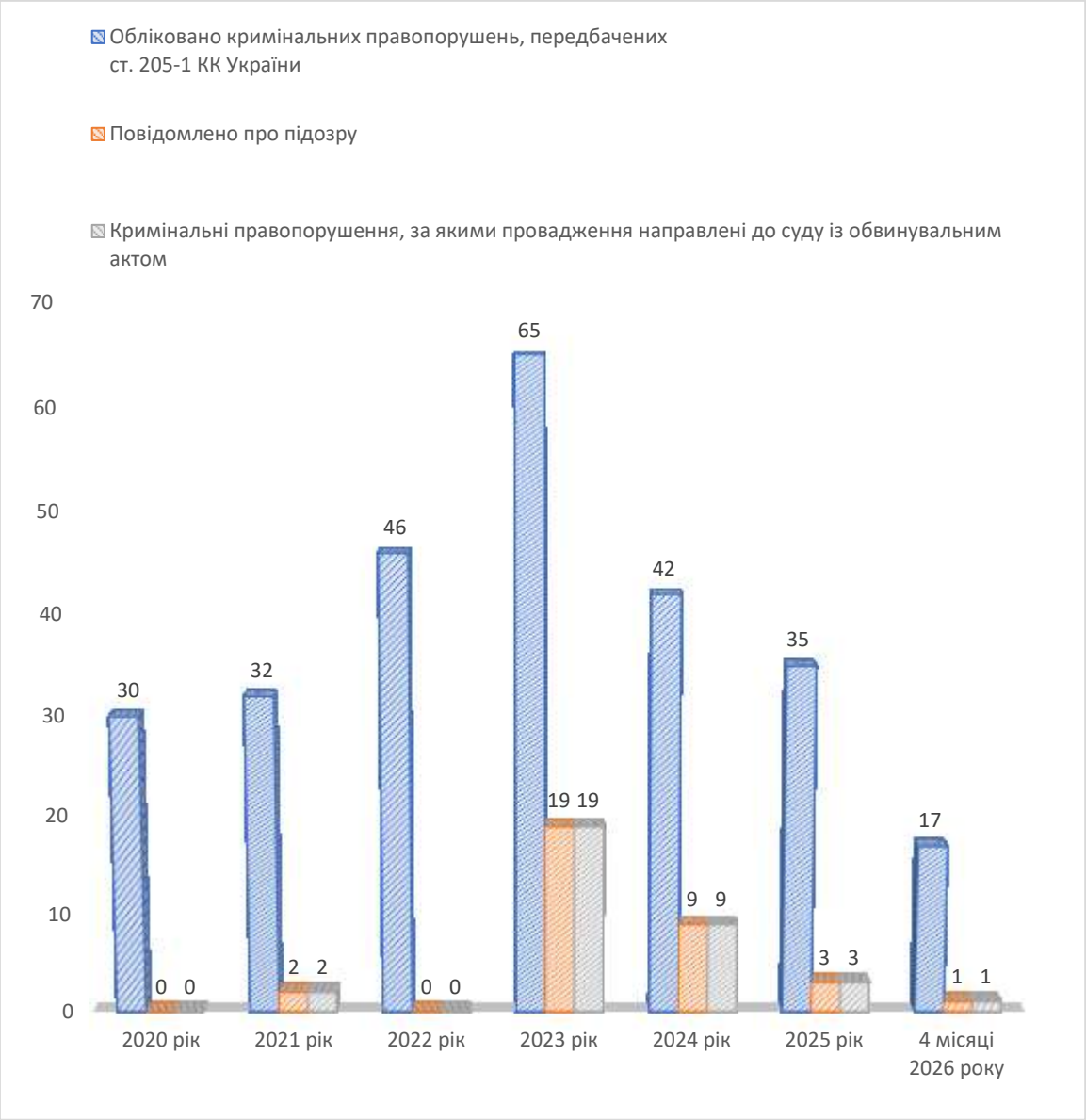
Згідно зі статистичною інформацією Офісу Генерального прокурора, до Єдиного реєстру досудових розслідувань упродовж 2020–2026 років внесено відомості про кримінальні правопорушення, передбачені ст. 376-1 КК України: у 2020 році – 30 кримінальних проваджень (повідомлень про підозру – 0), у 2021 році – 32 (2 підозри), у 2022 році – 46 (0 підозр), у 2023 році – 65 (19 підозр), у 2024 році – 42 (9 підозр), у 2025 році – 35 (3 підозри), а за чотири місяці 2026 року – 17 (1 підозра).

