УДК 343.35:328.185 (477)
DOI https://doi.org/10.32850/sulj.2021.4.19

ОКРЕМІ АСПЕКТИ ЗАПРОВАДЖЕННЯ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ ДОСУДОВОГО РОЗСЛІДУВАННЯ

Лісніченко Д. В., Мудрецька Г. В.

У статті аналізуються окремі аспекти запровадження інформаційно-телекомунікаційної системи досудового розслідування. Зауважено, що інформаційно-телекомунікаційна система оцифровує паперову документацію, що, своєю чергою, дає змогу обмінюватися файлами в межах кримінальних проваджень між співробітниками та структурними підрозділами одного органу, а також між різними органами в процесі розслідування.

Наголошено, що як і будь-яка інформаційна система, яку використовують судові та правоохоронні органи (автоматизована система документообігу суду, Єдиний реєстр досудових розслідувань, інформаційно-телекомунікаційна система досудового розслідування має бути нормативно врегульована, тобто мають бути прийняті нормативно-правові акти, які врегульовують питання її впровадження та функціонування. Нормативно закріпленими мають бути положення не тільки аспекти допустимості і достатності електронних доказів, але й питання відповідальності за збереження інформації, яка міститься в такій системі.

Впровадження інформаційно-аналітичної системи управління процесами досудового розслідування є одним з елементів реформи прокуратури та органів досудового розслідування, що покращить процес здійснення досудового розслідування та нагляду за додержанням законів органами, що провадять оперативно-розшукову діяльність, дізнання, досудове слідство тощо.

Констатується, що успішність реалізації інформаційно-телекомунікаційної реформи є розбудова єдиної інформаційної системи між прокуратурою, судовою владою та органами правопорядку, які розслідують або розглядають кримінальні провадження.

Акцентовано, що метою інформаційно-телекомунікаційної системи досудового розслідування є забезпечення автоматизації кримінально-процесуальної діяльності органів досудового розслідування та суду. Порядок використання такої системи має вводитись законом, а детальні аспекти її функціонування мають бути прописані в спеціальному Положенні про таку систему.

***Ключові слова**: кримінальне провадження; досудове розслідування; інформаційно-телекомунікаційна система; інформаційна безпека.*

Lisnichenko D. V., Mudretska H. V. Certain aspects of introduction of information and telecommunications system of pre-trial investigation

The article analyzes some aspects of the introduction of information and telecommunication system of pre-trial investigation. It is noted that the information and telecommunication system digitizes paper documents, which, in turn, allows the exchange of files in criminal proceedings between employees and departments of one body, as well as between different bodies in the investigation.

It was emphasized that, like any information system used by judicial and law enforcement agencies (automated court document management system, Unified Register of Pre-Trial Investigations, information and telecommunication system of pre-trial investigation, it should be regulated, ie regulations should be adopted to regulate The issues of its implementation and functioning The provisions of not only the admissibility and sufficiency of electronic evidence, but also the issue of responsibility for the preservation of information contained in such a system should be regulated.

The introduction of an information-analytical system for managing pre-trial investigation processes is one of the elements of the reform of the prosecutor's office and pre-trial investigation bodies, which will improve the process of pre-trial investigation and supervision of compliance with laws by bodies conducting operational investigative activities, inquiries, pre-trial investigations, etc.

It is stated that the success of the information and telecommunication reform is the development of a single information system between the prosecutor's office, the judiciary and law enforcement agencies that investigate or consider criminal proceedings. It is emphasized that the purpose of the information and telecommunication system of pre-trial investigation is to ensure the automation of criminal procedure of pre-trial investigation bodies and the court. The procedure for using such a system should be introduced by law, and detailed aspects of its operation should be prescribed in a special Regulation on such a system.

Key words: *criminal proceedings; pre-trial investigation; information and telecommunication system; informational security.*

Постановка проблеми та її актуальність. Автоматизація досудового розслідування є дієвим шляхом економії часу, ресурсів і забезпечення дотримання розумних строків, що є основним викликом у системі кримінальної юстиції. Ці процеси суттєво спрощують доступ до інформації, тим самим забезпечують підвищення рівня ефективності роботи судових та правоохоронних органів у боротьбі з організованою злочинністю. Електронне кримінальне провадження покликане спростити роботу правоохоронних органів та сприяти підвищенню якості захисту прав громадян. Це «розумна» інформаційно-аналітична система, що оцифровує паперову документацію, дозволяє обмінюватись файлами в межах кримінального провадження. Вона здатна спростити роботу суб'єктів кримінального провадження, які залучені до досудового розслідування. Це інструмент адміністрування та управління електронними версіями файлів кримінальних проваджень. Впровадження інформаційно-аналітичної системи управління процесами досудового розслідування є одним з елементів реформи прокуратури та органів досудового розслідування, що покращить процес здійснення досудового розслідування та нагляду за додержанням законів органами, що провадять оперативно-розшукову діяльність, дізнання, досудове слідство тощо.

