DOI https://doi.org/10.51647/kelm.2022.8.29

AKTUALNE WYZWANIA ZWIĄZANE Z ZAPEWNIENIEM SKUTECZNOŚCI UZYSKIWANIA I WYKORZYSTYWANIA DOWODÓW ELEKTRONICZNYCH W DOCHODZENIU CYBERPRZESTĘPSTW. DOŚWIADCZENIE USA

Oleksandr Kolosov
aspirant Katedry Wymiaru Sprawiedliwości w Sprawach Karnych
Dydaktyczno-Naukowego Instytutu Prawa Państwowego Uniwersytetu Podatkowego (Irpień, Ukraina)
ORCID ID: 0000-0003-0128-5565
kolosov2424@gmail.com

Adnotacja. Artykuł bada aktualne wyzwania związane z zapewnieniem skuteczności uzyskiwania i wykorzystywania dowodów elektronicznych w dochodzeniu cyberprzestępstw. Badanie opiera się na doświadczeniach USA. Zbadano pojęcia, treści i etapy kryminalistyki cyfrowej. Omówiono kwestie dopuszczalności dowodów na podstawie standardu Dauberta. Omówiono ulepszenia w pozyskiwaniu i przetwarzaniu dowodów cyfrowych, w szczególności poprzez zbudowanie zestawu narzędzi do rekonstrukcji plików FileTSAR do analizy próbek.

Sformułowano propozycje dotyczące: 1) definicji pojęcia dowodów elektronicznych i kryteriów ich dopuszczalności w Kodeksie Postępowania Karnego Ukrainy; 2) potrzeby wykorzystania doświadczenia USA w opracowaniu analogowego zestawu narzędzi do selektywnej analizy i rekonstrukcji plików FileTSAR, który przestrzega modelu procesu sortowania w dziedzinie kryminalistyki komputerowej, w celu uzyskania danych dowodowych na miejscu zdarzenia.

Słowa kluczowe: dowody elektroniczne, kryminalistyka cyfrowa, cyberprzestępczość, amerykańskie doświadczenie, ekspert kryminalistyczny, przepisy dotyczące postępowania karnego Ukrainy.

CURRENT PROBLEMS OF ENSURING THE EFFICIENCY OF OBTAINING AND USING ELECTRONIC EVIDENCE DURING THE INVESTIGATION OF CYBER CRIMES. USA EXPERIENCE

Oleksandr Kolosov
Postgraduate Student at the Department of Criminal Justice
Educational and Scientific Institute of Law of the State Tax University (Irpin, Ukraine)
ORCID ID: 0000-0003-0128-5565
kolosov2424@gmail.com

Abstract. The article studies the actual problems of ensuring the efficiency of obtaining and using electronic evidence in the investigation of cybercrime. The study is based on the experience of the United States. The concepts, content and stages of digital forensics are investigated. The issues of admissibility of evidence based on the Daubert standard are considered. The issues of improving the collection and processing of digital evidence are considered, in particular, by creating File Toolkit for Selective Analysis Reconstruction (FileTSAR).

Proposals have been formulated for: 1) defining the concept of electronic evidence and the criteria for their admissibility in the Criminal Procedure Code of Ukraine; 2) the need to use the experience of the United States in the development of an analogue of the File Toolkit for Selective Analysis Reconstruction FileTSAR that follows the Computer Forensics Field Triage Process Model for the on-the-scene acquisition of probative data.

Key words: electronic evidence, digital forensics, cybercrimes, American experience, forensic investigator, criminal procedural legislation of Ukraine.

АКТУАЛЬНІ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ЕФЕКТИВНОСТІ ОТРИМАННЯ ТА ВИКОРИСТАННЯ ЕЛЕКТРОННИХ ДОКАЗІВ ПІД ЧАС РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ. ДОСВІД США

Олександр Колосов
аспірант кафедри кримінальної юстиції
Навчально-наукового інституту права Державного податкового університету (Ірпінь, Україна)
ORCID ID: 0000-0003-0128-5565
kolosov2424@gmail.com

Анотація. У статті досліджуються актуальні проблеми забезпечення ефективності отримання та використання електронних доказів під час розслідування кіберзлочинів. За основу дослідження взято досвід США. Досліджено поняття, зміст та етапи цифрової криміналістики. Розглянуто питання прийнятності доказів на основі стандарту

Дауберта. Розглянуто питання покращення отримання та обробки цифрових доказів, зокрема, шляхом створення файлового набору інструментів для реконструкції вибіркового аналізу FileTSAR.

Сформульовано пропозиції щодо: 1) визначення поняття електронних доказів та критеріїв їх допустимості у кримінальному процесуальному кодексі України; 2) необхідності використання досвіду США у розробленні аналогу набору інструментів для вибіркового аналізу та реконструкції файлів FileTSAR, який дотримується моделі процесу сортування на місцях комп`ютерної криміналістики, з метою отримання доказових даних на місці події.

Ключові слова: електронні докази, цифрова криміналістика, кіберзлочини, американський досвід, експерт-криміналіст, кримінальне процесуальне законодавство України.

Вступ. Одним із найактуальніших питань у відношенні забезпечення національної безпеки будь-якої держави є питання створення безпечного кіберпростору та забезпечення інформаційної безпеки. Стрімкий розвиток інформаційних технологій зумовив стрибок кіберзлочинності, у зв`язку з чим кожне підприємство, установа та організація будь-якої форми власності та кожний індивідуальний користувач інформаційних систем можуть бути піддані загрозі зі сторони кіберзлочинців. Враховуючи теперішні безпекові виклики вкрай актуальним є питання ефективного використання електронних доказів під час розслідування кіберзлочинів. Важливим є дослідження зарубіжного досвіду у питанні дослідження електронних доказів з метою формування пропозицій для розвитку національних підходів боротьби із кіберзлочинністю. Так, у даному відношенні, у статті досліджено досвід Сполучених Штатів Америки.

