УДК 343.13:004.6
DOI https://doi.org/10.32782/2524-0374/2021-8/77

КОПІЯ ЕЛЕКТРОННОЇ ІНФОРМАЦІЇ ЯК ДОКАЗ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ: ПРОЦЕСУАЛЬНИЙ ТА ТЕХНІЧНИЙ АСПЕКТИ

COPY OF ELECTRONIC INFORMATION AS EVIDENCE IN CRIMINAL PROCEEDINGS: PROCEDURAL AND TECHNICAL ASPECTS

Каланча І.Г., к.ю.н., прокурор,
Чернівецька окружна прокуратура Чернівецької області,
асистент кафедри процесуального права
Чернівецький національний університет імені Юрія Федьковича

Гаркуша А.М., начальник відділу детективів кримінальної лабораторії
Управління аналітики та обробки інформації Національного антикорупційного бюро України

Стаття присвячена висвітленню технічних та юридичних аспектів копії електронної інформації як доказу в кримінальному провадженні. Проаналізовано кримінальну процесуальну процедуру збирання інформації, що міститься в електронному носії інформації як доказу в кримінальному провадження шляхом виготовлення копії такої інформації. Проаналізовано процесуальну форму збирання доказів, які мають електронну форму, шляхом копіювання інформації, що виражено у формулі: «копія інформації × (слідчий або прокурор + спеціаліст) = оригінал документа». Вказано, що, з огляду на норми ч. 4 ст. 99 Кримінального процесуального кодексу України, копія електронної інформації є документом у контексті ч. 2 ст. 84 Кримінального процесуального кодексу України. Авторами розроблено систему процесуальних сценаріїв, що передбачають необхідність виготовлення копії інформації. Проаналізовано технічний аспект процесу копіювання інформації та вказано на важливість уникнення слідчими, прокурорами помилок щодо диференціації процесів виготовлення фізичної копії (образу) електронного носія інформації та копії окремого електронного файлу. Наголошено на доцільності застосування ДСТУ ISO/IEC 27037:2017 (ISO/IEC 27037:2012, IDT) «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів» під час кримінального провадження. У роботі запропоновано низку адміністративних та організаційних заходів, спрямованих на розширення практики використання копії електронної інформації як доказу в кримінальному провадженні. Авторами вказано на необхідність внесення змін до ч. 4 ст. 99 Кримінального процесуального кодексу України щодо доповнення нормою про обов'язок спеціалістом підтвердження цілісності та справжності скопійованих даних.
Ключові слова: докази, електронна інформація, копія, носії інформації, гешування.

The article is devoted to technical and procedural sides of a digital evidence copy as evidence in criminal investigations. In this research, a review was conducted on how information stored on digital media is collected as evidence through an acquisition process according to the rules of the Criminal Procedure Code of Ukraine. Also, a review was conducted on procedural prescriptions that should be followed during the process of creating a digital evidence copy. The process can be expressed as a formula: "information copy × (case investigator OR prosecutor AND specialist) = document original". The paper points out that according to the provision of part 4 article 99 of the Criminal Procedure Code of Ukraine a digital evidence copy falls under the category of a document as a source of evidence as mentioned in part 2 article 84 of the Criminal Procedure Code of Ukraine. Authors developed a set of plans which foresees a need to perform digital evidence acquisition. This work also describes the technical side of digital evidence acquisition. It is outlined that an investigator or a prosecutor should be aware of the difference between bitwise copy (physical copy) and a copy of single files. It is mentioned that the standard DSTU ISO/IEC 27037:2017 (ISO/IEC 27037:2012, IDT) Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence is worth to apply as a practical guideline in investigations. The work offered administrative and organization measures aimed at extending the practice of using a digital evidence copy as evidence. The authors pointed out the need for amending part 4 article 99 of the Criminal Procedure Code of Ukraine concerning the obligation of a specialist to verify a digital evidence copy.
Key words: digital evidence, information stored electronically, digital media, digital evidence copy, hash function.

Постановка проблеми. У сучасних умовах широкого застосування інформаційних технологій електронні носії інформації (далі – ЕНІ) потенційно є важливим та інформативним джерелом доказів у кримінальному провадженні. Фізичне вилучення ЕНІ не завжди є процесуально або технічно можливим, тому копіювання вбачається ефективним способом отримання доказів з відповідного електронного носія. Водночас, з огляду на недоліки кримінального процесуального закону, неоднорідну практику правозастосування та відсутність спеціальних знань у сфері інформаційних технологій, значна частина слідчих та прокурорів не завжди в змозі організувати правильне виготовлення копії електронної інформації, що призводить до втрати доказів (через невміння їх збирати та зберігати) або визнання зібраних доказів недопустимими (через порушення процесуальних та технічних норм).

