УДК 343.14:004
DOI https://doi.org/10.24144/2307-3322.2025.90.4.36

ОРГАНІЗАЦІЙНІ АСПЕКТИ РОБОТИ З ДОКАЗАМИ, ЩО МАЮТЬ ЕЛЕКТРОННУ ФОРМУ В КРИМІНАЛЬНОМУ ПРОЦЕСІ УКРАЇНИ

Каланча І.Г.,
кандидат юридичних наук,
начальник Новоселицького відділу
Чернівецької окружної прокуратури Чернівецької області,
доцент кафедри публічного права
факультету права та міжнародних відносин
Київського столичного університету імені Бориса Грінченка,
тренер Тренінгового центру прокурорів України
ORCID: 0000-0002-5246-7337

Каланча І.Г. Організаційні аспекти роботи з доказами, що мають електронну форму в кримінальному процесі України.

Стаття присвячена комплексному дослідженню організаційних аспектів роботи з доказами, що мають електронну форму, в кримінальному процесі України. Обґрунтовано, що організаційна готовність суб'єктів кримінального провадження до роботи з доказами, що мають електронну форму охоплює: матеріально-технічне забезпечення, кадрову спроможність та нормативне забезпечення. Встановлено, що матеріально-технічне забезпечення органів досудового розслідування, прокуратури та суду потребує покращення. Також вказано, що кадрова спроможність правоохоронних органів і суду є істотним викликом. Відсутність чітко визначених кваліфікаційних вимог до осіб, які здійснюють первинний контакт з електронними носіями інформації, дефіцит міждисциплінарних знань і навичок, а також нерівномірність підготовки між різними підрозділами створюють ризики втрати доказів або визнання їх недопустимими. Вирішення цього завдання потребує уніфікації підходів до підготовки кадрів, створення профільних підрозділів ІТ-криміналістів та впровадження міжвідомчих програм професійного навчання .Встановлено, що нормативне забезпечення роботи з доказами, що мають електронну форму, має фрагментарний характер. Досліджені в статті методичні рекомендації містять важливі положення, однак відсутній єдиний стандарт, обов'язковий для всіх органів досудового розслідування, що унеможливлює формування послідовної практики правозастосування. Автором наголошується, що особливо важливим є імплементація положень ДСТУ ISO/IEC 27037:2017 та розробка стандартних операційних процедур. Відзначається, що ефективна взаємодія між суб'єктами кримінального провадження є необхідною умовою забезпечення належної роботи з доказами, що мають електронну форму. Вказано на потребу в стандартизації підходів та розширенні практики міжвідомчої співпраці. Вказано на важливість належного зберігання доказів, що мають електронну форму, та контроль доступу до них, що потребує нормативного врегулювання та технологічного забезпечення. Вказано на часті випадки деградації електронних носіїв інформації на яких зберігаються докази досліджуваної форми, відсутність централізованих сховищ і недосконаліть механізмів розмежування повноважень створюють ризики втрати або спотворення доказів. Автором наголошується на необхідності запровадження практики резервного копіювання із застосуванням технологій гешування, впровадження практики використання надійних електронних носіїв інформації здатних забезпечити довготривале зберігання цифрових даних, створення відомчих сховищ цифрових даних.

Ключові слова: докази, що мають електронну форму; кримінальний процес; гешування; цифрова криміналістика; резервна копія; ідентифікація доказів; цілісність доказів; ДСТУ ISO/IEC 27037:2017; електронні докази; цифрові докази.

Kalancha I.G. Organizational aspects of processing digital evidence in criminal procedure of Ukraine.

The article is devoted to a comprehensive study of the organizational aspects of working with digital evidence in criminal proceedings in Ukraine. The argument is made that the organizational readiness of criminal justice actors to work with digital evidence is comprised of three elements: material and technical resources, human resources, and a regulatory framework. It has been determined that there is a necessity for enhancement of the material and technical support provided to pre-trial investigation bodies, the prosecution service and the courts. It has also been highlighted that the human resources of law enforcement agencies and the courts represent a considerable challenge. The absence of clearly defined qualification requirements for individuals engaging with electronic data storage devices, the paucity of interdisciplinary knowledge and skills, and the variability in the level of training across different units give rise to the risk of evidence being misplaced or deemed inadmissible. Addressing this issue necessitates the harmonization of training methodologies, the establishment of specialized IT forensic units, and the execution of inter-agency professional training programs. It has been determined that the regulatory framework governing the handling of digital evidence is characterized by a state of fragmentation. The methodological recommendations examined in the article contain important provisions, but there is no single standard that is mandatory for all pre-trial investigation bodies, which makes it impossible to develop consistent law enforcement practices. The author emphasizes the particular importance of implementing the provisions of DSTU (Ukrainian State Standard) ISO/IEC 27037:2017 and developing standard operating procedures. It is imperative to acknowledge that effective interaction between criminal justice actors is a prerequisite for ensuring the proper handling of digital evidence. The necessity for standardization of approaches and the augmentation of interagency cooperation practices is indicated. The importance of proper storage of digital evidence and control of access to it is noted, which requires regulatory regulation and technological support. It is imperative to acknowledge that frequent cases of degradation of electronic data storage devices on which evidence in the form under investigation is stored, the absence of centralized storage facilities and the imperfection of mechanisms for the division of powers give rise to risks of loss or distortion of evidence. The author emphasizes the need to introduce backup practices using hashing technologies, the use of reliable electronic data storage devices capable of ensuring long-term storage of digital data, and the creation of departmental digital data storage facilities.