Проблематкою дослідження забезпечення інформаційної безпеки займалися такі українські вчені як Арістова І. В., Березовська І. Р., Дзьобаня О. П., Калюжний Р. А., Кормич Б. А., Ліпкан В. А., Марущак А. І., Цимбалюк В. С., Юдін О. К. та інші. Проблематиці протидії кіберзлочинності присвячено роботи таких вітчизнаних вчених як Азарова Д.С., Біленчука П. Д., Бутузова В. М., Вєхова В. Б., Гавловського В. Д., Голубєва В. О., Іванченко О. Ю., Карчевського М. В., Музики А. А., Пашнєва Д. В., Цимбалюка В. С., Шеломенцева В. П. та ін..

Мета статті полягає у дослідженні особливостей досвіду Сполучених Штатів Америки щодо забезпечення ефективності отримання та використання електронних доказів під час розслідування кіберзлочинів.

Нормативною базою дослідження є Кримінальний процесуальний кодекс України, Цивільний процесуальний кодексу України, Закон України «Про електронні документи та електронний документообіг» від 22 травня 2003 року № 851-IV. Також використовувались статистичні та аналітичні матеріали з національних, американських та інших зарубіжних джерел.

Основна частина. У досліджені використано методи аналізу, синтезу та порівняння. Проаналізовано нормативно-правовий базис України у частині забезпечення електронних доказів у кримінальному процесі в Україні та американський досвід у даному відношенні. Завданнями дослідження є:

– висвітлення статистичних даних у США, Канаді, країнах Європи та Україні щодо стану кіберзлочинності;

– визначення поняття доказів згідно Кримінального процесуального кодексу України із порівнянням такого визначення у цивільному процесуальному законодавстві України.

– визначення суті електронного доказу;

– визначення поняття та етапів цифрової криміналістики;

– визначення етапів отримання електронних доказів;

– визначення вимог до електронних доказів;

– визначення позитивного досвіду США щодо покращення ефктивності отримання та обробки цифрових доказів під час розсідування кіберзлочинів.

Відповідно до Оцінки загрози організованої злочинності в Інтернеті The (англ. «Internet Organised Crime Threat Assessment») (IOCTA) кіберзлочинність стає все більш агресивною та конфронтаційною. Фішинг, фармінг і шахрайське використання кредитної/дебетової картки – це лише деякі з типів кіберзлочинів, про які користувачі повинні знати (O'Flaherty, 2021).

У Сполучених Штатах Америки 60 мільйонів американців зіштовхувались з шахрайським використанням особистих даних, як показує статистика крадіжки особистих даних. Згідно зі статистикою кіберзлочинності за 2017 рік, особисті облікові дані 16,7 мільйона споживачів були вкрадені та використані без їх відома. Це призвело до розкрадання 16,8 мільярдів доларів у споживачів за один рік. 59% американців повідомляють, що стикалися з кіберзлочинами або якимось чином потрапили до рук комп'ютерного хакера. Це складає 152 мільйони американських споживачів, чия безпека в Інтернеті так чи інакше була порушена. У 2018 році 105 мільйонів американців заявили, що стикалися з кіберзлочинами. Кіберзлочинність вплинула на 41% американського населення станом на 2018 рік (Vojinovic Ivana, 2022).

Для порівняння, у Канаді та країнах Європи проблема кіберзлочинності також є вкрай нагальною. Згідно звіту CyberEdge Group про захист від кіберзагроз (CDR) за 2020 рік встановлено, що 78 відсотків канадських організацій зазнали принаймні одну кібератаку протягом 12 місяців. У 2021 році цей показник зріс до 85,7 відсотків канадських компаній. У звіті CyberEdge за 2020 рік уточнюється питання програм-вимагачів і встановлено, що 72 відсотки респондентів у Канаді мали справу з програмами-вимагачами у 2020 році. У 2021 році ця цифра суттєво впала до лише 61,2 відсотка організацій (O`Driscoll Aimee, 2022).

Канадський центр боротьби з шахрайством (англ. «The Canadian Anti-Fraud Centre») (CAFC) підрахував, що у 2021 році канадці втратили через шахрайство загалом 230 мільйонів канадських доларів. Згідно даного центру шахрайство з інвестиціями було найпоширенішим видом шахрайства у 2021 році, що коштувало канадцям понад 70 мільйонів доларів і все частіше включало криптовалюти (O`Driscoll Aimee, 2022).

Згідно аналізу Пола Скелдона «Яка дійсність злочинності у реальному світі та кіберзлочинності в Європі?» (англ. "What is the reality of real-world and cybercrime in Europe?") опублікованого 10 грудня 2021 року, найнебезпечнішою країною у відношенні кіберзлочинності також є Велика Британія. Згідно з дослідженням, проведеним компанією Detica для Кабінету міністрів, Велика Британія щорічно зазнає збитків у розмірі 27 мільярдів фунтів стерлінгів через кіберзлочинність, причому переважними жертвами є британський бізнес. 13,64 на кожні 100 000 громадян Великобританії зазнають фінансових втрат через кіберзлочинність, що є найвищим показником у Європі (Skeldon Paul, 2021).

Щодо України, згідно звітності Офісу Генерального прокурора України (Єдиний звіт про осіб, які вчинили кримінальні правопорушення) за 2020 рік кількість осіб яким було повідомлено про підозру у вчиненні кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (р. XVI Кримінального кодексу України), зокрема серед яких були: несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361 ККУ); створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361-1 ККУ); несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361-2 ККУ); несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362 ККУ); інші, складала 1243 осіб. Кількість осіб, відносно яких вироки та ухвали набрали законної сили щодо таких кримнальних правопорушень у 2020 році становила 0 осіб (Офіс Генерального прокурора України).

За 2021 рік кількість осіб, яким було повідомлено про підозру у вчиненні таких кримінальних правопорушень складала 1732 особи. Кількість осіб, відносно яких вироки та ухвали набрали законної сили щодо таких кримнальних правопорушень у 2021 році становила 0 осіб (Офіс Генерального прокурора України).