Аналіз останніх досліджень і публікацій. Незважаючи на широкий інтерес науковців до доказів, що мають електронну форму, специфіки їх відшукання, збирання і застосування, відсутні системні наукові дослідження правової природи копії електронної інформації як доказу в кримінальному провадженні. Окремі питання досліджували Ю.Ю. Орлов, С.С. Чернявський (2017) [7], Є.С. Хижняк (2017) [9], О.П. Метелев (2019) [6], А.В. Столітній, І.Г. Каланча (2019) [8] та інші. У цьому напрямі варто зазначити окремі навчальні матеріали для поліцейських (2019; 2020) [10; 11], адвокатів (2020) [5] та суддів (2019) [12], що, однак, частково є недосконалими щодо технічних аспектів роботи з доказами, що мають електронну форму. З приводу збирання доказів в електронній формі висловлювалися Я. Вебер та З. Смутни (2015) [14]. Також варто зазначити роботу «Електронні докази та електронні підписи» (2021) за редакцією С. Мейсона та Д. Сенга [15], що становить значний науковий та практичний інтерес.

Мета статті. Метою роботи є формулювання процесуальних та технічних аспектів створення копії електронної інформації як доказу в кримінальному провадженні.

Виклад основного матеріалу. У процесі виявлення під час слідчих (розшукових) дій ЕНІ збирання інформації, що міститься на них, як доказів може здійснюватися двома способами: вилученням носія або інформаційної системи, до якого він входить, або копіюванням інформації, що зберігається на відповідному ЕНІ. Кожен із цих способів має власні переваги, недоліки та обмеження.

Вилучення як класичний спосіб збирання доказів у формі матеріальних об'єктів, до яких належать ЕНІ

та інформаційні системи, попри всі очевидні переваги, має низку недоліків. Зокрема, це стосується випадків неможливості вилучення або неефективності дослідження ЕНІ після вилучення у разі загрози зупинення критично важливих функцій бізнес-процесів або наявності шифрування тощо.

Альтернативою є збирання інформації, що міститься в ЕНІ, як доказу в кримінальному провадженні шляхом виготовлення копії такої інформації. Відповідна процесуальна процедура з'явилась у Кримінальному процесуальному кодексі України (далі – КПК України) лише в 2017 році [1, с. 1] та складається з таких компонентів:

– встановлення загальної заборони на тимчасове вилучення електронних інформаційних систем або їх частин (комп'ютерів – *прим. авт.*), мобільних терміналів систем зв'язку (телефонів – *прим. авт.*) із вичерпним переліком виключень (абз. 3 ч. 2 ст. 168 КПК України);

– передбачення права слідчого, прокурора здійснювати із залученням спеціаліста копіювання інформації, що міститься в інформаційних (автоматизованих) системах, телекомунікаційних системах, інформаційно-телекомунікаційних системах, їх невід'ємних частинах під час проведення огляду, обшуку (абз. 4 ч. 2 ст. 168 КПК України);

– визнання копії інформації, що міститься в інформаційних (автоматизованих) системах, телекомунікаційних системах, інформаційно-телекомунікаційних системах, їх невід'ємних частинах, виготовленої слідчим, прокурором із залученням спеціаліста як оригіналу документа (ч. 4 ст. 99 КПК України).

Логіку законодавця можемо прослідкувати за пояснювальною запискою до законопроєкту, де метою таких змін вказано захист учасників кримінального провадження від необґрунтованого вилучення документів та комп'ютерної техніки та захист інтересів суб'єктів господарювання, які потерпають від фактичного блокування своєї діяльності внаслідок необґрунтованого вилучення комп'ютерної техніки та серверного обладнання в рамках кримінального провадження [13, с. 2–3].

Таким чином, у КПК України з'явився альтернативний спосіб збирання інформації, що має електронну форму, – **збирання доказів, що мають електронну форму шляхом копіювання інформації**, для якого передбачено процесуальну форму, що можна представити як формулу*:* ***«копія інформації × (слідчий або прокурор + спеціаліст) = оригінал документа»***.