Key words: evidence in electronic form; criminal procedure; hashing; digital forensics; backup copy; evidence identification; evidence integrity; DSTU (Ukrainian State Standard) ISO/IEC 27037:2017; electronic evidence; digital evidence.

Постановка проблеми. Стрімкий розвиток цифрових технологій зумовив не лише появу нових джерел доказової інформації, а й висунув перед суб'єктами кримінального провадження низку нових викликів, пов'язаних з ідентифікацією, збиранням, збереженням, перевіркою та оцінкою доказами, що мають електронну форму. Ефективність роботи з останніми значною мірою визначається не лише процесуальними нормами, але й організаційною спроможністю суб'єктів кримінального провадження. У цьому контексті важливою є оцінка стану організаційної готовності уповноважених органів до роботи з такими доказами, з урахуванням наявних інституційних моделей, кадрового забезпечення, матеріально-технічної бази та нормативної регламентації.

Метою цієї статті є комплексний аналіз організаційної готовності суб'єктів кримінального провадження України до роботи з доказами, що мають електронну форму, із виявленням наявних проблем матеріально-технічного, кадрового та нормативного забезпечення, а також обґрунтуванням напрямів удосконалення інституційної спроможності, стандартизації процедур та підвищення професійної компетентності для забезпечення цілісності, автентичності та допустимості таких доказів у кримінальному процесі.

Стан опрацювання проблематики. У сучасній науці кримінального процесу питання використання доказів, що мають електронну форму, активно досліджується. У колективній монографії під ред. В.А. Колесника (2024) систематизовано доктринальні підходи та окреслено потребу належного правового регулювання процедур їх збирання й оцінки [9]. Значний вплив на практику здійснили методичні рекомендації, які закріпили положення ДСТУ ISO/IEC 27037:2017, хоча й залишили низку дискусійних питань [4; 5], а також містять практичні аспекти доступу до електронних носіїв інформації [6]. А.М. Гаркуша зосереджує увагу на питаннях допустимості та до-

стовірності резервних копій комп'ютерних даних, наголошуючи на ролі гешування [7]. Організаційні проблеми роботи з такими доказами розглядалися у спільній роботі А.М. Гаркуші та автора (2021) [8], а також у соціологічних дослідженнях автора (2025), яке засвідчило наявність міжвідомчого дисбалансу в досліджуваній сфері [10]. Важливо вказати на дослідження Торбаса О.О. [12] щодо використання OSINT при розслідуванні кримінальних правопорушень. Таким чином, хоча науковий інтерес до проблематики є значним, організаційні аспекти роботи з доказами, що мають електронну форму, досі залишаються фрагментарно висвітленими у вітчизняній науці, а відтак потребують комплексного аналізу.

Виклад основного матеріалу. Організаційна готовність суб'єктів кримінального провадження до роботи з доказами, що мають електронну форму, є важливим чинником ефективності процесу їх ідентифікації, збирання, здобуття, збереження, дослідження, аналізу та представлення.

Першим аспектом досліджуваного питання є *матеріально-технічне забезпечення суб'єктів кримінального провадження, наявність спеціалізованого обладнання та належної інфраструктури*. Насамперед, йдеться про забезпечення органів досудового розслідування цифровими криміналістичними інструментами, що дозволяють здійснювати роботу з доказами, що мають електронну форму, відповідно до міжнародних стандартів. До таких належать пристрої write-blocker (апаратні засоби блокування запису), forensic workstations (криміналістичні робочі станції), програмне забезпечення для створення та аналізу криміналістичних образів (FTK, EnCase, X-Ways Forensics), системи гешування та перевірки цілісності даних. Наявність у органів досудового розслідування відповідних технічних та програмних засобів для роботи з доказами, що мають електронну форму є критично необхідною умовою здійснення результативних слідчих (розшукових) дій.