Беручи до уваги вищенаведену статистичну інформацію в Україні, варто зауважити, що така різниця між кількістю осіб, яким було повідомлено про підозру у вчиненні кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів) та кількістю осіб, відносно яких вироки та ухвали набрали законної сили, свідчить про складність доказування, зокрема, в частині роботи із електронними доказами та їх носіями. У той самий час статистичні дані Сполучених Штатів Америки, а також країн Європейського Союзу та Канади вказують на глобальність проблеми кіберзлочинності.

Згідно ст. 84 Кримінального процесуального кодексу України (надалі – КПК України) доказами в кримінальному провадженні є фактичні дані, отримані у передбаченому цим Кодексом порядку, на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню. Процесуальними джерелами доказів є показання, речові докази, документи, висновки експертів (Закон України, 2001).

Таким чином, станом на сьогоднішній день в українському кримінальному процесуальному законодавстві відсутнє поняття електронних доказів, що ускладнює питання їх використання під час розслідувань кримінальних правопорушень. У зв`язку з цим виникає потреба у визначенні критеріїв допустимості електронних доказів у кримінальному процесі.

Проте поняття електронних доказів присутнє у Цивільному процесуальному кодексі України (надалі – ЦПК України) (Закон, 2004). Зокрема, ч. 5 ст. 43 у статті визначено, що документи (в тому числі процесуальні документи, письмові та електронні докази тощо) можуть подаватися до суду, а процесуальні дії вчинятися учасниками справи в електронній формі з використанням Єдиної судової інформаційно-телекомунікаційної системи, за винятком випадків, передбачених цим Кодексом. У статті 76 ЦПК України вказано, що доказами є будь-які дані, на підставі яких суд встановлює наявність або відсутність обставин (фактів), що обґрунтовують вимоги і заперечення учасників справи, та інших обставин, які мають значення для вирішення справи. Ці дані встановлюються такими засобами: 1) письмовими, речовими і електронними доказами; 2) висновками експертів; 3) показаннями свідків.

У ст. 8 Закону України «Про електронні документи та електронний документообіг» від 22 травня 2003 року № 851-IV визначено, що допустимість електронного документа як доказу не може заперечуватися виключно на підставі того, що він має електронну форму (Закон, 2003).

За своєю суттю електронний доказ є, насамперед, цифровим об'єктом, який: був засобом чи знаряддям вчинення кримінального правопорушення (наприклад, вірусна програма, за допомогою якої було здійснено несанкціонований доступ до інформації; телеграм-канал, створений для збуту наркотичних засобів і т.п.); зберіг електронно-цифрові сліди кримінального правопорушення (наприклад, відеозапис із цифрової камери відеоспостереження, на якому зафіксовано зображення особи, яка вчинила кримінальне правопорушення; метадані, в яких зафіксовано час входу ідентифікованого користувача в автоматизовану систему; інформація про електронний переказ коштів, які були надані як неправомірна вигода службовій особі тощо); був предметом вчинення кримінального правопорушення (наприклад, вебсайт, на якому розміщені матеріали порнографічного характеру); був об'єктом кримінально протиправних дій (об'єкт авторського права, який незаконно поширювався мережею Інтернет; викрадена криптовалюта тощо); містить інші відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження

(наприклад, інформація, розміщена на сторінці в соціальній мережі, дає змогу охарактеризувати особу обвинуваченого) (Козицька, 2020: 418–421). Можна виділити основні ознаки електронних доказів: нематеріальний вигляд; можливість існування оригіналу електронного доказу в кількох місцях одночасно; можливість, без втрати характеристик, копіювання на різні пристрої; для відтворення необхідно використовувати відповідні технічні засоби (Найченко А.М., Куртакова Г.О., 2018: 72–85).

У США існує дві основні сфери правового регулювання, які впливають на дії щодо кібербезпеки, пов'язані зі збором мережевих даних: (1) повноваження щодо моніторингу та збору даних і (2) допустимість методів збору (Cybersecurity and Infrastructure Security Agency, 2008: 4). На сайті Національного інституту юстиції США визначено поняття цифрових доказів як інформацію, яка зберігається або передається у бінарній формі, на яку можна покладатися в суді (National Institute of Justice). Досліджуючи проблематику електронних доказів, варто зауважити, що дана проблема безпосередньо пов'язана з темою цифрової криміналістики.

У криміналістичній науці одним з ключових понять є «цифрова криміналістика» (англ. «digital forensics»). Цифрова криміналістика – це практика виявлення, отримання та аналізу електронних доказів. Цифрові криміналістичні дані зазвичай використовують у судових розглядах (BlueVoyant).

Відповідно до Першого семінару з досліджень у галузі цифрової криміналістики (англ. «First Digital Forensics Research Workshop»), який був проведений 7–8 серпня 2001 року у Ютиці, штат Нью-Йорк, США, цифрову криміналістику було визначено як використання науково обґрунтованих та перевірених методів для збереження, збирання, перевірки, ідентифікації, аналізу, інтерпретації, документування та подання цифрових доказів, отриманих із цифрових джерел, з метою полегшення чи сприяння реконструкції подій, визнаних злочинними, або допомоги попереджати несанкціоновані дії, які можуть порушити заплановані операції (Digital Forensic Research Conference, 2001: 16).

Інтерпол визначає цифрову криміналістику як галузь криміналістики, яка зосереджена на ідентифікації, отриманні, обробці, аналізі та звітності щодо даних, що зберігаються в електронному вигляді (Interpol).

Серед американських інституцій у яких широко використовуються та розвиваються цифрові криміналістичні дослідження можна виділити наступні: Департамент юстиції Сполучених Штатів; Національний інститут стандартів та технологій (NIST) Департаменту торгівлі Сполучених Штатів; SANS Інститут, США; Міжнародна рада консультантів з електронної комерції (EC-Council), США; Асоціація з управління і аудиту інформаційної системи (Information System Audit and Control Association, ISACA), США (Носов, 2016).