Не вдаючись до дискусії щодо правової природи електронних даних у частині зарахування до того чи іншого процесуального джерела доказів у контексті ч. 2 ст. 84 КПК України, з огляду на положення ч. 4 ст. 99 КПК України вважаємо, що виготовлена за наведеною процесуальною формулою копія електронної інформації є *документом*. Вказане є важливим для правильного розуміння правової природи копії електронної інформації як доказу в кримінальному провадженні.

З урахуванням вимог абз. 3 ч. 2 ст. 168 КПК України та практики правозастосування слідчий, прокурор можуть зіткнутися з необхідністю виготовлення копії інформації в значній кількості випадків. Деякі наведено нижче.

І. Під час проведення *обшуку або огляду місця події* копіювання інформації доцільно здійснювати:

1.1. у разі відсутності підстав для тимчасового вилучення майна;

1.2. у разі неможливості вилучення інформаційних систем через їх організаційну (структурну) складність або фізичну громіздкість;

1.3. у разі неможливості вилучення інформаційної системи через ризики припинення виробничого процесу;

1.4. у разі недоцільності вимкнення інформаційної системи через ризик втрати доступу до інформації (наприклад, за умови неможливості згодом успішно запустити розшифрування у разі вимкнення системи з активним шифруванням);

1.5. у разі копіювання інформації з модулів оперативної пам'яті інформаційної системи;

1.6. у разі потреби створення копії інформації для подання її разом із клопотанням до суду з метою накладення арешту на тимчасове вилучене майно – ЕНІ або інформаційну систему, на яких ця інформація виявлена;

1.7. у разі доцільності копіювання інформації для зменшення ризиків втрати інформації з первинного носія через його пошкодження або деградацію внаслідок впливу інших негативних факторів після вилучення.

ІІ. Під час досудового розслідування також виникає необхідність виготовлення копії електронної інформації з ЕНІ, що вже знаходяться у володінні сторони обвинувачення (шляхом проведення огляду речей і документів) у таких випадках:

2.1. з метою подальшого детального вивчення, описання, друку конкретних документів, виявлених під час огляду;

2.2. з метою створення копії інформації ЕНІ заради зменшення ризику втрати інформації з первинного носія (виготовлення автономної копії-доказу з огляду на тактичну доцільність);

2.3. з метою видачі копії інформації особі, яка є володільцем цієї інформації та звернулася до слідчого з клопотанням про надання копії в порядку ч. 3 ст. 100 КПК України;

2.4. з метою долучення до кримінального провадження копії інформації з ЕНІ замість оригінального ЕНІ, що в разі потреби підлягає видачі особі, яка є володільцем носія та звернулася до слідчого з клопотанням про надання оригіналу цього ЕНІ в порядку ч. 3 ст. 100 КПК України;

2.5. з метою збереження інформації, що міститься на ЕНІ, у зв'язку з виконанням ухвали слідчого судді про повернення носія інформації власнику;

2.6. з метою створення копії інформації (як частини матеріалів досудового розслідування), щодо якої прокурором в порядку ч. 3 ст. 217 КПК України прийнято рішення про виділення матеріалів досудового розслідування в окреме провадження;

2.7. з метою створення копії інформації, отриманої за результатами проведення негласних слідчих (розшукових) дій для використання в порядку ст. 257 КПК України;

2.8. з метою надання стороні захисту для ознайомлення та копіювання копії інформації замість оригіналу на етапі відкриття матеріалів кримінального провадження іншій стороні в порядку ст. 290 КПК України.

ІІІ. Крім того, відповідно до ч. 1 ст. 159 КПК України тимчасовий доступ до речей і документів здійснюється виключно шляхом зняття копії інформації, якщо доступ судом був наданий до електронних інформаційних систем або їх частин (комп'ютерів – *прим. авт.*) чи мобільних терміналів систем зв'язку (телефонів – *прим. авт.*).

ІV. Виготовлення копії інформації в електронній формі як резервної копії оригінальних примірників технічних носіїв інформації зафіксованої процесуальної дії передбачено в ч. 3 ст. 107 КПК України. Резервні копії таких примірників дозволяється зберігати окремо від матеріалів кримінального провадження. Допустимість створених у такий спосіб резервних копій без участі спеціаліста визнається судом з урахуванням виключних підстав, передбачених п. 1 ч. 5 ст. 99 КПК України, коли оригінал документа втрачений або знищений не з вини сторони, яка його надає.