Проте реалії вітчизняної правоохоронної системи не дозволяють повноцінно збирати, зберігати та передавати матеріали та інформацію в електронній системі на всіх стадіях кримінального провадження. У процесі створення і введення в дію таких інформаційно-аналітичних систем виникають проблеми технічного, соціально-технічного, організаційного і правового характеру. Зокрема, недоліком існування інформаційно-аналітичних систем є те, що вони функціонують як відокремлені інститути. Крім того, варто звернути увагу, що висловлюються побоювання щодо застосування цифрових технологій у сфері кримінального провадження: чи вдасться забезпечити конфіденційність баз даних від хакерських атак, особливо в умовах гібридної війни; чи позитивно вплине діджиталізація кримінального провадження на забезпечення прав особи в кримінальному провадженні тощо. Проведені раніше дослідження, які стосувались аналізу законодавчого забезпечення електронного кримінального провадження, мали поверховий характер і здебільшого торкались аналізу можливостей ЄРДР. Тому виникла необхідність розробки на державному рівні Концепції електронного кримінального провадження із визначенням основних етапів її запровадження з подальшим удосконаленням положень чинного Кримінального процесуального кодексу та інших законодавчих актів України, що регулюють правові відносини, пов'язані із запровадженням електронного кримінального провадження; удосконалення системи захисту персональних даних – системи інформаційної безпеки тощо.

Аналіз останніх досліджень і публікацій. Окремі проблемні питання використання інформаційних та телекомунікаційних технологій під час досудового розслідування досліджувались у роботах таких учених: В. Білоус, В. Бірюкова, В. Голубєва, М. Гуцалюка, М. Карчевського, Є. Лук'янчикова, Т. Михальчук, А. Молдована, А. Рибченко, М. Смирнова, А. Столітнього, В. Уварова, І. Хараберюша, В. Хахановського, Д. Цехана, С. Чернявського, Г. Чигриної та інших учених. Разом із тим потребують подальшого дослідження переваги та ризики запровадження інформаційно-телекомунікаційної системи досудового розслідування в Україні.

Мета статті полягає у формулюванні ключових положень Концепції інформаційно-телекомунікаційної системи органу досудового розслідування.

Виклад основного матеріалу. Проєктом Закону № 5246 «Про внесення змін до Кримінального процесуального кодексу України щодо запровадження інформаційно-телекомунікаційної системи досудового розслідування» [1], прийнятому Верховною Радою 01.06.2021 р., передбачено утворення та функціонування під час здійснення кримінальних проваджень у взаємодії з наявними системами Єдиного реєстру досудових розслідувань (ЄРДР), Єдиної судової інформаційно-телекомунікаційної системи (ЄСІТС), Інформаційно-телекомунікаційної системи досудового розслідування (ІТСДР). Положеннями вказаного законопроєкту, зокрема, визначається: функціональне призначення інформаційно-телекомунікаційної системи досудового розслідування; рівність правового статусу паперових та електронних документів у кримінальному процесі; надання доступу до матеріалів, які зберігаються в інформаційно-телекомунікаційній системі досудового розслідування учасникам кримінального провадження; можливість інтеграції інформаційно-телекомунікаційної системи досудового роз-

слідування з іншими інформаційними системами, зокрема з Єдиним реєстром досудових розслідувань та автоматизованою системою документообігу суду.

Крім того, проєктом пропонується зрівняти правовий статус паперових та електронних документів у кримінальному процесі. Таке оцифрування значною мірою розширить процесуальні можливості учасників кримінального провадження та суду досліджувати матеріали кримінального провадження, документи та докази в електронній формі. Запровадження інформаційно-телекомунікаційної системи досудового розслідування дозволить мінімізувати та, як наслідок, повністю відмовитись у майбутньому від паперового провадження у кримінальному процесі.