Відповідно до Міжнародної ради консультантів з електронної комерції (EC-Council), США, до етапів цифрової криміналістики відносяться:

1) Етап I – Перша відповідь. Дія, яка виконується відразу після виникнення безпекового інциденту, що значною мірою залежить від характеру інциденту.

2) Етап II – Обшук та вилучення. Фахівці шукають пристрої, задіяні у скоєнні злочину з подальшим їх ретельним вилученням з метою отримання інформації.

3) Етап III – Збирання доказів. Після етапу обшуку та вилучення фахівці, які мають чітко визначені криміналістичні методи роботи з доказами, використовують отримані пристрої для збору даних.

4) Етап IV – Забезпечення доказів. Експерт-криміналіст, який визначає чи є зібрані дані точними, достовірними та доступними, повинен мати доступ до безпечного середовища, де він може забезпечити докази.

5) Етап V – Збір даних. Це процес отримання інформації, що зберігається в електронному вигляді з підозрюваних цифрових активів, який допомагає отримати уявлення про інцидент, тоді як неправильний процес може змінити дані, тим самим пожертвувавши цілісністю доказів.

6) Етап VI – Аналіз даних. Під час аналізу даних відповідальний персонал сканує отримані дані, щоб визначити доказову інформацію, яка може бути подана до суду. Цей етап присвячений вивченню, ідентифікації, поділу, перетворенню та моделюванню даних для перетворення їх у корисну інформацію.

7) Етап VII – Оцінка доказів. Процес оцінки доказів пов'язує доказові дані з безпековим інцидентом. Повинна бути проведена ретельна оцінка, що ґрунтується на межах розгляду справи.

8) Етап VIII – Документація та звітність. Це етап після розслідування, який охоплює звітність та документування всіх результатів.

9) Етап IX – Дача показів як свідок-експерт. Експерт-криміналіст повинен звернутися до свідка-експерта, фахівця який розслідує злочини з метою отримання доказів, щоб підтвердити точність показань (EC-Council).

На кожному етапі отримання електронних доказів для різних типів кримінальної діяльності застосовують певні засоби, прийоми та методи. Цифрова криміналістика визначає наступні суттєві для розслідування кіберзлочинів питання: поняття, характеристика, прийнятність та принципи роботи з електронними доказами; джерела електронних доказів; особливості обшуку і вилучення джерел електронних доказів при фізичному та віддаленому доступі; пошук доказів в мережі Інтернет; окремі аспекти дослідження і оцінки електронних доказів; підготовка та представлення електронних доказів (Носов, 2016).

Цифрова криміналістика займається широким спектром даних, що дозволяє експерту досліджувати докази щодо унікальних обставин, пов'язаних із подією. Кожен випадок і середовище є різними та представляють унікальні виклики (J.S. Held).

Відповідно до Керівництва щодо інтеграції криміналістичної техніки у реагування на інциденти (англ. «Guide to integrating forensic techniques into incident response») (Рекомендації Національного інституту стандартів і технологій, США) (надалі – «Керівництво») до основних етапів процесу судової експертизи належать:

збирання, дослідження, аналіз та звітність (National Institute of Standards and Technology U.S. Department of Commerce, 2006: 3-2–3-7). Таким чином, відповідно до Керівництва дані етапи визначаються наступним чином:

1. Збирання даних (виявлення потенційних джерел даних та отримання даних із них).

1.1. Визначення можливих джерел даних. Найбільш очевидними та поширеними джерелами даних є настільні комп'ютери, сервери, мережні пристрої зберігання даних та ноутбуки.

1.2. Отримання даних. Збір даних має виконуватися з використанням триетапного процесу: розробка плану отримання даних, отримання даних та перевірка цілісності отриманих даних.

1.2.1. Розробка плану отримання даних. Аналітик повинен створити план, який визначає пріоритети джерел та встановлює порядок отримання даних. Важливими чинниками визначення пріоритетів є такі:

– Ймовірне значення. Грунтуючись на розумінні аналітиком ситуації та попередньому досвіді в подібних ситуаціях, аналітик повинен бути спроможним оцінити відносну ймовірну цінність кожного потенційного джерела даних.

– Волатильність. Волатильні дані – це дані в діючій системі, які втрачаються після вимкнення комп'ютера або з часом. Волатильні дані також можуть бути втрачені внаслідок інших дій, що виконуються в системі.

– Необхідний обсяг зусиль. Зусилля включають не тільки час, витрачений аналітиками та іншими співробітниками організації (включно з юрисконсультами), але й вартість обладнання та послуг (наприклад, зовнішніх експертів).

1.2.2. Отримання даних. Отримання даних може виконуватися як локально, так і через мережу. Під час локального отримання даних існує більший контроль над системою та даними. При зборі даних через мережу слід приймати рішення щодо типу даних, які необхідно зібрати, та обсягу зусиль, що використовуються.

1.2.3. Перевірка цілісності даних. Перевірка цілісності даних зазвичай складається з використання інструментів для обчислення дайджесту повідомлення оригінальних та скопійованих даних, а потім порівняння дайджестів, щоб переконатися, що вони однакові.

1.3. Реагування на інциденти. У багатьох випадках аналітик повинен працювати з групою реагування на інциденти, щоб ухвалити рішення про стримування (наприклад, відключення мережевих кабелів, відключення живлення, посилення заходів фізичної безпеки, коректне відключення хоста). З метою стримування інциденту, можуть бути здійснені наступні кроки: -захист периметра навколо комп'ютера та обмеження доступу для уповноваженого персоналу під час процесу збору, з метою гарантування, що докази не будуть змінені; – документування списку усіх користувачів, які мають доступ до комп'ютера, оскільки ці особи можуть надати паролі або інформацію про те, де знаходяться конкретні дані; – якщо комп'ютер підключено до мережі, від'єднання мережних кабелів, підключених до комп'ютера, може запобігти зміні даних комп'ютера віддаленими користувачами; – якщо комп'ютер використовує бездротове мережне з'єднання, зовнішній мережний адаптер може бути відключений від комп'ютера або внутрішній мережний адаптер може бути вимкнений, щоб розірвати мережне з'єднання; відключення точки доступу (декількох точок доступу) до бездротової мережі, яку використовує комп'ютер.