Щодо результативності завершення досудового розслідування, у вигляді направлення обвинувальних актів до суду, встановлено такі показники: у 2020 році – 0 кримінальних проваджень (0 %), у 2021 році – 2 (6,2 %), у 2022 році – 0 (0 %), у 2023 році – 19 (29,2 %), у 2024 році – 9 (21,4 %), у 2025 році – 3 (8,5 %), у 2026 році – 1 (2,8 %).

Розрахунок середнього показника за досліджуваний період свідчить, що середній рівень направлення кримінальних проваджень до суду становить близько 9,7 %, що є вкрай низьким індикатором ефективності завершення досудового розслідування зазначеної категорії кримінальних правопорушень.

Додаток А-1

Графічне зображення результативності досудового розслідування кримінальних правопорушень, передбачених ст. 376-1 КК України (2020–2026 рр.)



Додаток Б

Аналітична довідка
за результатами анкетування слідчих та прокурорів щодо проблем розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя

З метою дослідження практичних проблем розслідування кримінальних правопорушень, передбачених ст. 376-1 КК України, проведено анкетування 112 слідчих Національної поліції України та 36 прокурорів. Опитування було спрямоване на з'ясування рівня методичного забезпечення, оцінки складності розслідування, потреб у професійній спеціалізації, особливостей взаємодії між суб'єктами кримінального провадження, а також визначення найбільш актуальних тактичних аспектів проведення окремих слідчих (розшукових) дій.

Отримані результати свідчать про наявність комплексу організаційних, нормативних, технічних і методичних проблем, що негативно впливають на ефективність досудового розслідування незаконного втручання в роботу автоматизованих систем у сфері правосуддя.

Рівень методичного забезпечення

Результати опитування засвідчили недостатній рівень забезпечення практичних працівників спеціалізованими методичними рекомендаціями щодо розслідування кримінальних правопорушень, передбачених ст. 376-1 КК України. Так, лише 31 % слідчих та 20 % прокурорів зазначили, що їм відомі спеціалізовані методичні матеріали з указаних питань. Водночас 69 % слідчих і 80 % прокурорів повідомили про відсутність у них відповідної інформації.

Наведені показники свідчать про недостатню розробленість та поширеність спеціалізованих криміналістичних рекомендацій, орієнтованих на особливості розслідування незаконного втручання в роботу автоматизованих систем у сфері правосуддя. Відсутність належного методичного забезпечення може негативно позначатися на якості планування досудового розслідування, своєчасності

виявлення цифрових слідів, правильності організації взаємодії та ефективності доказування.

Оцінка складності розслідування

Більшість опитаних респондентів підтвердили, що розслідування кримінальних правопорушень, передбачених ст. 376-1 КК України, супроводжується суттєвими складнощами. Таку позицію висловили 69 % слідчих та 65 % прокурорів. Водночас лише 10 % слідчих і 21 % прокурорів не погодилися із твердженням про складність цієї категорії проваджень, а 21 % слідчих і 14 % прокурорів обрали інший варіант відповіді.

Отримані дані підтверджують, що переважна більшість практичних працівників усвідомлює специфічний характер розслідування незаконного втручання в роботу автоматизованих систем, що зумовлений необхідністю роботи з цифровими слідами, технічно складними інформаційними системами, потребою залучення спеціальних знань, а також труднощами встановлення механізму несанкціонованого доступу та ідентифікації причетних осіб.

Самооцінка професійного рівня

Оцінюючи власний професійний рівень, 72 % слідчих та 60 % прокурорів охарактеризували свої професійні якості як добрі. Водночас 28 % слідчих і 40 % прокурорів визначили їх як достатні.

Такі результати свідчать про загалом позитивну самооцінку професійної підготовки працівників органів досудового розслідування та прокуратури. Разом із тим вони не виключають існування об’єктивних труднощів, пов’язаних із розслідуванням кіберорієнтованих кримінальних правопорушень, що потребують вузькоспеціалізованих технічних знань і постійного оновлення професійних навичок.

Необхідність спеціалізації та навчання

Щодо необхідності проведення спеціалізованого навчання слідчих у сфері розслідування зазначеної категорії кримінальних правопорушень, позитивну відповідь надали 18 % слідчих та 35 % прокурорів. Водночас 72 % слідчих і 65 % прокурорів вважають таке навчання необов’язковим.

Наведені результати можуть свідчити про недостатнє усвідомлення окремими працівниками специфіки цифрових доказів та складності сучасних механізмів втручання в автоматизовані системи. Водночас значно вищий показник серед прокурорів може пояснюватися їхньою процесуальною роллю в оцінці якості досудового розслідування та доказової бази.