Описані ситуації утворюють систему процесуальних сценаріїв, що передбачають необхідність виготовлення копії електронної інформації або ЕНІ під час кримінального провадження.

Розроблена авторами система процесуальних сценаріїв у сукупності з розробленим авторами статті алгоритмом прийняття рішень щодо вилучення ЕНІ під час обшуку, огляду [4, с. 159–165] спрямована на забезпечення

слідчих, прокурорів методологією ефективної оцінки оперативної обстановки щодо прийняття рішень у частині поводження з ЕНІ.

Якщо слідчим, прокурором за результатами аналізу оперативної обстановки під час проведення слідчих (розшукових) дій або з огляду на процесуальну необхідність прийнято рішення про здійснення копіювання інформації, що зберігається на ЕНІ, задля забезпечення можливості використання такої інформації як доказу під час кримінального провадження необхідне дотримання двох аспектів: процесуального та технічного.

Процесуальний аспект полягає в дотриманні слідчим, прокурором вимог ч. 4 ст. 99 КПК України щодо необхідності залучення спеціаліста, тобто дотримання наведеної нами попередньо формули. У цьому аспекті варто зауважити, що формальне виконання вимоги КПК України щодо залучення спеціаліста не гарантує тотожності копії інформації оригіналу. Залучений стороною обвинувачення спеціаліст має володіти необхідними знаннями та навичками у сфері інформаційних технологій та бути здатним правильно реалізувати процес копіювання, що має включати верифікацію (перевірку) цілісності та справжності інформації з наданням відповідних гарантій. Варто звернути увагу на окремі випадки формального виконання слідчими вимог ч. 4 ст. 99 КПК України щодо залучення спеціаліста при копіюванні інформації, що має електронну форму, з одночасним недотриманням технічних аспектів щодо гарантування цілісності та справжності інформації, що може дискредитувати виготовлену копію.

Таким чином, очевидною стає необхідність дотримання технічного аспекту процесу копіювання інформації, значення якого важко переоцінити.

Для забезпечення технічного аспекту процесу копіювання інформації доцільно застосовувати ДСТУ ISO/IEC 27037:2017 (ISO/IEC 27037:2012, IDT) «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів» (далі – ДСТУ ISO/IEC 27037:2017) [3, с. 1–31].

Стандарт розрізняє процеси виготовлення фізичної або порозрядної копії (образу) ЕНІ та копії окремого електронного файлу [3, с. 7–8]. Під час виготовлення копії конкретного файлу здійснюється копіювання конкретного блоку електронної інформації з визначеним ім'ям, розміром та атрибутами. У разі виготовлення фізичної копії ЕНІ копіюються послідовно всі інформаційні блоки носія інформації, що призначені для зберігання даних (від першого до останнього біта). Створення такої копії є створенням образу інформації з ЕНІ, що є тотожним оригінальному ЕНІ. Тобто, наприклад, у разі виявлення під час обшуку інформаційної системи з вбудованим ЕНІ загальною ємністю 64 гігабайти та записаною на ньому інформацією об'ємом 12 гігабайт, копіюючи лише наявні файли, отримаємо 12 гігабайт даних, а у разі виготовлення фізичної копії ЕНІ – 64 гігабайти. Крім того, у процесі подальшого проведення дослідження фізичної копії ЕНІ можна відновити видалені електронні дані, що не виявлені первинним оглядом ЕНІ, який проведений лише стосовно наявних файлів.

Наведений приклад ілюструє важливість розуміння технічного аспекту роботи з електронним даними під час кримінального провадження та необхідність забезпечення систематичного навчання та підвищення кваліфікації слідчих, прокурорів щодо роботи з доказами, що мають електронну форму.

Положення ДСТУ ISO/IEC 27037:2017 детально описують умови, за яких копіювання інформації для використання в юридичних процедурах може вважатися надійним та допустимим із технічного погляду. Загалом варто виділити дві вимоги: 1) недопустимість внесення змін до первинної інформації, що є об'єктом копіювання, до початку копіювання, під час та після його проведення. Одним із варіантів є підключення ЕНІ до комп'ютера спеціаліста чи слідчого, що здійснюється в режимі «тільки читання», наприклад, із використанням пристрою блокування запису; 2) верифікація (перевірка) копії інформації шляхом гешування первинної інформації, копії інформації та порівняння отриманих геш-значень. Це забезпечує змогу математично перевірити та підтвердити цілісність та справжність копії інформації, записаної на цільовий ЕНІ [3, с. 7].