2. Дослідження. Даний етап включає оцінку і вилучення відповідних фрагментів інформації із зібраних даних. Цей етап може також включати обхід або ослаблення функцій ОС або програм, які приховують дані та код, таких як стиснення даних, шифрування та механізми керування доступом.

3. Аналіз. Аналіз повинен включати ідентифікацію людей, місць, предметів та подій, а також визначення того, як ці елементи пов'язані між собою, щоб можна було зробити висновок. Часто ці зусилля включатимуть зіставлення даних між кількома джерелами.

4. Звітність. Заключна фаза, яка є процесом підготовки та подання інформації, отриманої в результаті етапу аналізу. У рамках процесу звітування аналітики повинні виявити будь-які проблеми, які, можливо, необхідно виправити, наприклад недоліки політики або процедурні помилки. На звітність впливають наступні чинники:

– Альтернативні пояснення. Коли інформація про подію неповна, остаточне пояснення того, що сталося, може бути неможливим. Якщо подія має два чи більше правдоподібних пояснення, кожне з них має бути розглянуто належним чином у процесі звітування. Аналітики повинні використовувати методичний підхід, з метою спроби доведення або спростування кожного можливого запропонованого пояснення.

– Врахування аудиторії. Важливо знати аудиторію, якій будуть показані дані чи інформація.

– Корисна інформація. Звітування також включає визначення корисної інформації, отриманої з даних, яка може дозволити аналітику збирати нові джерела інформації.

Якщо порівнювати вимоги до доказів в Україні та США, зокрема електронних, усі докази у кримінальному процесі України мають відповідати чотирьом вимогам, що висуваються до їх змісту та форми, а саме: належності, допустимості, достовірності та достатності. Так, відповдіно до ст. 94 КПК України слідчий, прокурор, слідчий суддя, суд за своїм внутрішнім переконанням, яке грунтується на всебічному, повному й неупередженому дослідженні всіх обставин кримінального провадження, керуючись законом, оцінюють кожний доказ з точки зору належності, допустимості, достовірності, а сукупність зібраних доказів – з точки зору достатності та взаємозв'язку для прийняття відповідного процесуального рішення.

Відповідно до КПК України належними є докази, які прямо чи непрямо підтверджують існування чи відсутність обставин, що підлягають доказуванню у кримінальному провадженні, та інших обставин, які мають значення для кримінального провадження, а також достовірність чи недостовірність, можливість

чи неможливість використання інших доказів. Доказ визнається допустимим, якщо він отриманий у порядку, встановленому КПК України. Недопустимий доказ не може бути використаний при прийнятті процесуальних рішень, на нього не може посилатися суд при ухваленні судового рішення (Закон, 2012).

Щодо допустимості доказів, відповідно до позиції Кримінального касаційного суду, висловленої у постанові від 11.02.2020 у справі №761/33311/15-к, даючи оцінку недопустимості доказу, суд має проаналізувати критерії допустимості доказів, а саме законність джерела, законний спосіб їх отримання, процесуальне оформлення ходу і результатів проведення слідчих дій (Касаційний кримінальний суд, 2020). Варто зауважити, що з урахуванням відсутності поняття у кримінальному процесуальному законодавстві України «електронних» або «цифрових» доказів, перевірити електронний доказ за вищевказаними чотирма критеріями є складним завданням.

Варто зауважити, що у чинному кримінальному процесуальному законодавстві України не закріплено визначення достовірності та достатності доказів. Проте відповідні нормативні закріплення є у Цивільному процесуальному кодексі України (далі – ЦПК) та Господарському процесуальному кодексі України (далі – ГПК) та Кодексі адміністративного судочинства (далі – КАС). Відповідно, до ЦПК (ст. 79) (Закон, 2004) та КАС (ст. 75) (Закон, 2005) достовірними є докази, на підставі яких можна встановити дійсні обставини справи. Визначення достовірності доказів є відмінним у ГПК (ст. 78) (Закон, 1991), де достовірними є докази, створені (отримані) за відсутності впливу, спрямованого на формування хибного уявлення про обставини справи, які мають значення для справи.

Також національне цивільне процесуальне та господарське процесуальне законодавство встановлює визначення достатності доказів. Згідно ст. 80 ЦПК (Закон, 2004) та ст. 76 КАС (Закон, 2005) достатніми є докази, які у своїй сукупності дають змогу дійти висновку про наявність або відсутність обставин справи, які входять до предмета доказування. Питання про достатність доказів для встановлення обставин, що мають значення для справи, суд вирішує відповідно до свого внутрішнього переконання.У Сполучених Штатах Америки, щоб електронні докази були прийняті в суді, вони повинні пройти тест на допуск. Суддя приймає рішення про прийнятність доказів на основі стандарту Дауберта (англ. «Daubert standard»). Наукова достовірність техніки або методу першопочатково оцінюється за допомогою п'яти факторів Дауберта: 1) рецензування та публікація; 2) загальне визнання у відповідному експертному середовищі; 3) потенціал для тестування або фактичне тестування; 4) відомий або потенційний рівень помилок; 5) наявність і дотримання стандартів, що контролюють використання техніки або методу (Breß, Kiltz, Schäler, 2013: 117).

Також у питанні допуску електронних (цифрових) доказів важливим є забезпечення цілісності доказів. Підтвердження цілісності цифрових доказів вимагає залучення цифрових судових експертів, які володіють знаннями, навичками та досвідом використання та застосування ряду комплексних методів і інструментів інформатики та інформаційної безпеки. Цифрові судово-медичні експерти використовують свої навички та інструменти, щоб створити непрямі докази цілісності та достовірності доказів, або вони надають докази та висновки, що заперечують автентичність електронної інформації (Manes, Downing, Watson, Thrutchley, 2007: 32).