Наприклад, важливим чинником, що ускладнює ефективну роботу з доказами, що мають електронну форму, є її нестабільний, динамічний характер. Частина цифрових слідів існує лише упродовж обмеженого проміжку часу та може зникнути ще до того, як слідчий отримає необхідну процесуальну передумову – ухвалу слідчого судді на проведення тимчасового доступу до речей і документів або обшуку. Саме тому сучасна практика роботи з електронною інформацією дедалі більше потребує технологій негайного реагування, здатних фіксувати швидкоплинні прояви цифрової активності.

Другою складовою організаційної готовності суб'єктів кримінального провадження до роботи з доказами, що мають електронну форму є *кадрова спроможність органів досудового розслідування, прокуратури, суду та інших учасників кримінального провадження з числа державного сектору*.

Кадрове забезпечення роботи з доказами досліджуваної категорії, виступає одним із ключових елементів ефективності досудового розслідування у цифровому середовищі. Специфіка таких доказів обумовлює потребу у міждисциплінарній компетенції осіб, які залучаються до роботи з ними. До цього кола належать оперативні працівники, слідчі, детективи, прокурори, спеціалісти, експерти та навіть судді.

Одним із системних викликів для ефективного кримінального провадження, пов'язаного з використанням доказів, що мають електронну форму, є істотний дефіцит фахових знань у суб'єктів кримінального провадження. Відсутність належного рівня спеціалізованої підготовки у сфері цифрових технологій безпосередньо впливає на здатність ідентифікувати, вилучати, аналізувати й правильно інтерпретувати цифрову інформацію під час кримінального провадження.

Певна частина слідчих, прокурорів та суддів не володіє знаннями щодо технічних та процесуальних аспектів подолання логічного захисту, таких як дешифрування, доступ до хмарних ресурсів, робота з віртуальними середовищами, застосування спеціалізованого програмного забезпечення. Це нерідко призводить до порушення процедури вилучення й зберігання даних, прийняття помилкових процесуальних рішень, що в подальшому може вплинути на допустимість відповідного доказу**.** Також, технічна необізнаність суб'єктів кримінального провадження потенційно є фактором недооцінки або переоцінки доказу, що може мати суттєві негативні наслідки для кримінального провадження.

Як на рівні КПК України, так і підзаконних нормативно-правових актів фактично не встановлено уніфікованих кваліфікаційних вимог до осіб, що здійснюють первинний контакт з електронними носіями інформації, зокрема під час обшуку або тимчасового доступу. Це створює ризики неналежної фіксації цифрових даних, втрати або спотворення їх змісту, що, у свою чергу, може

призвести до визнання доказу недопустимим. Брак профільної підготовки, сертифікацій або програм підвищення кваліфікації суб'єктів, які фактично залучаються до роботи з доказами, що мають електронну форму, залишається однією з суттєвих прогалин у кадровій політиці більшості органів досудового розслідування.

Додатково спостерігається суттєвий дисбаланс у професійному рівні та технічній підготовленості між підрозділами різних відомств: тоді як окремі спеціалізовані підрозділи Національного антикорупційного бюро України (далі – НАБУ), Кіберполіції та Служби безпеки України демонструють високий рівень компетентності, регіональні слідчі підрозділи деяких органів досудового розслідування (далі – ОДР) часто не мають елементарної експертизи чи кадрового ресурсу для роботи з доказами досліджуваної форми.

Очевидною є проблема навіть на рівні практики вилучення електронних носіїв інформації, яка суттєво різниться у різних органів досудового розслідування та навіть регіональних «традицій», обумовлених позиціями апеляційних судів відповідних областей. Уніфікація кваліфікаційної підготовки представників ОДР та прокурорів до роботи з доказами, що мають електронну форму відповідно до вимог ДСТУ ISO/IEC 27037:2017 (ISO/IEC 27037:2012, IDT) «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів» [2] є очевидною та навіть перестиглою з огляду на час запровадження цього стандарту – з січня 2019 року.

Ще одним з надзвичайно актуальних на сьогодні питань для кадрового забезпечення ОДР є підготовка фахівців з розвідки на основі відкритих джерел або ж Open Source Intelligence (далі – OSINT) [11; 12]. В умовах цифрової трансформації джерел інформації інструменти OSINT набувають дедалі більшого значення в діяльності органів досудового розслідування. OSINT дозволяє оперативно отримувати інформацію з відкритих джерел, зокрема соціальних мереж, інтернет-форумів, публічних баз даних, ЗМІ, сервісів архівування веб-сторінок, доменних реєстрів тощо. Ефективна робота з відповідними інструментами вимагає системного навчання та постійного підвищення кваліфікації. В цьому напрямі важливим є також впровадження стандартів Протоколу Берклі в роботу ОДР, що передбачає відповідну підготовку працівників.

Відтак, уніфікація підходів до кадрового забезпечення, таких як створення спеціалізованих структурних підрозділів (наприклад, криміналістичних лабораторій), міжвідомчого переліку профільних посад і кваліфікаційних вимог до суб'єктів кримінального провадження, які взаємодіють з доказами, що мають електронну форму (наприклад, внутрішньовідомча сертифікація) видається нагальною потребою для забезпечення адекватної роботи суб'єктів кримінального провадження в досліджуваній сфері.