Як вірно зауважують Я. Вебер та З. Смутни (2015) у статті Standard ISO 27037:2012 and Collection of Digital Evidence: Experience in the Czech Republic, стандарт ISO/IEC 27037:2012 в кількох місцях зазначає про необхідність обрахування контрольних сум для перевірки цілісності даних, але при цьому мало наголошено на тому, що ці значення, отримані під час гешування, мають бути зафіксовані безпосередньо в протоколі процесуальної дії. Виконання цієї вимоги здатне забезпечити перевірку зібраних доказів на цілісність та справжність [14, с. 297]. Видається, що запровадження вказаної практики національними органами досудового розслідування матиме позитивний вплив.

Виготовлення копії інформації з дотриманням визначених у ДСТУ ISO/IEC 27037:2017 процедур та наведенням гарантій цілісності та справжності забезпечує можливість повторно перевірити та підтвердити цілісність та справжність копії інформації будь-яким технічним спеціалістом у будь-який час, що створює переконливий та технічно досконалий для сторони обвинувачення доказ.

За умови дотримання стороною обвинувачення процесуальних та технічних аспектів у процесі виготовлення копії інформації в електронній формі утворюються унікальні умови гарантування цілісності та справжності даних копії, а відповідно, збирання допустимого доказу.

Висновки. Копія електронної інформації вже нині є дієвим інструментом доказування за умови дотримання процесуальних та технічних аспектів її виготовлення.

Водночас із метою розширення практики використання копії електронної інформації як доказу в кримінальному провадженні, підвищення ефективності та забезпечення дотримання процесуальної процедури, пропонується вжити низку адміністративних та організаційних заходів, серед яких:

– систематичне навчання та підвищення кваліфікації слідчих, прокурорів щодо роботи з доказами, що мають електронну форму;

– забезпечення органів досудового розслідування базовими технічними засобами (апаратними та програмними), призначеними для роботи з ЕНІ;

– створення в системі правоохоронних органів структурно та процесуально не залежних від органу досудового розслідування криміналістичних лабораторій, що спеціалізуються на роботі з доказами, що мають електронну форму, працівників яких може бути залучено як спеціалістів у процесі проведення слідчих (розшукових) дій для роботи з доказами, що мають електронну форму (за прикладом позитивного досвіду Національного антикорупційного бюро України);

– інформування суддів щодо технічних аспектів роботи з доказами, що мають електронну форму, в процесі проведення спільних наукових та науково-практичних заходів, зокрема, із залученням Національної школи суддів України та міжнародних партнерів.

Окрім того, необхідні системні зміни в підході до копії електронної інформації як доказу в кримінальному провадженні, що передбачають гарантування цілісності та справжності інформації не «церемоніальним» залученням спеціаліста, а наданням гарантій незмінності первинної інформації з урахуванням вимог ДСТУ ISO/IEC 27037:2017. З огляду на наведене, на нашу думку, ч. 4 ст. 99 КПК України доцільно доповнити нормою щодо обов'язку спеціаліста підтвердити цілісність та справжність створеної копії інформації.

Системний підхід до вдосконалення кримінальної процесуальної процедури та практики застосування в частині розширення можливостей використання копії інформації як доказу в кримінальному провадженні сприятиме ефективному збиранню доказів, забезпеченню прав як безпосередніх учасників кримінального провадження, так і осіб, на яких може вплинути вилучення ЕНІ та інформаційних систем, мінімізації впливу кримінальних процесуальних процедур на бізнес-процеси.