Беручи до уваги вищевикладене можна зробити висновок, що процес отримання електронних доказів є достатньо громіздким. Враховуючи широкомасштабність кіберзлочинності та опанування кіберзлочинцями нових навичок у сфері інформаційних технологій, перед експертами-криміналістами постає завдання оптимізації робочих процесів з метою підвищення ефективності розслідування та розкриття кіберзлочинів.

У даному відношенні звертаємось до досвіду Сполучених Штатів Америки, де з метою покращення отримання та обробки цифрових доказів, Національний інститут юстиції (англ. "National Institute of Justice") (NIJ) надав фінансування Університету Пердью та Університету Род-Айленда. Університет Пердью створив файловий набір інструментів для реконструкції вибіркового аналізу FileTSAR (англ. "File Toolkit for Selective Analysis Reconstruction (FileTSAR)") для великих комп'ютерних мереж, який дозволяє отримувати доказові дані на місці події. Потім FileTSAR дозволяє проводити детальне криміналістичне дослідження на місці або в середовищі цифрової криміналістичної лабораторії з метою забезпечення допустимих цифрових доказів (National Institute of Justice). Основними функціями цього інструменту є захоплення потоків даних і надання механізму для вибіркової реконструкції документів, зображень, електронної пошти та розмов VoIP (Adam, 2020).

FileTSAR об'єднує в одному повному пакеті найпопулярніші інструменти розслідування з відкритим кодом, які використовуються групами правоохоронних органів цифрової криміналістики на місцевому, державному, національному та глобальному рівнях (Adam, 2020).

Даний набір інструментів можна використовувати для виявлення мережевого трафіку для відстеження кіберзлочинців, виявлення співробітників, які надсилають комерційну таємницю чи іншу конфіденційну інформацію, або для відтворення викривальних розмов чи дій співробітників або зовнішньої діяльності (Baker, 2020).

FileTSAR дотримується моделі процесу сортування на місцях комп`ютерної криміналістики (англ. Computer Forensics Field Triage Process Model), розробленої Маркусом Роджерсом та його колегами для отримання доказових даних на місці події (National Institute of Justice). Модель процесу сортування на місцях комп`ютерної криміналістики була запропонована в 2006 році в журналі "The Journal of Digital Forensics Security and Law", та визначається як слідчі процеси, які проводяться протягом перших кількох годин розслідування, які надають інформацію, яка використовується під час опитування підозрюваного та етапу

здійснення обшуку. Через потребу в отриманні інформації за відносно короткий проміжок часу модель зазвичай передбачає аналіз відповідної комп'ютерної системи на місці/польових умовах. Основна увага моделі націлена на: негайне знайдення корисних доказів; ідентифікацію постраждалих, що піддані гострому ризику; керівництво поточним розслідуванням; визначення потенційних обвинувачень; точну оцінку небезпеки правопорушника для суспільства (Arshad, 2020).

Таким чином, за допомогою інструментарію FileTSAR збір та аналіз даних з мережі поділений на декілька процесів: 1) захоплення пакетів (тобто запис трафіку пакетів у мережі); 2) аналіз протоколу (тобто розбір різних мережевих протоколів і полів); 3) пошук і аналіз; 4) візуалізація (Purdue University, 2019: 1).

Робота FileTSAR виглядає наступним чином:

1) Модуль Collector записує мережевий трафік і зберігає трафік у сховищі (англ. «Storage»).

2) Модуль Indexer приймає вхідні дані від модуля Collector, а потім обробляє їх щодо вмісту файлу (Purdue University, 2019: 2). Дані архівуються в активних каталогах справ у підсистемі зберігання, і їх можна досліджувати, шукати та візуалізувати пізніше. Аналізатор визначає взаємозв'язок файлів, потоків, пакетів, користувачів і часових ліній. Аналізатор також реконструює документи, зображення, електронну пошту та голос через Інтернет-протокол (National Institute of Justice).

Візуалізатор визначає тенденції, шаблони або повторення. Він містить веб-панель, доступ до якої мають лише автентифіковані користувачі. Ця автентифікація забезпечує підзвітність системи, реєструє всі дії та підтримує ланцюжок зберігання будь-яких зібраних доказів (National Institute of Justice).

Висновки. Отже, сучасному світі проблема кіберзлочинів набула широких масштабів. Статистичні дані України, США, Канади та країн Європи щодо стану кіберзлочинності чітко демонструють нагальну потребу у виробленні ефективних та злагоджених механізмів отримання та використання електронних доказів з метою розкриття відповідних злочинів.

Наукою, що зосереджена на виявленні, отриманні та аналізі електронних доказів є цифрова криміналістика. У статті визначено етапи цифрової криміналістики відповідно до Міжнародної ради консультантів з електронної комерції.

Проблемою залишається відсутність в кримінальному процесуальному законодавстві України поняття електронних доказів. Визначення такого поняття у національному кримінальному процесуальному законодавстві забезпечить уникнення складнощів під час визначення відповідності електронних доказів вимогам, що висуваються до їх змісту та форми, зокрема належності і допустимості.

Окрім проблеми визначення електронних доказів важливим є питання їх отримання. Відповідно до досвіду США з метою покращення отримання та обробки цифрових доказів, Національний інститут юстиції надав фінансування Університету Пердью та Університету Род-Айленда. Університет Пердью створив файловий набір інструментів для реконструкції вибіркового аналізу (FileTSAR) для великих комп'ютерних мереж, який дозволяє отримувати доказові дані на місці події.

У зв`язку з вищевикладеним вважаємо за необхідне визначення у кримінальному процесуальному кодексі України поняття електронних доказів та визначення критеріїв допустимості електронних доказів у кримінальному процесі. Надання такого визначення забезечить ефективність отримання та використання електронних доказів під час розслідування кіберзлочинів, а отже і вплине на рівень розкриття таких злочинів.

Також з метою підвищення ефективності розслідування та розкриття кіберзлочинів вважаємо за необхідне використання досвіду США у розробленні аналогу набору інструментів для вибіркового аналізу та реконструкції файлів FileTSAR (англ. «The Toolkit for Selective Analysis & Reconstruction of Files FileTSAR»), який дотримується моделі процесу сортування на місцях комп`ютерної криміналістики (англ. Computer Forensics Field Triage Process Model), з метою отримання доказових даних на місці події.