Проблеми взаємодії під час досудового розслідування

Однією з ключових проблем, виявлених у ході дослідження, є недостатня ефективність взаємодії між суб'єктами, залученими до розслідування незаконного втручання в роботу автоматизованих систем.

Найбільш поширеною проблемою респонденти визначили низький рівень матеріально-технічного забезпечення діяльності, пов'язаної з фіксацією, збереженням та дослідженням цифрової інформації. На це вказали 46 % слідчих і 45–47 % прокурорів.

Другим за значущістю чинником є відсутність належної зацікавленості або ініціативності окремих суб'єктів взаємодії, що було відзначено 32 % слідчих та 31 % прокурорів.

Крім того, 17–18 % респондентів звернули увагу на нерозуміння окремими учасниками змісту, завдань і меж взаємодії, а 15–18 % – на недосконалість нормативного регулювання міжвідомчої та внутрішньо-системної взаємодії.

Отримані результати свідчать, що проблеми взаємодії мають комплексний характер і охоплюють не лише нормативно-правові, а й організаційні, кадрові та ресурсні аспекти. Це ускладнює оперативне отримання технічної інформації, забезпечення її збереження та використання у процесі доказування.

Тактичні особливості проведення обшуку

Окремий блок питань був присвячений визначенню найбільш важливих тактичних аспектів проведення обшуку у кримінальних провадженнях цієї категорії.

Найбільш значущим чинником респонденти визначили необхідність урахування ризику швидкого знищення або дистанційного видалення інформації, що підтримали 61 % слідчих та 62 % прокурорів.

Необхідність забезпечення раптовості проведення обшуку відзначили 56 % слідчих та 55 % прокурорів.

Водночас 48–49 % респондентів акцентували увагу на необхідності одночасного контролю за поведінкою присутніх осіб, а 51–52 % – на важливості своєчасного виявлення об’єктів, які зовні можуть не сприйматися як джерела доказової інформації.

Наведені результати підтверджують специфічний характер обшуку у провадженнях щодо незаконного втручання в роботу автоматизованих систем, де особливого значення набувають швидкість реагування, технічна підготовка слідчо-оперативної групи, контроль за цифровим середовищем та мінімізація ризику втрати електронних доказів.

Висновки

Результати анкетування свідчать про наявність об’єктивних труднощів у розслідуванні кримінальних правопорушень, передбачених ст. 376-1 КК України, що обумовлені недостатнім рівнем методичного забезпечення, обмеженими матеріально-технічними можливостями, проблемами міжвідомчої взаємодії та специфікою роботи з цифровими доказами.

Встановлено потребу у вдосконаленні криміналістичних рекомендацій щодо розслідування незаконного втручання в роботу автоматизованих систем, розробленні спеціалізованих алгоритмів проведення слідчих (розшукових) дій, підвищенні рівня технічного забезпечення органів досудового розслідування та розширенні практики залучення спеціалістів і судових експертів.

Отримані результати підтверджують доцільність подальшого розвитку науково-методичних підходів до формування криміналістичної методики розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя.

Додаток В

Аналітична довідка

за результатами вивчення 105 кримінальних проваджень за фактами незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя

З метою дослідження криміналістично значущих особливостей незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя проведено вивчення 105 кримінальних проваджень зазначеної категорії. Аналіз матеріалів досудового розслідування дозволив установити типові характеристики осіб, причетних до вчинення таких кримінальних правопорушень, особливості способів приховування протиправної діяльності, специфіку слідової картини, напрями використання спеціальних знань, а також найбільш поширені види судових експертиз.

Отримані результати свідчать про складний характер зазначених кримінальних правопорушень, їх високий рівень латентності, адаптованість до цифрового середовища та значну залежність ефективності розслідування від своєчасного виявлення й дослідження цифрових слідів.

Характеристика осіб, причетних до незаконного втручання

За результатами вивчення кримінальних проваджень встановлено, що переважну більшість осіб, причетних до незаконного втручання в роботу автоматизованих систем у сфері правосуддя, становлять чоловіки – 79,5 %, тоді як частка жінок складає 20,5 %.

Аналіз вікових характеристик свідчить, що найбільш кримінально активною є категорія осіб віком від 40 до 54 років – 41,3 %. Особи віком 29–39 років становлять 25,9 %, від 18 до 28 років – 12,8 %, від 55 до 59 років – 11,6 %, а 8,4 % складають особи віком 60 років і старше.