Вже сьогодні недоліки кадрової спроможності можливо компенсувати шляхом створення сталої інституційної системи підготовки, підвищення кваліфікації та сертифікації суб'єктів кримінального провадження, які залучені до роботи з доказами, що мають електронну форму.

Одним з ключових напрямів удосконалення є розробка та впровадження міжвідомчих програм професійного навчання, орієнтованих на цифрову криміналістику, з урахуванням специфіки кримінального процесуального законодавства України, міжнародних стандартів, а також галузевих особливостей (наприклад, щодо кіберзлочинів, торгівлі людьми, воєнних злочинів тощо). Відповідні тренінгові програми мають передбачати як теоретичну частину, так і практичні модулі з роботи з цифровими носіями інформації, застосування спеціалізованого програмного забезпечення, документування процесуальних дій з дотриманням вимог щодо забезпечення цілісності доказів, що мають електронну форму.

Окремої уваги заслуговує потреба в інтеграції цифрової грамотності до освітніх програм юридичних та правоохоронних вишів, що забезпечить формування первинної компетентності майбутніх фахівців щодо доказів, що мають електронну форму, їх властивостей та правового статусу в межах кримінального процесу.

Третьою складовою організаційної готовності суб'єктів кримінального провадження є *наявність нормативної основи* (норми кримінального процесуального законодавства, закони та підзаконні нормативно-правові акти, відомчі інструкції та регламенти тощо) *щодо роботи під час кримінального провадження з доказами, що мають електронну форму*.

Важко переоцінити необхідність забезпечення належного правового регулювання питання доказів, що мають електронну форму в КПК України. У межах діяльності окремих відомств (зокрема НАБУ) існують внутрішні інструкції, що регламентують алгоритми дій при роботі з цифро-

вими носіями та комп'ютерними даними. Ці документи, як правило, мають обмежений доступ і застосовуються в межах певного відомства.

Однак ключовою проблемою є відсутність єдиних для всіх органів досудового розслідування уніфікованих стандартів, який регламентував би мінімально необхідні вимоги до дій усіх правоохоронних органів під час роботи з доказами, що мають електронну форму та який би був визначений як обов'язковий до використання. Така фрагментарність регламентації унеможливлює формування єдиної практики правозастосування.

На сьогодні одним із ключових шляхів методологічного забезпечення суб'єктів кримінального провадження в досліджуваному напрямі є методичні рекомендації, що потребують подальшого аналізу. Наприклад, методичні рекомендації «Використання електронних носіїв інформації з медіа-контентом у якості джерел доказів» (2019) висвітлюють поняття та види електронних носіїв інформації, тактичні особливості отримання доступу до електронних носіїв інформації, порядок пошуку власника Інтернет-сторінки, особливості призначення експертиз носіїв інформації та інші питання [6]. Варто вказати на методичні рекомендації «Використання електронних (цифрових) доказів у кримінальних провадженнях» (2017) [4] та їх друге видання (2020) [5], що в питаннях окремих процесуальних і технічних рекомендацій є досить спірними, однак містять в повному обсязі ДСТУ ISO/IEC 27037:2017 (ISO/IEC 27037:2012, IDT) «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів» [2], отримання якого зазвичай є утрудненим (потребує придбання в ДП «УкрНДНЦ» або ж безкоштовного отримання правоохоронними органом за запитом), адже є об'єктом авторського права. Також вартим уваги є Збірка навчальних матеріалів тренінгу для суддів «Застосування електронних доказів під час розгляду справ, пов'язаних з корупцією» (2019) [3], що містить цікаві матеріали щодо технічної природи доказів, що мають електронну форму (принципи функціонування мережі Інтернет, телефон як доказ, судова експертиза доказів, що мають електронну форму, способи виявлення прихованих файлів, технічні особливості криптовалюти тощо).

Додатково варто зазначити, що більшість відомчих матеріалів лише точково регулюють питання роботи з певним видом пристроїв або стосуються специфічних ситуацій та лише частково враховують положення ДСТУ ISO/IEC 27037:2017 або Протоколу Берклі.

На нашу думку, використання розрізнених методичних рекомендацій як інструменту вдосконалення знань суб'єктів кримінального провадження щодо роботи з доказами, що мають електронну форму, під час кримінального провадження є неефективним з огляду на відсутність єдиного теоретичного розуміння окресленої теми та узгодженого підходу до їх процесуальної оцінки. Враховуючи зазначене, перспективним напрямом досліджуваного аспекту є розробка та впровадження єдиних для всіх суб'єктів кримінального провадження стандартних операційних процедур щодо роботи з доказами досліджуваної категорії.