Проте можливість впровадження електронного обігу документів у кримінальний процес та повноцінне використання такої системи без порушення процесуальних норм можливе лише після розробки та прийняття значної кількості підзаконних нормативно-правових актів. Норми щодо управління, внесення змін та доступу до системи потребують детального опрацювання з урахуванням практики її використання, адже лише повноцінне визначення, кому і які повноваження будуть надані, дозволить ефективно використовувати новостворену систему. Зокрема, потрібно буде створити програмне забезпечення Інформаційно-телекомунікаційної системи досудового розслідування, прийняти відповідне Положення, які мають бути узгоджені Офісом Генерального прокурора з керівниками органів досудового розслідування (державних органів, у складі яких діють органи досудового розслідування), упровадити функціонування цієї системи у прокуратурі, органах досудового розслідування та забезпечити її взаємодію з ЄРДР та ЄСІТС, забезпечити відповідний захист системи.

До прийняття вказаного законопроєкту вже відбувались спроби діджиталізації кримінального провадження на стадії досудового розслідування. Зокрема, 30 квітня 2020 р. відбувся запуск пілотного проєкту системи електронного кримінального провадження eCase. Першими в дії її перевірили Національне антикорупційне бюро України, Спеціалізована антикорупційна прокуратура та Вищий антикорупційний суд.

За результатами використання пілотної версії eCase Національне антикорупційне бюро України у своєму звіті за перше півріччя 2020 р. зазначило, що існує три групи основних ризиків, які можуть виникнути на шляху повноцінного запуску системи: 1) нормативні. Насамперед для початку роботи eCase MS у законодавстві має з'явитися поняття «електронне кримінальне провадження». Йдеться про ухвалення закону, що передбачає відповідні зміни до Кримінального процесуального кодексу України. Крім того, основні правила діяльності eCase MS мають закріпитися міжвідомчим положенням. Нині як законопроєкт, так і проєкт положення підготовлені та перебувають на розгляді відповідно в Офісі Президента України й Офісі Генпрокурора та Вищої ради правосуддя; 2) інтегративні. Застереження щодо інтеграції стосуються поєднання роботи eCase MS із Єдиним реєстром досудових розслідувань та автоматизованою системою документообігу суду «Д3». Без допомоги в цьому власників систем – Офісу Генпрокурора та Державної судової адміністрації – детективи, прокурори і судді муситимуть дублювати дані в різних системах; 3) безпекові. Стосовно питання безпеки, безумовно, важливого для всіх бенефіціарів системи, то eCase MS підлягає державній експертизі у сфері технічного захисту інформації, яку має здійснити Державна служба спеціального зв'язку та захисту інформації. На цей час систему попередньо перевірили на зовнішні і внутрішні втручання експерти, що запрошені EUACI. Працівники антикорупційних органів, які обслуговуватимуть eCase MS, уже і самі мають досвід її тестування на проникнення [2].

Д. Кисленко зазначає, що використання комп'ютерних систем для прийняття процесуальних рішень нині видається дещо нереалістичним. Адже вдосконалення національної моделі досудового розслідування щодо забезпечення прав та законних інтересів особи в умовах діджиталізації кримінального провадження має відбуватися в декількох напрямах: по-перше, використання системи «Безпечне місто» в інтересах кримінального провадження та з метою захисту прав його учасників: встановлення камер для проведення загального спостереження; встановлення керованих (роботизованих) камер, які дозволяють оператору Системи скерувати камеру на ту чи іншу частину зображення, приблизити його до необхідного рівня; встановлення панорамних (оглядових) керованих камер, які дозволяють водночас проводити огляд значної частини міста; встановлення аналітичних камер (200 LPR) з розширеними аналітичними функціями: визначення кольору та марки автомобіля, підрахунок кількості транспорту тощо. По-друге, всебічне використання фото та відеозапису із вилученням з переліку учасників

кримінального провадження таких суб'єктів, як поняті. Висока інформативність відеозапису дає можливість подальшого відтворення як картини всієї слідчої дії (за умови безперервності ведення запису), так і її окремих елементів з метою перевірки правомірності та допустимості дій осіб, що беруть участь у ній, а також оцінки достовірності отриманих результатів. По-третє, використання комп'ютерних систем для прийняття процесуальних рішень [3].

А. Столітній вважає, що запровадження електронного кримінального провадження організаційно та технічно найбільш доцільно здійснювати на базі ЄРДР у чотири етапи: 1) удосконалення функціоналу ЄРДР; 2) залучення слідчого судді до електронного кримінального провадження; 3) залучення всіх суб'єктів кримінального провадження до електронного кримінального провадження за допомогою зовнішніх ресурсів цифрового обміну повідомленнями (електронна пошта); 4) перехід до здійснення електронних кримінальних процесуальних процедур із використанням особистих віртуальних кабінетів [4, с. 24].