Отримані показники свідчать, що незаконне втручання в роботу автоматизованих систем у більшості випадків здійснюється особами, які мають достатній професійний досвід, тривалий стаж роботи, належний рівень обізнаності щодо функціонування відповідних інформаційних систем, а також знання внутрішніх процедур діяльності органів та установ системи правосуддя.

За сімейним станом переважають особи, які перебувають у шлюбі – 61,4 %, тоді як 38,6 % не перебувають у шлюбі. Такі результати дають підстави стверджувати, що вчинення зазначених кримінальних правопорушень не пов'язується виключно із соціальною дезадаптацією або нестабільним способом життя, а нерідко здійснюється особами із відносно стабільним соціальним статусом.

Використання спеціальних знань у кримінальних провадженнях

Вивчення матеріалів кримінальних проваджень показало значну роль спеціальних знань під час розслідування незаконного втручання в роботу автоматизованих систем.

Найчастіше спеціалісти залучалися до проведення слідчих (розшукових) дій – у 52 % випадків. Надання консультацій щодо виявлення, фіксації та вилучення цифрових слідів мало місце у 45 % кримінальних проваджень. У 31 % випадків спеціалісти надавали пояснення у суді відповідно до ст. 357, 358 КПК України.

Наведені результати свідчать, що розслідування цієї категорії кримінальних правопорушень об'єктивно потребує активного використання спеціальних знань у сфері комп'ютерної техніки, інформаційної безпеки, телекомунікацій та цифрової криміналістики. Участь спеціалістів має важливе значення як на початковому етапі досудового розслідування, так і під час подальшого дослідження електронних доказів.

Способи приховування незаконного втручання

Аналіз кримінальних проваджень дозволив установити, що приховування незаконного втручання в роботу автоматизованих систем найчастіше здійснюється шляхом внесення до системи недостовірних або змінених даних – у 62 % випадків.

Використання чужих облікових записів зафіксовано у 51 % кримінальних проваджень, а видалення або модифікація електронних записів – у 46 % випадків.

Такі дані свідчать про високий рівень адаптації способів приховування до особливостей цифрового середовища. Особи, причетні до втручання, нерідко намагаються створити уявлення про легітимність виконаних дій, ускладнити ідентифікацію фактичного користувача або знищити електронні сліди протиправної діяльності.

Установлено, що способи приховування можуть охоплювати не лише технічні дії щодо модифікації інформації, а й організаційні заходи, спрямовані на інсценування технічних помилок, перекладання відповідальності на інших працівників або створення формальних підстав для внесення змін до інформаційної системи.

Особливості ідеальних слідів

У ході дослідження встановлено, що важливу роль у доказуванні відіграють ідеальні сліди, носіями яких є особи, обізнані про обставини незаконного втручання.

Найчастіше такими особами виступають працівники органів та установ системи правосуддя, які безпосередньо або опосередковано спостерігали використання автоматизованих систем – 28,7 %.

Особи, які виявили ознаки незаконного втручання або повідомили про них, становлять 24,5 %, а працівники, що здійснювали технічне обслуговування чи налаштування програмного забезпечення, – 15,2 %.

Наведені результати свідчать про важливість своєчасного встановлення кола осіб, які можуть володіти інформацією щодо функціонування автоматизованих систем, особливостей доступу до них, технічних збоїв або підозрілих змін у роботі програмного забезпечення.

Значення судових експертиз

Результати дослідження підтверджують ключову роль судових експертиз під час розслідування незаконного втручання в роботу автоматизованих систем.

Найбільш значущою визнано комп’ютерно-технічну експертизу, яка призначалася у 76 % кримінальних проваджень. Експертиза телекомунікаційних систем і засобів застосовувалася у 51 % випадків, експертиза у сфері технічного захисту інформації – у 43 %, а почеркознавча й технічна експертиза документів – у 34 % проваджень.

У разі поєднання незаконного втручання з корупційними проявами призначалися також економічні експертизи (22 %) та експертизи відео- і звукозапису (17 %).

Отримані результати свідчать, що ефективне доказування у провадженнях цієї категорії є неможливим без використання спеціальних експертних знань, спрямованих на встановлення механізму втручання, способу доступу до системи, характеру змін у цифрових даних, а також зв’язку між технічними діями та конкретною особою.

Висновки

Проведене дослідження дозволило встановити, що незаконне втручання в роботу автоматизованих систем в органах та установах системи правосуддя характеризується високим рівнем технічної складності, попередньою підготовкою та значною адаптацією до цифрового середовища.