Досліджена попередньо організаційна готовність суб'єктів кримінального провадження до роботи з доказами, що мають електронну форму передбачає забезпечення рівних матеріально-технічних можливостей, наявності спеціалізованих підрозділів та фахових кадрів у їх структурі (для забезпечення фахової комунікації) а також застосування спільних для всіх, науково обґрунтованих та технологічно оптимізованих, підходів до роботи. Все це є передумовою для *ефективної взаємодії між суб'єктами кримінального провадження* під час роботи з доказами, що мають електронну форму. На сьогодні це питання є малодослідженим та залишається дискусійним, що обумовимо необхідність звернутися до самих суб'єктів правозастосування для з'ясування їх думки з відповідних питань.

Для з'ясування рівня взаємодії між суб'єктами правозастосування щодо пошуку доказів, що мають електронну форму автором проведено опитування під час якого респондентам поставлено запитання «Чи виникає у Вашій роботі необхідність звертатись до колег для пошуку доказів, що мають електронну форму?» та запропоновано надати розгорнуті відповіді. 54% респондентів вказують, що не мають такої потреби, 37% вказують на необхідність звертатись до колег для пошуку доказів, що мають електронну форму, з них 3% додатково конкретизують, що звертаються для цього до спеціалістів. Ще 7% вказують, що звертаються до працівників підрозділів кіберполіції. Також до 2% респондентів (19 осіб) всі з яких є працівниками кіберполіції вказують, що вони і є тими колегами до яких звертаються за допомогою в пошуку доказів, що мають електронну форму. З огляду на те, що 37% респондентів вказують на необхідність звертатись до колег для пошуку доказів, що мають електронну форму (більше 2/3 з цих 37% є прокурорами), така потреба вимагає

вирішення або шляхом створення й розширенням штатів профільних спеціалістів, або ж шляхом навчання прокурорів самостійно шукати та фіксувати докази досліджуваної категорії [10].

Позитивним прикладом ефективної організації роботи з доказами, що мають електронну форму під час кримінального провадження є досвід НАБУ в частині створення в своїй структурі криміналістичної лабораторії зі штатом відомчих спеціалістів, які організаційно не підпорядковані керівнику органу досудового розслідування, є процесуально незалежними та можуть залучатися до слідчих дій для реалізації процедур, визначених ДСТУ ISO/IEC 27037:2017.

З урахуванням проведеного нами попереднє дослідження [8, с. 72–75], варто наголосити, що ефективне проведення досудового розслідування значної частини кримінальних правопорушень потребує залучення ІТ-криміналістів як спеціалістів (в порядку ст. 71 КПК України). Процесуальні традиції та звичаї в частині роботи з доказами, що мають електронну форму доцільно переосмислити, залучаючи експертів лише щодо складних питань, що вимагають відповідного висновку. Саме так зроблено, наприклад, в Німеччині, де компетенція ІТ-криміналістів та ІТ-експертів розділені, де спеціалісти ІТ-криміналісти функціонально наближені до слідчих підрозділів, як це відтворено у випадку НАБУ [8, с. 75]. Враховуючи зазначене, варто розглянути можливість створення в структурі всіх правоохоронних органів підрозділів ІТ-криміналістів, що зможуть забезпечити ефективну роботу з доказами, що мають електронну форму під час кримінального провадження.

Поряд з організаційною готовністю системи кримінальної юстиції до ефективної роботи з доказами, що мають електронну форму надзвичайно актуальним є питання ***зберігання доказів****, що мають електронну форму та контролю доступу до них.*

Зберігання електронних носіїв інформації у межах кримінального провадження вимагає дотримання суворих технічних параметрів, що забезпечують збереження їх цілісності та автентичності інформації. Цей процес охоплює як фізичне зберігання електронних носіїв інформації, так і створення та архівацію криміналістичних образів (побітових копій), резервних копій, вимоги до транспортування тощо. З огляду на високу чутливість цифрових даних до зовнішніх чинників, одним із ключових технічних аспектів є забезпечення контрольованого середовища з регульованими температурними і показниками вологості, ізоляцією від електромагнітного випромінювання та захистом від механічного або статичного ураження.

Технічні вимоги до зберігання електронних носіїв інформації під час кримінального провадження на разі законодавцем не встановлені. Водночас, окремі аспекти визначено в ДСТУ ISO/IEC 27037:2017. Національні нормативно-правові акти та методичні рекомендації наразі не охоплюють у повному обсязі всі аспекти поводження з доказами, шо мають електронну форму, що створює потребу в розробці цього питання в межах пропонованих нами стандартних операційних процедур.