На практиці інформаційно-телекомунікаційна система досудового розслідування має своїм завданням удосконалити положення кримінального провадження і вплинути на ефективність досудового розслідування та виконання завдань кримінального процесу. Проте в умовах нинішнього протистояння збройній агресії використання кібератак – накопичення матеріалів кримінальних проваджень у цифрованому вигляді, передача матеріалів кримінальних проваджень на носіях тощо – не лише не оптимізує роботу слідчого, прокурора і судді, а може призвести до створення численних процесуальних конфліктів щодо отримання матеріалів, суттєво полегшить доступ до матеріалів кримінального провадження осіб, які не мають жодного відношення до процесуальної діяльності. Отже, аби повністю відмовитись від паперового провадження на стадіях досудового розслідування та розгляду справи у суді, необхідно передбачати відповідну програму, належно обґрунтовану, соціально зважену, економічно вивірену, з визначенням тих етапів, які не стануть на заваді досягненню мети та виконання завдань кримінального процесу.

Способи захисту інформації в електронному кримінальному провадженні неодноразово здійснювались науковцями. Зокрема, П. Біленчук і М. Малій вважають, що електронний цифровий підпис повною мірою може забезпечити такий захист. Автори пояснюють це тим, що такий підпис має жорсткий зв'язок з документом, який підписується, високу захищеність від підробки, що зумовлено великим обсягом математичних розрахунків [5, с. 27]. Н. Топчій вважає, що наявний електронний документообіг в Україні, який регулюється законами «Про електронні документи та електронний документообіг» від 22.05.2003 № 851-IV, «Про електронні довірчі послуги» від 05.10.2017 № 2155-VIII і «Про електронний цифровий підпис» від 22.05.2003 р. № 852-IV, може сприяти подальшому формуванню електронного кримінального провадження [6, с. 214]. І. Каланча, досліджуючи електронне кримінальне провадження, вказує, що одним із перших етапів створення інформаційно-телекомунікаційної системи органу досудового розслідування має бути створення нормативної бази, яка включатиме, зокрема: розробку Положення про порядок ведення такої системи, Правил розмежування доступу до такої системи, Положення про обмін даними між системою і ЄРДР [7, с. 16].

Окрему увагу слід звернути на інформацію, що належить до державної таємниці. Зокрема, потрібно з'ясувати, чи дозволяє законодавство у сфері охорони державної таємниці роботу з деякими відомостями негласних слідчих (розшукових) дій (відомості про факт або методи проведення негласної слідчої (розшукової) дії; відомості, що дають змогу ідентифікувати особу, місце або річ, щодо якої проводиться чи планується проведення негласної слідчої (розшукової) дії, розголошення яких створює загрозу національним інтересам і безпеці) в електронних системах. Так, відповідно до Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їхніх результатів у кримінальному провадженні, затвердженої наказом Генеральної прокуратури, Міністерства внутрішніх справ України, Служби безпеки України, адміністрації Державної прикордонної служби України, Міністерства фінансів України, Міністерства юстиції України від 16.11.2012 № 114/1042/516/1199/936/1687/5 [8], засекречування матеріальних носіїв інформації щодо проведення негласних слідчих (розшукових) дій здійснюється слідчим, прокурором, співробітником уповноваженого оперативного підрозділу, слідчим суддею шляхом надання на підставі Зводу відомостей, що становлять державну таємницю. Відповідно до ст. 35 Закону України «Про державну таємницю» від 21.01.1994 № 3855-XII

технічний та криптографічний захисти секретної інформації здійснюються в порядку, встановленому Президентом України [9]. Відповідний Указ Президента України «Про Положення про порядок здійснення криптографічного захисту інформації в Україні» був затверджений 22 травня 1998 року за № 505/98 [10]. У п. 7 цього Положення зазначено, що для криптографічного захисту інформації, що становить державну таємницю, та службової інформації, створеної на замовлення державних органів або яка є власністю держави, використовуються криптосистеми і засоби криптографічного захисту, допущені до експлуатації. Відповідно до Закону України «Про захист інформації в інформаційно-телекомунікаційних мережах» від 05.07.1994 № 80/94-ВР в абз. 6 ст. 8 вказано, що обробка інформації з обмеженим доступом, у тому числі тієї, яка містить державну таємницю, можлива лише із застосуванням комплексної системи захисту інформації [11]. Порядок створення такої системи встановлюється Державною службою спеціального зв'язку та захисту інформації України (Порядок, затверджений наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 16 жовтня 2018 року № 141/ДСК). Відповідно до п. 14 Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених Постановою Кабінету Міністрів України від 29 березня 2006 р. № 373, підключення систем, у яких обробляється службова інформація та інформація, що становить державну таємницю, до глобальних мереж передачі даних здійснюється з використанням засобів криптографічного захисту інформації, які допущені до експлуатації для криптографічного захисту інформації відповідного ступеня обмеження доступу, та/або апаратних, апаратно-програмних засобів технічного захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи у сфері технічного захисту інформації та реалізують функції безпеки односпрямованої (односторонньої) передачі даних та/або двоспрямованої передачі даних з урахуванням їх змістового аналізу [12].