Типовими особами, причетними до таких кримінальних правопорушень, є соціально адаптовані особи середнього віку, які мають професійний досвід та обізнаність щодо функціонування автоматизованих систем.

Ефективність досудового розслідування значною мірою залежить від своєчасного виявлення цифрових слідів, активного використання спеціальних знань, належної організації взаємодії між суб’єктами розслідування та правильного призначення судових експертиз.

Отримані результати можуть бути використані для подальшого вдосконалення криміналістичної методики розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя, а також підвищення ефективності практичної діяльності органів досудового розслідування.

Додаток Г

ЗАТВЕРДЖУЮ
Заступник начальника Головного слідчого управління Національної поліції України – начальник управління організації роботи та методичного забезпечення, д. ю. н., професор, заслужений юрист України
полковник поліції

Артем ШЕВЧИШЕН

___._____ 2026 року

АКТ

Про впровадження у практичну діяльність Головного слідчого управління Національної поліції України результатів дисертаційного дослідження Моісеєва М.Г.

Комісія у складі

Голови:	начальника 3-го відділу (методичної роботи та правового забезпечення) управління організації роботи та методичного забезпечення Головного слідчого управління Національної поліції України, доктора філософії в галузі права, майора поліції Романова Максима
членів комісії:	заступника начальника 3-го відділу (методичної роботи та правового забезпечення) управління організації роботи та методичного забезпечення Головного слідчого управління Національної поліції України, полковника поліції Гіжі Ігоря
	старшого слідчого в ОВС 3-го відділу (методичної роботи та правового забезпечення) управління організації роботи та методичного забезпечення Головного слідчого управління Національної поліції України, доктора філософії в галузі права, майора поліції Крушеницького Андрія

комісія відповідно до наказу Національної поліції України № 692 від 17.06.2025 «Про затвердження Порядку участі працівників слідчих

підрозділів Національної поліції України в науковій та освітній діяльності», склала цей акт щодо розгляду основних положень і результатів дисертаційного дослідження Моісеєва Максима Геннадійовича на тему «Основи методики розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя», поданого на здобуття наукового ступеня доктора філософії за спеціальністю 081 Право.

Дисертаційне дослідження присвячене розробленню наукових основ методики розслідування незаконного втручання в роботу автоматизованих систем органів та установ системи правосуддя України в умовах цифровізації судової влади. У роботі сформульовано авторське визначення цього виду кримінального правопорушення, розроблено його криміналістичну характеристику, запропоновано класифікацію типових слідчих ситуацій і версій, обґрунтовано підходи до виявлення та дослідження цифрових доказів, визначено засади взаємодії учасників розслідування та підготовлено пропозиції щодо вдосконалення кримінального процесуального законодавства у сфері забезпечення кібербезпеки правосуддя.

Комісією встановлено, що висновки, які містяться у дисертаційному дослідженні, можуть використовуватись у практичній діяльності слідчих підрозділів Національної поліції України під час проведення занять у системі службової підготовки, а також при проведенні нарад і семінарів, а викладені в них пропозиції та рекомендації можуть бути корисними під час розслідування кримінальних правопорушень, зокрема вчинених жінками.

Матеріали, викладені у висновках дисертаційного дослідження, можуть використовуватись під час підготовки листів-роз'яснень до органів досудового розслідування України, оскільки мають як необхідний теоретичний та методологічний рівень, так і практичну цінність, що сприятиме вдосконаленню їх процесуальної діяльності.

Голова комісії: **Максим РОМАНОВ**

Члени комісії: **Ігор ГІЖА**

Андрій КРУШЕНИЦЬКИЙ

ЗАТВЕРДЖУЮ
Проректор Національної
академії внутрішніх справ
доктор юридичних наук, професор,
заслужений юрист України
полковник поліції

Олег ТАРАСЕНКО

06.05 2026 року

АКТ

06.05 2026 м. Київ № 144-м

Впровадження результатів дисертації Моісеєва М.Г. на тему «Основи методики розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя» в наукову діяльність НАВС

Уклала комісія з виявлення, узагальнення та впровадження позитивного досвіду роботи у складі:

– т.в.о. начальника відділу організації наукової діяльності, кандидата філософських наук, старшого дослідника майора поліції Ольги Антіпової;

– начальника відділу докторантури та ад'юнктури, доктора юридичних наук, професора підполковника поліції Олени Тихонової;

– завідувача кафедри криміналістики та судової медицини, кандидата юридичних наук, доцента майора поліції Андрія Антощука;

– завідувача науково-дослідної лабораторії з проблем протидії злочинності навчально-наукового інституту поліцейської діяльності, доктора юридичних наук, професора, заслуженого діяча науки і техніки України майора поліції Андрія Вознюка;

– завідувача загальної бібліотеки Людмили Гайдар.