У зв’язку з актуальними викликами, зокрема загрозами кібератак та ризиками втрати інформації через технічні збої, особливої ваги набуває ідея створення централізованого відомчого віртуального сховища для резервного зберігання доказів, що мають електронну форму. Таке сховище має бути ізольованим від загальних мереж, підтримувати систему регулярного бекапування, а також передбачати можливість довготривалого зберігання інформації на стрічкових носіях (tape storage), які мають підвищений захист від логічного знищення або шифрування у разі зовнішнього втручання. Реалізація такої моделі підвищила б рівень цифрової безпеки кримінального провадження в умовах гібридних загроз і сприяла б формуванню єдиної системи роботи з доказами, що мають електронну форму.

Водночас вже сьогодні актуалізується питання деградації електронних носіїв інформації, що використовуються для зберігання доказів, що мають електронну форму під час кримінального провадження, що створює загрозу їх цілісності.

Фізична та логічна деградація носіїв даних є однією з малодосліджених, проте критично важливих загроз для цілісності а відтак і доказової цінності цифрової інформації під час кримінального провадження. На відміну від традиційних матеріальних носіїв (паперу чи фізичних предметів), цифрові носії інформації схильні до руйнування їх фізичного середовища з плином часу, технічної нестабільності та деградації, що може спричинити часткову або повну втрату інформації навіть без зовнішнього впливу.

У відповідь на ці загрози актуальним є впровадження носіїв, орієнтованих на довготривале зберігання: спеціалізовані SSD з низьким рівнем зношення, WORM-системи, які не допускають

перезапису, а також «холодне» архівування – зберігання носіїв у контрольованому середовищі з обмеженим доступом і періодичним дублюванням вмісту. Застосування подібних носіїв може бути виправданим у випадках, коли цифрова інформація повинна зберігатися багато років до моменту її дослідження у суді.

Однак на сьогодні величезна кількість доказів, що мають електронну форму зберігається на електронних носіях інформації у формі флеш-накопичувачів (USB, SD-карти), що мають високі ризики деградації даних та втрати доказу. Вказане потребує вжиття від держателя цього доказу (слідчого, прокурора, судді тощо) заходів щодо збереження цілісності даних та можливості їх подальшого використання під час кримінального провадження. Відповіддю не цей виклик є запровадження сталої практики виготовлення резервних копій доказів, що мають електронну форму.

Вказане питання детально досліджено Гаркушею А.М., з доводами якого варто погодитись. Вчений вказує, що законодавство передбачає можливість створення та зберігання резервних копій технічних носіїв інформації, на яких зафіксовано процесуальні дії, з метою забезпечення надання доказів у разі втрати чи пошкодження оригіналів. КПК України не встановлює детального порядку їх формування, однак на практиці копіювання комп'ютерних даних здійснюється на електронні носії великої ємності або у централізовані сховища. Протокол процесуальної дії має містити спосіб ідентифікації копій, найчастіше – гешування (MD5, SHA1, SHA256) чи електронний підпис, а також відповідні геш-коди як унікальні значення, що підтверджують тотожність даних. Допустимість таких копій визначається ч. 3, ч. 4 та п. 1 ч. 5 ст. 99 КПК України залежно від обставин їх створення. У разі оспорення достовірності копій їх цілісність підтверджується шляхом порівняння геш-кодів, зафіксованих під час створення резервного носія, із геш-кодами, обчисленими під час перевірки [7, с. 43-47].

Наступним важливим аспектом досліджуваного нами питання зберігання доказів є *контроль доступу до доказів, що мають електронну форму*. Правове регулювання цього процесу вимагає чіткого розмежування повноважень суб'єктів кримінального процесу, забезпечення технічної захищеності інформації.

Розмежування доступу здійснюється відповідно до процесуальних ролей. Слідчий, як ініціатор слідчих дій, відповідає за тимчасове зберігання електронних носіїв інформації та організацію доступу до інформації. Його завдання полягає не лише у виявленні та вилученні електронних носіїв інформації, а й у забезпеченні їх безпечного функціонального обігу. Прокурор виконує контрольну функцію, приймаючи рішення щодо правомірності та необхідності доступу до інформації, у тому числі оцінюючи обсяг і межі втручання в особисту сферу. Захисник реалізує право на ознайомлення із зібраними доказами відповідно до ст. 290 КПК України, однак таке ознайомлення не повинно ставити під загрозу конфіденційність персональної інформації інших осіб, що міститься на носіях, які вилучені під час кримінального провадження. У цьому контексті особливе значення має чітке визначення обсягу доступної інформації. Експерт або технічний спеціаліст отримує доступ до цифрової інформації або до електронних носіїв інформації виключно в межах наданого процесуального доручення (ухвали суду або постанови прокурора чи слідчого) і не має права виходити за межі завдання, визначеного для проведення експертного дослідження.