Таким чином, робота з інформацією, яка містить державну таємницю в інформаційно-телекомунікаційній системі досудового розслідування, можлива лише за наявності комплексної системи захисту інформації.

Отже, метою інформаційно-телекомунікаційної системи досудового розслідування є забезпечення автоматизації кримінально-процесуальної діяльності органів досудового розслідування та суд. Порядок використання такої системи має вводитись законом, а детальні аспекти її функціонування мають бути прописані у спеціальному Положенні про таку систему. Положення має містити такі норми: що являє собою Інформаційно-телекомунікаційна система досудового розслідування, мета її функціонування, суб'єкти, які використовуватимуть цю систему, її правовий статус, порядок доступу та захисту інформації в цій системі, аспекти взаємодії з будь-якою іншою інформаційною системою, яку використовують судові та правоохоронні органи (автоматизована система документообігу суду, Єдиний реєстр досудових розслідувань, «АСКОД», «Мегаполіс» тощо).

Література

1. Про внесення змін до Кримінального процесуального кодексу України щодо запровадження інформаційно-телекомунікаційної системи досудового розслідування : Закон України від 01.06.2021 р. № № **1498-IX.** URL: https://zakon.rada.gov.ua/laws/show/1498-20#Text.

2. Національне антикорупційне бюро України: звіт за перше півріччя 2020 р. С. 71. URL: https://nabu.gov.ua/report/zvit-pershe-pivrichchya-2020-roku.

3. Кисленко Д.П. Захист прав особи в аспекті діджиталізації кримінального провадження. *Наукові записки Львівського університету бізнесу та права. Серія економічна. Серія юридична.* 2021. Випуск 29. URL: https:// https://zenodo.org/record/5578672#.YoEKWstBzIU.

4. Столітній А. Концепція електронного кримінального провадження в Україні. *Вісник Національної академії прокуратури України.* 2018. № 4(56). С. 24–35.

5. Біленчук П., Малій М. Новітні засоби забезпечення кібербезпеки. *Бизнес и безопасность*. 2019. № 5. С. 27–28.

6. Топчій Н.С. Необхідність впровадження електронного кримінального провадження. *The Journal of Eastern European Law* / Журнал *східноєвропейського права*. 2019. № 69. С. 213–217.

7. Столітній А.В., Каланча І.Г. Концепція інформаційно-телекомунікаційної системи органу досудового розслідування. *Юридичний часопис Національної академії внутрішніх справ*. 2019. № 2(18). С. 14–23. URL: DOI: https://doi.org/10.33270/04191802.14.

8. Інструкція про організацію проведення негласних слідчих (розшукових) дій та використання їхніх результатів у кримінальному провадженні : затверджена наказом Генеральної про-

куратури, Міністерства внутрішніх справ України, Служби безпеки України, адміністрації Державної прикордонної служби України, Міністерства фінансів України, Міністерства юстиції України від 16.11.2012 № 114/1042/516/1199/936/1687/5. URL: https://zakon.rada.gov.ua/laws/show/v0114900-12#Text.

9. Про державну таємницю : Закон України від 21.01.1994 р. № **3855-XII.** URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text.

10. Про Положення про порядок здійснення криптографічного захисту інформації в Україні : Указ Президента України від 22 травня 1998 року № 505/98. URL: https://zakon.rada.gov.ua/laws/show/505/98#Text.

11. Про захист інформації в інформаційно-телекомунікаційних мережах : Закон України від 05.07.1994 № 80/94-ВР https://zakon.rada.gov.ua/laws/show/80/94-вр#Text.

12. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : Постанова Кабінету Міністрів України від 29 березня 2006 р. № 373. URL: https://zakon.rada.gov.ua/laws/show/373-2006-п#Text.

Лісніченко Д. В.,
кандидат юридичних наук,
доцент кафедри кримінального процесу
Одеського державного університету
внутрішніх справ

Мудрецька Г. В.,
кандидат юридичних наук,
доцент кафедри кримінального процесу
Одеського державного університету
внутрішніх справ