Комісія розглянула й узагальнила матеріали дисертації, поданої на здобуття ступеня доктора філософії зі спеціальності 081 «Право», наукові праці аспіранта кафедри кримінального процесу Національної академії внутрішніх справ Моісеєва Максима Геннадійовича на тему «Основи методики розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя» та на основі проведеного аналізу дійшла висновку, що надана робота містить низку обґрунтованих теоретичних положень і практичних рекомендацій спрямованих на удосконалення правового

регулювання кримінальних процесуальних інститутів, що впливають на швидкість досудового розслідування, а також формулювання на їх основі пропозицій щодо оптимізації законодавства та правозастосовної практики, що дає підстави запровадити їх для використання в науковій діяльності Національної академії внутрішніх справ.

Проаналізовано основні результати дослідження Моісеєва М.Г., зокрема наукові праці, в яких опубліковані теоретичні положення дисертації:

1. Моісеєв М. Г. Основні засади електронного судочинства у праві Європейського Союзу та незалежній Україні: порівняльний аспект. *Публічне право.* 2022. № 48. С. 167-174. DOI https://doi.org/10.32782/2306-9082/2022-48-19

2. Моісеєв М. Г. Криміналістична характеристика незаконного втручання в роботу автоматизованих систем в органах правосуддя. *Юридичний вісник.* 2023. № 3. С. 265–277. DOI: https://doi.org/10.32782/yuv.v3.2023.33

3. Моісеєв М. Г., Зарубей В. В. Криміналістична характеристика особи злочинця, що незаконно втручається в роботу автоматизованих систем в органах та установах системи правосуддя. *KELM.* 2024 № 8 (68). С. 122–132. DOI: https://doi.org/10.51647/kelm.2024.8.17

4. Моісеєв М. Г. Обшук під час розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя. *Наукові інновації та передові технології.* № 4 (56). 2026. С. 3331–3344. DOI: https://doi.org/10.52058/2786-5274-2026-4(56)-3331-3343

5. Моісеєв М. Г. Основні засади електронного судочинства в праві Європейського союзу. *Кримінальне судочинство: права людини під час дії надзвичайного або воєнного стану* : міжнар. наук.-практ. конф. (Київ, 18 листоп. 2022 р.). Київ : Нац. акад. внутр. справ, 2022. С. 215–218. URL : https://elar.navs.edu.ua/server/api/core/bitstreams/0c56ce37-2df4-48cb-b8d8-1d5fe007a70a/content

7. Моісеєв М. Г. Можливості застосування міжнародного досвіду щодо удосконалення електронного судочинства в Україні при запровадженні воєнного стану. *Кримінальне процесуальне право на сучасному етапі розвитку України* : матеріали круглого столу, присвяч. 40-річчю кафедри кримінального процесу (Київ, 27 жовт. 2023 р.). Київ : Нац. акад. внутр. справ, 2023. С. 282–286. URL : https://elar.navs.edu.ua/server/api/core/bitstreams/ece9dd4d-8e55-4ed1-bfae-ebb66a98894e/content#page=283&zoom=100,72,481

8. Моісеєв М. Г. Електронне судочинство в умовах воєнного стану. *Кримінальне судочинство: сучасний стан та перспективи розвитку* : міжвідом. наук.-практ. конф. (Київ, 28 квіт. 2023 р.). Київ : Нац. акад. внутр. справ, 2023. С. 174–177. URL : https://elar.navs.edu.ua/server/api/core/bitstreams/72b10f52-7185-4e4c-b36f-943b408c5f7b/content

9. Моісеєв М. Г. Особа правопорушника як елемент криміналістичної характеристики незаконного втручається в роботу автоматизованих систем в органах та установах системи правосуддя. *Кримінологія і війна: екзистенційні виклики для України* : міжвідом. наук.-практ. круглого столу (Київ, 6 листоп. 2025 р.). Київ : Нац. акад. внутр. справ, 2025. С. 272–274.

На основі проведеного аналізу комісія зробила висновок про те, що вищезазначені матеріали дисертаційного дослідження Моісеєва М. Г. застосовуються під час підготовки монографій, підручників, навчальних посібників, методичних рекомендацій, узагальнення аналітичних матеріалів, обґрунтування пропозицій до чинних проєктів нормативно-правових актів, підготовка яких потребує проведення відповідних наукових досліджень або містить наукову складову.