Список використаних джерел:

1. O'Flaherty Bea (2021). Cybersecurity ranked in European cities. URL: https://www.iotinsider.com/security/cybersecurity-ranked-in-european-cities/ (дата звернення: 12.12.2022)
2. Vojinovic Ivana (2022). More Than 70 Cybercrime Statistics – A $6 Trillion Problem. URL: https://dataprot.net/statistics/cybercrime-statistics/#:~:text=60%20million%20Americans%20have%20experienced%20identity%20fraud%2C%20identity%20theft%20statistics%20show.&text=According%20to%20cyber%20crime%20statistics%20from%202017%2C%2016.7%20million%20consumers,consumers%20in%20a%20single%20year (дата звернення: 12.12.2022)
3. O`Driscoll Aimee (2022). Canada cyber security and cyber crime statistics (2020–2022). URL: https://www.comparitech.com/blog/information-security/canada-cyber-crime-statistics/ (дата звернення: 12.12.2022)
4. Skeldon Paul (2021). ANALYSIS What is the reality of real-world and cybercrime in Europe? URL: https://www.telemediaonline.co.uk/analysis-what-is-the-reality-of-real-world-and-cybercrime-in-europe/ (дата звернення: 14.12.2022)
5. Про осіб, які вчинили кримінальні правопорушення. Сайт Офісу Генерального прокурора України. URL: https://gp.gov.ua/ua/posts/pro-osib-yaki-vchinili-kriminalni-pravoporushennya-2 (15.12.2022)
6. Кримінальний кодекс України. Кодекс. Закон України N 2341-III від 05 квітня 2001 р. База даних «Законодавство України». ВР України. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 15.12.2022)
7. Цивільний процесуальний кодекс України. Кодекс. Закон України № 1618-IV від 18 березня 2004 р. *База даних «Законодавство України».* ВР України. URL: https://zakon.rada.gov.ua/laws/show/1618-15#Text (дата звернення: 15.12.2022)

8. Про електронні документи та електронний документообіг. Кодекс. Закон України № 851-IV від 22 травня 2003 р. *База даних «Законодавство України».* ВР України. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення: 17.12.2022)
9. Козицька О.Г. Щодо поняття електронних доказів у кримінальному провадженні. *Юридичний науковий електронний журнал*. 2020. Вип. 8. С. 418–421. DOI: 10.32782/2524-0374/2020-8/103.
10. Найченко А.М., Куртакова Г.О. Електронні докази: Реалії сьогодення. *Експерт: парадигми юридичних наук і державного управління*. Вип. 1 (1). 2018. С. 72-85. DOI: 10.32689/2617-9660-2018-1-1-72-85.
11. Computer Forensics. Cybersecurity and Infrastructure Security Agency. URL: https://www.cisa.gov/uscert/sites/default/files/publications/forensics.pdf (дата звернення: 17.12.2022)
12. Digital evidence and forensics. National Institute of Justice. URL: https://nij.ojp.gov/digital-evidence-and-forensics (дата звернення: 17.12.2022)
13. Understanding Digital Forensics: Process, Techniques, and Tools. BlueVoyant. URL: https://www.bluevoyant.com/knowledge-center/understanding-digital-forensics-process-techniques-and-tools (дата звернення: 18.12.2022)
14. A Road Map for Digital Forensic Research. Digital Forensic Research Conference. URL: https://dfrws.org/wp-content/uploads/2019/06/2001_USA_a_road_map_for_digital_forensic_research.pdf (дата звернення: 18.12.2022)
15. Digital forensics. Interpol. URL: https://www.interpol.int/en/How-we-work/Innovation/Digital-forensics#:~:text=Digital%20forensics%20is%20a%20branch,crucial%20for%20law%20enforcement%20investigations (дата звернення: 18.12.2022)
16. Носов В.В. Використання цифрової криміналістики при розслідуванні кіберзлочинів. URL: https://univd.edu.ua/science-issue/issue/959 (дата звернення: 18.12.2022)
17. How Well Do You Know Digital Forensics? EC-Council. URL: https://www.eccouncil.org/what-is-digital-forensics/#phase-ix---testify-as-an-expert-witness (дата звернення: 18.12.2022)
18. What Is Digital Forensics: Applications, Processes, and Real-World Scenarios. J.S. Held. URL: https://jsheld.com/insights/articles/what-is-digital-forensics-applications-processes-and-real-world-scenarios (дата звернення: 20.12.2022)
19. Guide to Integrating Forensic Techniques into Incident Response. National Institute of Standards and Technology U.S. Department of Commerce. URL: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-86.pdf (дата звернення: 20.12.2022)
20. Кримінальний процесуальний кодекс України. Кодекс. Закон України № 4651-VI від 13 квітня 2012 р. *База даних «Законодавство України».* ВР України. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 20.12.2022)
21. Постанова від 11.02.2020 № 761/33311/15-к. Верховний Суд. Касаційний кримінальний суд. URL: https://verdictum.ligazakon.net/document/87672462 (дата звернення: 20.12.2022)
22. Кодекс адміністративного судочинства України. Кодекс. Закон України N 2747-IV від 06 липня 2005 р. *База даних «Законодавство України».* ВР України. URL: https://zakon.rada.gov.ua/laws/show/2747-15#Text (дата звернення: 21.12.2022)
23. Господарський процесуальний кодекс України. Кодекс. Закон України N 1798-XII від 06 липня 1991 р. *База даних «Законодавство України».* ВР України. URL: https://zakon.rada.gov.ua/laws/show/2747-15#Text (дата звернення: 21.12.2022)
24. Breß Sebastian, Kiltz Stefan, Schäler Martin (2013). Forensics on GPU Coprocessing in Databases – Research Challenges, First Experiments, and Countermeasures. pp. 115–130. URL: https://dl.gi.de/bitstream/handle/20.500.12116/17423/115.pdf?sequence=1&isAllowed=y (дата звернення: 21.12.2022)
25. Manes Gavin W., Downing Elizabeth, Watson Lance, Thrutchley Christopher (2007). *New Federal Rules and Digital Evidence*. pp. 31–40. URL: https://core.ac.uk/download/pdf/217157581.pdf (дата звернення: 21.12.2022)
26. Improving the Collection of Digital Evidence. National Institute of Justice. URL: https://nij.ojp.gov/topics/articles/improving-collection-digital-evidence (дата звернення: 22.12.2022)
27. Adam Chris (2020). Cyber toolkit a 'complete package' for detectives, companies to follow a criminal's digital footprint. URL: https://www.purdue.edu/newsroom/releases/2020/Q1/cyber-toolkit-a-complete-package-for-detectives,-companies-to-follow-a-criminals-digital-footprint1.html (дата звернення: 21.12.2022)
28. Baker Pam (2020). Purdue University Launches Open Source, All-in-One Network Forensics Toolkit. URL: https://www.channelfutures.com/mssp-insider/purdue-university-launches-open-source-all-in-one-network-forensics-toolkit (дата звернення: 21.12.2022)
29. Arshad Shoaib (2020). Computer Forensics Field Triage Process Model (CFFTPM). URL: https://medium.com/@shoaib629/computer-forensics-field-triage-process-model-cfftpm-67cb678ffbe8 (дата звернення: 21.12.2022)
30. FileTSAR Final Summary Overview. Purdue University. 2019. URL: https://www.ojp.gov/pdffiles1/nij/grants/254635.pdf (дата звернення: 21.12.2022)