ЛІТЕРАТУРА

1. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 р. № 4651-VI (зі змін. і доп.). URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 23.07.2021).
2. Про внесення змін до деяких законодавчих актів щодо забезпечення дотримання прав учасників кримінального провадження та інших осіб правоохоронними органами під час здійснення досудового розслідування : Закон України № 2213-VIII від 16.11.2017 р. URL: https://zakon.rada.gov.ua/laws/show/2213-19#n30 (дата звернення: 12.07.2021).
3. ДСТУ ISO/IEC 27037:2017 (ISO/IEC 27037:2012, IDT) Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів. Чинний від 01.01.2019 р. Київ : УкрНДНЦ, 2018. VI, 31 с.
4. Гаркуша А.М., Каланча І.Г. Алгоритм прийняття рішень щодо вилучення електронних носіїв інформації під час обшуку. *Кримінальна юстиція в Україні: реалії та перспективи* : матеріали круглого столу, м. Львів, 11 червня 2021 р. Львів : Львівський державний університет внутрішніх справ, 2021. С. 159–165. URL: https://www.lvduvs.edu.ua/documents_pdf/biblioteka/nauk_konf/11_06_2021.pdf (дата звернення: 21.08.2021).
5. Литвинчук О.І. Електронні докази. Обшук. Частина 1 / О.І. Литвинчук, М.С. Сорока, І.В. Колесников та ін. Харків : Фактор, 2020. 80 с. URL: https://unba.org.ua/assets/uploads/publications/%D0%9F%D0%94%D0%A4_%20Electronni%20Dokazy%20Obshuk%20Part1.pdf (дата звернення: 17.07.2021).
6. Метелев О.П. Проблеми визначення допустимості і належності електронних (цифрових) доказів у кримінальному процесі. *Вісник кримінального судочинства.* 2019. № 3. С. 224–238. URL: https://vkslaw.knu.ua/images/verstka/3_2019_METELEV.pdf (дата звернення: 17.07.2021).
7. Орлов Ю.Ю. Чернявський С.С. Електронне відображення як джерело доказів у кримінальному провадженні. *Науковий часопис Національної академії внутрішніх справ.* 2017. № 3 (140). С. 13-24. DOI: –https://doi.org/10.33270/01191134.15. (дата звернення: 17.07.2021).
8. Столітній А.В., Каланча І.Г. Формування інституту електронних доказів у кримінальному процесі України. *Проблеми законності.* 2019. Вип. 146. С. 179–191. URL: http://nbuv.gov.ua/UJRN/Pz_2019_146_17 (дата звернення: 18.08.2021).
9. Хижняк Є.С. Особливості огляду електронних документів під час розслідування кримінальних проваджень. *Держава та регіони.* Серія Право. 2017. № 4 (58). С. 80–85. URL: http://www.law.stateandregions.zp.ua/archive/4_2017/15.pdf (дата звернення: 02.08.2021).
10. 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. URL: http://er.dduvs.in.ua/bitstream/123456789/3885/1/Використ%20ЕНІ%20в%20якості%20ДД.pdf%20(дата%20звернення:%2017.07.2021).
11. 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. URL: http://elar.naiau.kiev.ua/bitstream/123456789/17605/1/%D0%92%D0%B8%D0%BA%D0%BE%D1%80%D0%B8%D1%81%D1%82%D0%B0%D0%BD%D0%BD%D1%8F%20%D0%B5%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B8%D1%85%20%28%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B8%D1%85%29%20%D0%B4%D0%BE%D0%BA%D0%B0%D0%B7%D1%96%D0%B2.pdf (дата звернення: 17.07.2021).
12. Застосування електронних доказів під час розгляду справ, пов'язаних із корупцією: збірка навчальних матеріалів тренінгу для суддів. 138 с. URL: http://www.nsj.gov.ua/files/1581330611Посібник%20Електронні%20докази%202019.pdf%20(дата%20звернення:%2018.07.2021)
13. Пояснювальна записка до проєкту Закону України «Про внесення змін до деяких законодавчих актів щодо забезпечення дотримання прав учасників кримінального провадження та інших осіб правоохоронними органами під час здійснення досудового розслідування». URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=62853&pf35401=438050 (дата звернення: 10.08.2021).
14. Veber J. & Smutny Z. Standard ISO 27037:2012 and Collection of Digital Evidence: Experience in the Czech Republic. *14th European Conference on Cyber Warfare & Security*, Hatfield, UK, 2-3 July 2015. P. 294-299. URL: https://www.researchgate.net/profile/Zdenek-Smutny/publication/283226153_Standard_ISO_270372012_and_Collection_of_Digital_Evidence_Experience_in_the_Czech_Republic/links/569a87dd08ae6169e55b844f/Standard-ISO-270372012-and-Collection-of-Digital-Evidence-Experience-in-the-Czech-Republic.pdf (access date: 12.08.2021).
15. Electronic Evidence and Electronic Signatures: Fifth Edition. Edited by Stephen Mason and Daniel Seng. 2021. 539 p. URL: https://humanities-digital-library.org/index.php/hdl/catalog/view/electronic-evidence-and-electronic-signatures/214/408-1 (access date: 21.08.2021).