Члени комісії:

Ольга АНТІПОВА

Олена ТИХОНОВА

Андрій АНТОЩУК

Андрій ВОЗНЮК

Людмила ГАЙДАР

ЗАТВЕРДЖУЮ
Проректор Національної
академії внутрішніх справ
доктор юридичних наук, професор,
заслужений діяч науки і техніки України
полковник поліції

Сергій ЧЕРНЯВСЬКИЙ

06.05. 2026 року

АКТ

06.05. 2026 м. Київ № 143-01

Впровадження результатів дисертації Моісеєва М. Г. на тему «Основи методики розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя» в освітній процес НАВС

Уклала експертна комісія з виявлення, узагальнення та впровадження позитивного досвіду роботи у складі:

– т.в.о. начальника відділу організації освітнього процесу, кандидата юридичних наук, старшого наукового співробітника полковника поліції Віктора Корольчука;

– начальника відділу докторантури та ад'юнктури, доктора юридичних наук, професора полковника поліції Олени Тихонової;

– завідувача кафедри криміналістики та судової медицини, кандидата юридичних наук, доцента майора поліції Андрія Антощука;

– завідувача загальної бібліотеки Людмили Гайдар.

Комісія розглянула й узагальнила матеріали дисертації, поданої на здобуття ступеня доктора філософії зі спеціальності 081 «Право», наукові праці аспіранта кафедри кримінального процесу Національної академії внутрішніх справ Моісеєва Максима Геннадійовича на тему: «Основи методики розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя».

Проаналізовано основні результати дослідження Моісеєва М. Г., зокрема наукові праці, в яких опубліковані теоретичні положення дисертації:

1. Моісеєв М. Г. Основні засади електронного судочинства у праві Європейського Союзу та незалежній Україні: порівняльний аспект. *Публічне право.* 2022. № 48. С. 167-174. DOI https://doi.org/10.32782/2306-9082/2022-48-19

2. Моісеєв М. Г. Криміналістична характеристика незаконного втручання в роботу автоматизованих систем в органах правосуддя. *Юридичний вісник.* 2023. № 3. С. 265–277. DOI: https://doi.org/10.32782/yuv.v3.2023.33

3. Моісеєв М. Г., Зарубей В. В. Криміналістична характеристика особи злочинця, що незаконно втручається в роботу автоматизованих систем в органах та установах системи правосуддя. *KELM.* 2024 № 8 (68). С. 122–132. DOI: https://doi.org/10.51647/kelm.2024.8.17

4. Моісеєв М. Г. Обшук під час розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя. *Наукові інновації та передові технології.* № 4 (56). 2026. С. 3331–3344. DOI: https://doi.org/10.52058/2786-5274-2026-4(56)-3331-3343

5. Моісеєв М. Г. Основні засади електронного судочинства в праві Європейського союзу. *Кримінальне судочинство: права людини під час дії надзвичайного або воєнного стану* : міжнар. наук.-практ. конф. (Київ, 18 листоп. 2022 р.). Київ : Нац. акад. внутр. справ, 2022. С. 215–218. URL : https://elar.navs.edu.ua/server/api/core/bitstreams/0c56ce37-2df4-48cb-b8d8-1d5fe007a70a/content

7. Моісеєв М. Г. Можливості застосування міжнародного досвіду щодо удосконалення електронного судочинства в Україні при запровадженні воєнного стану. *Кримінальне процесуальне право на сучасному етапі розвитку України* : матеріали круглого столу, присвяч. 40-річчю кафедри кримінального процесу (Київ, 27 жовт. 2023 р.). Київ : Нац. акад. внутр. справ, 2023. С. 282–286. URL : https://elar.navs.edu.ua/server/api/core/bitstreams/ece9dd4d-8e55-4ed1-bfae-ebb66a98894e/content#page=283&zoom=100,72,481

8. Моісеєв М. Г. Електронне судочинство в умовах воєнного стану. *Кримінальне судочинство: сучасний стан та перспективи розвитку* : міжвідом. наук.-практ. конф. (Київ, 28 квіт. 2023 р.). Київ : Нац. акад. внутр. справ, 2023. С. 174–177. URL : https://elar.navs.edu.ua/server/api/core/bitstreams/72b10f52-7185-4e4c-b36f-943b408c5f7b/content

9. Моісеєв М. Г. Особа правопорушника як елемент криміналістичної характеристики незаконного втручається в роботу автоматизованих систем в органах та установах системи правосуддя. *Кримінологія і війна: екзистенційні виклики для України* : міжвідом. наук.-практ. круглого столу (Київ, 6 листоп. 2025 р.). Київ : Нац. акад. внутр. справ, 2025. С. 272–274.