В цьому аспекті актуальними є різновиди сучасних програмних рішень, що містять інтегровані алгоритми chain of custody. Такі технічні засоби контролю мають відповідати сучасним стандартам інформаційної безпеки. З огляду на викладене, перспективним напрямом є запровадження уніфікованої цифрової платформи для забезпечення контролю доступу до доказів, що мають електронну форму. Така платформа має базуватись на цифровій ідентифікації учасників провадження, з обов'язковим журналюванням усіх взаємодій з доказом. Централізована система управління доступом із можливістю призначення ролей та рівнів дозволів, а також обов'язковий аудит усіх взаємодій з доказами в рамках chain of custody, дозволить мінімізувати ризики фальсифікації та забезпечити дотримання принципу належної правової процедури. Запровадження таких технічних і організаційних рішень потребує відповідного процесуального оформлення та нормативного закріплення.

Ще одним важливим питанням, що пов'язане з контролем доступу до доказів але перебуває в етичній площині, є *обмеження доступу до інформації, що міститься на носіях, які вилучені під час кримінального провадження, однак не має доказового значення та належить до персональної інформації інших осіб***.**

У процесі роботи з доказами, що мають електронну форму, особливого значення набуває проблема доступу до інформації, яка не має безпосереднього доказового значення, але міститься на носіях або у цифрових облікових записах, до яких здійснюється доступ під час кримінального провадження. Йдеться, передусім, про чутливу інформацію: особисте листування, приватні фотографії, відеозаписи, медичні або фінансові дані, а також відомості, що становлять комерційну таємницю третіх осіб. У певних випадках така інформація не пов'язана з обставинами кримінального правопорушення, однак через технологічну невіддільність від пристрою, що, наприклад, вилучений під час обшуку, вона виявляється доступною як для сторони обвинувачення, так і для сторони захисту під відкриття матеріалів досудового розслідування.

Правова конструкція, передбачена ст. 290 КПК України, покладає на сторону обвинувачення обов'язок надати іншій стороні доступ до всіх матеріалів досудового розслідування, у тому числі до копій документів – сюди ж належать всі комп'ютерні дані, всі відомості з вилучених електронних носіїв інформації та виготовлені копії цифрових даних з пристроїв, що оглядалися. Водночас чинне законодавство не містить механізму обмеження доступу до інформації, що була виявлена та збережена, але не включена до переліку доказів у провадженні. Це створює потенційну загрозу порушення права на повагу до приватного життя, особливо у випадках, коли відомості про інтимне, особисте або конфіденційне передаються на носіях у межах відкриття матеріалів стороною обвинувачення.

Таким чином, процесуальне регулювання доступу до інформації, що не має доказового значення, повинно бути уточнене із урахуванням вимог пропорційності, мінімізації втручання та спеціального режиму обробки чутливих персональних даних, вилучених у межах кримінального провадження.

Висновок. Комплексний аналіз організаційних аспектів роботи з доказами, що мають електронну форму, у кримінальному процесі України дозволяє сформулювати такі узагальнення.

1. Організаційна готовність суб'єктів кримінального провадження до роботи з доказами, що мають електронну форму охоплює кілька ключових складових:

а) матеріально-технічне забезпечення органів досудового розслідування, прокуратури та суду потребує покращення. Відсутність спеціалізованого обладнання й програмного забезпечення, а також нерівномірний рівень оснащеності різних відомств істотно ускладнює ідентифікацію, вилучення та дослідження доказів, що мають електронну форму;

б) кадрова спроможність правоохоронних органів і суду є істотним викликом. Відсутність чітко визначених кваліфікаційних вимог до осіб, які здійснюють первинний контакт з електронними носіями інформації, дефіцит міждисциплінарних знань і навичок, а також нерівномірність підготовки між різними підрозділами створюють ризики втрати доказів або визнання їх недопустимими. Вирішення цього завдання потребує уніфікації підходів до підготовки кадрів, створення профільних підрозділів IT-криміналістів та впровадження міжвідомчих програм професійного навчання;

в) нормативне забезпечення роботи з доказами, що мають електронну форму, має фрагментарний характер. Хоча окремі методичні рекомендації та внутрішньовідомчі інструкції містять важливі положення, відсутність єдиного загальнообов'язкового стандарту для всіх органів досудового розслідування унеможливлює формування послідовної практики правозастосування. У цьому контексті особливого значення набуває імплементація положень ДСТУ ISO/IEC 27037:2017 та розробка стандартних операційних процедур.

2. Ефективна взаємодія між суб'єктами кримінального провадження є необхідною умовою забезпечення належної роботи з доказами, що мають електронну форму. Вона передбачає узгодженість у процесуальних діях, обмін знаннями та ресурсами, залучення спеціалістів і створення сталих каналів комунікації між слідчими, прокурорами, спеціалістами, експертами та судом. Соціологічні дослідження підтверджують наявність міжвідомчого дисбалансу, що обумовлює потребу у стандартизації підходів та розширенні практики міжвідомчої співпраці.