На основі проведеного аналізу комісія зробила висновок, що праці Моісеєва М.Г. містять науково обґрунтовані теоретичні положення і практичні рекомендації, що дає підстави запровадити їх для використання в освітньому процесі Національної академії внутрішніх справ, зокрема при викладанні навчальних дисциплін «Кримінальний процес», «Криміналістика», «Досудове розслідування», «Розслідування окремих видів кримінальних правопорушень»,

«Актуальні проблеми застосування кримінального процесуального законодавства» , «Взаємодія органів досудового розслідування з оперативними підрозділами та іншими правоохоронними органами під час протидії кримінальним правопорушенням» під час навчально-методичних та дидактичних матеріалів, а також рекомендувати їх до вивчення під час самостійної роботи здобувачів вищої освіти.

Члени комісії: **Віктор КОРОЛЬЧУК**

Олена ТИХОНОВА

Андрій АНТОЩУК

Людмила ГАЙДАР

Додаток Д

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

у яких опубліковано основні наукові результати дисертації:

1. Моісеєв М. Г. Основні засади електронного судочинства у праві Європейського союзу та незалежній Україні: порівняльний аспект. *Публічне право*. 2022. № 4 (48). С. 167–174. DOI: https://doi.org/10.32782/2306-9082/2022-48-19

2. Моісеєв М. Г., Зарубей В. В. Криміналістична характеристика особи злочинця, що незаконно втручається в роботу автоматизованих систем в органах та установах системи правосуддя. *Knowledge, Education, Law, Management*. 2024 № 8 (68). С. 122–132. DOI: https://doi.org/10.51647/kelm.2024.8.17

3. Моісеєв М. Г. Криміналістична характеристика незаконного втручання в роботу автоматизованих систем в органах правосуддя. *Юридичний вісник*. № 3, 2023. С. 265–277. DOI: https://doi.org/10.32782/yuv.v3.2023.33

4. Зарубей В. В., Моісеєв М. Г. Тактика проведення огляду під час розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя. *Право.UA*. № 1. 2026. С. 274–278. DOI: https://doi.org/10.71404/LAW.UA.2026.1.36

5. Моісеєв М. Г. Обшук під час розслідування незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя. *Наукові інновації та передові технології.* № 4(56) 2026. С. 3331–3343. DOI: https://doi.org/10.52058/2786-5274-2026-4(56)-3331-3343

які засвідчують апробацію матеріалів дисертації:

6. Моісеєв М. Г. Основні засади електронного судочинства в праві Європейського союзу. *Кримінальне судочинство: права людини під час дії надзвичайного або воєнного стану* : міжнар. наук.-практ. конф. (Київ, 18 листоп. 2022 р.). Київ : Нац. акад. внутр. справ, 2022. С. 215–218.

URL : https://elar.navs.edu.ua/server/api/core/bitstreams/0c56ce37-2df4-48cb-b8d8-1d5fe007a70a/content

7. Моісеєв М. Г. Можливості застосування міжнародного досвіду щодо удосконалення електронного судочинства в Україні при запровадженні воєнного стану. *Кримінальне процесуальне право на сучасному етапі розвитку України* : матеріали круглого столу, присвяч. 40-річчю кафедри кримінального процесу (Київ, 27 жовт. 2023 р.). Київ : Нац. акад. внутр. справ, 2023. С. 282–286. URL : https://elar.navs.edu.ua/server/api/core/bitstreams/ece9dd4d-8e55-4ed1-bfae-ebb66a98894e/content#page=283&zoom=100,72,481

8. Моісеєв М. Г. Електронне судочинство в умовах воєнного стану. *Кримінальне судочинство: сучасний стан та перспективи розвитку* : міжвідом. наук.-практ. конф. (Київ, 28 квіт. 2023 р.). Київ : Нац. акад. внутр. справ, 2023. С. 174–177. URL : https://elar.navs.edu.ua/server/api/core/bitstreams/72b10f52-7185-4e4c-b36f-943b408c5f7b/content

9. Моісеєв М. Г. Особа правопорушника як елемент криміналістичної характеристики незаконного втручання в роботу автоматизованих систем в органах та установах системи правосуддя. *Кримінологія і війна: екзистенційні виклики для України* : міжвідом. наук.-практ. круглого столу (Київ, 6 листоп. 2025 р.). Київ : Нац. акад. внутр. справ, 2025. С. 272–274.