3. Зберігання доказів, що мають електронну форму, та контроль доступу до них потребує нормативного врегулювання та технологічного забезпечення. Деградація електронних носіїв інформації на яких зберігаються докази досліджуваної форми, відсутність централізованих сховищ і недосконаліть механізмів розмежування повноважень створюють ризики втрати або спотворення доказів. Необхідним є запровадження практики резервного копіювання із застосуванням технологій гешування, впровадження практики використання надійних електронних носіїв інфор-

мації здатних забезпечити довготривале зберігання цифрових даних, створення відомчих сховищ цифрових даних, інтегрованих у систему контролю доступу з обов'язковим журналюванням усіх дій відповідно до принципів chain of custody.

Таким чином, підвищення організаційної спроможності суб'єктів кримінального провадження у сфері роботи з доказами, що мають електронну форму, потребує комплексних заходів у трьох взаємопов'язаних напрямах — матеріально-технічному, кадровому та нормативному забезпеченні, поглибленні взаємодії між суб'єктами кримінального провадження а також запровадженні сучасних стандартів зберігання й контролю доступу до доказів. Це дозволить гарантувати їх цілісність, автентичність і допустимість, що безпосередньо вплине на ефективність кримінального провадження загалом.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Кримінальний процесуальний кодекс України: Закон України від 13 квітня 2012 року № 4651-VI (зі змін. і доп.). URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text.
2. ДСТУ ISO/IEC 27037:2017 Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів (ISO/IEC 27037:2012, IDT). Київ, ДП «УкрДНЦ», 2018. 31 с.
3. Браун С., Овсянніков В.С., Шинкоренко С.В. Застосування електронних доказів під час розгляду справ, пов'язаних з корупцією. Збірка навчальних матеріалів тренінгу для суддів. 2019. 138 с.
4. Використання електронних (цифрових) доказів у кримінальних провадженнях: метод. рек. / М.В. Гребенюк, В.Д. Гавловський, М.В. Гуцалюк, В.Г. Хахановський та ін.; за заг. ред. М.В. Гребенюка. Київ: МНДЦ при РНБО України, 2017. 76 с.
5. Використання електронних (цифрових) доказів у кримінальних провадженнях: метод. реком. / М.В. Гуцалюк, В.Д. Гавловський, В.Г. Хахановський та ін.; за заг. ред. О.В. Корнейка. Вид. 2-ге, доп. Київ: Вид-во Нац. акад. внутр. справ, 2020. 104 с.
6. Використання електронних носіїв інформації з медіа-контентом у якості джерел доказів: методичні рекомендації / Авт. колектив: А.В. Захарко, А.Г. Гаркуша, В.В. Рогальська, І.В. Краснобрижий, О.В. Брягін. Дніпро: Дніпропетровський державний університет внутрішніх справ, 2019. 73 с.
7. Гаркуша А.М. Допустимість і достовірність резервних копій комп'ютерних даних. *ІІІ Наукові читання пам'яті Ганса Гросса*: збірник тез міжнародної науковопрактичної конференції (м. Чернівці, 08 грудня 2023 р.). Чернівці: Чернівец. нац. унт. ім. Ю. Федьковича, 2023. С. 43–47.
8. Гаркуша А.М., Каланча І.Г. Виявлення та фіксація доказів, що мають електронну форму під час кримінального провадження: організаційні аспекти. Наукові читання пам'яті Ганса Гросса: збірник тез міжнародної науково-практичної конференції (м. Чернівці, 09 грудня 2021 р.). Чернівецький національний університет імені Юрія Федьковича. Чернівці: Технодрук, С. 72–75.
9. Електронні докази у кримінальному провадженні: поняття, збирання, використання в доказуванні: монографія / І.В. Гора, В.А. Колесник, В.В. Малюк, В.О. Ходанович, А.М. Черняк, Л.І. Щербина; за заг. ред. В.А. Колесника. Київ: 7БЦ, 2024. 484 с.
10. Каланча І.Г. Практика роботи з доказами, що мають електронну форму в кримінальному процесі України: соціологічне дослідження. *Успіхи і досягнення у науці*. № 1 (11). 2025.
11. Каланча І.Г. Результати OSINT як джерело доказів у кримінальному процесі України. Інновації, виклики та нові горизонти правового регулювання у світлі сучасних соціально-економічних та політичних трансформацій: Матеріали Всеукр. наук.-практ. конф. (м. Чернівці, 20 грудня 2024 р.) / відп. ред. К.А. Вознякovська. ТОМ 1, Чернівці, 2024. С. 43–49.
12. Торбас О.О. OSINT при розслідуванні кримінальних правопорушень: підручник. Одеса: Видавництво «Юридика», 2024. 180 с.