References:

1. O'Flaherty Bea (2021). Cybersecurity ranked in European cities. Retrieved from: https://www.iotinsider.com/security/cybersecurity-ranked-in-european-cities/ [in English]
2. Vojinovic Ivana (2022). More Than 70 Cybercrime Statistics – A $6 Trillion Problem. Retrieved from: https://dataprot.net/statistics/cybercrime-statistics/#:~:text=60%20million%20Americans%20have%20experienced%20identity%20fraud%2C%20identity%20theft%20statistics%20show.&text=According%20to%20cyber%20crime%20statistics%20from%202017%2C%2016.7%20million%20consumers,consumers%20in%20a%20single%20year [in English]
3. O`Driscoll Aimee (2022). Canada cyber security and cyber crime statistics (2020-2022). Retrieved from: https://www.comparitech.com/blog/information-security/canada-cyber-crime-statistics/ [in English]

4. Skeldon Paul (2021). ANALYSIS What is the reality of real-world and cybercrime in Europe? Retrieved from: https://www.telemediaonline.co.uk/analysis-what-is-the-reality-of-real-world-and-cybercrime-in-europe/ [in English]
5. Pro osib, yaki vchynyly kryminal′ni pravoporushennya. Sayt Ofisu Heneral′noho prokurora Ukrayiny. [On persons who have committed criminal offenses.]. Website of the Office of the General Prosecutor of Ukraine. Retrieved from: https://gp.gov.ua/ua/posts/pro-osib-yaki-vchinili-kriminalni-pravoporushennya-2 [in Ukrainian]
6. Kryminal′nyy kodeks Ukrayiny. Kodeks. Zakon Ukrayiny N 2341-III 05 kvitnya 2001 r. [Criminal code of Ukraine. Code. Law of Ukraine No. 2341-III April 5, 2001.]. Baza danykh «Zakonodavstvo Ukrayiny». VR Ukrayiny. Retrieved from: https://zakon.rada.gov.ua/laws/show/2341-14#Text [in Ukrainian]
7. Tsyvil′nyy protsesual′nyy kodeks Ukrayiny. Kodeks. Zakon Ukrayiny № 1618-IV vid 18 bereznya 2004 r. [Civil Procedure Code of Ukraine. Code. Law of Ukraine No. 1618-IV dated March 18, 2004.]. Baza danykh «Zakonodavstvo Ukrayiny». VR Ukrayiny. Retrieved from: https://zakon.rada.gov.ua/laws/show/1618-15#Text [in Ukrainian]
8. Pro elektronni dokumenty ta elektronnyy dokumentoobih. Kodeks. Zakon Ukrayiny № 851-IV vid 22 travnya 2003 r. [On electronic documents and electronic document flow. Code. Law of Ukraine No. 851-IV dated May 22, 2003.]. Baza danykh «Zakonodavstvo Ukrayiny». VR Ukrayiny. Retrieved from: https://zakon.rada.gov.ua/laws/show/851-15#Text [in Ukrainian]
9. Kozyts′ka O.H. Shchodo ponyattya elektronnykh dokaziv u kryminal′nomu provadzhenni. [Regarding the concept of electronic evidence in criminal proceedings.]. Yurydychnyy naukovyy elektronnyy zhurnal. 2020. issue 8. pp. 418–421. DOI: 10.32782/2524-0374/2020-8/103 [in Ukrainian]
10. Naychenko A.M., Kurtakova H.O. Elektronni dokazy: Realiyi s′ohodennya. Ekspert: paradyhmy yurydychnykh nauk i derzhavnoho upravlinnya. issue 1 (1). 2018. pp. 72-85. DOI: 10.32689/2617-9660-2018-1-1-72-85 [in Ukrainian]
11. Computer Forensics. Cybersecurity and Infrastructure Security Agency. Retrieved from: https://www.cisa.gov/uscert/sites/default/files/publications/forensics.pdf [in English]
12. Digital evidence and forensics. National Institute of Justice. Retrieved from: https://nij.ojp.gov/digital-evidence-and-forensics [in English]
13. Understanding Digital Forensics: Process, Techniques, and Tools. BlueVoyant. Retrieved from: https://www.bluevoyant.com/knowledge-center/understanding-digital-forensics-process-techniques-and-tools [in English]
14. A Road Map for Digital Forensic Research. Digital Forensic Research Conference. Retrieved from: https://dfrws.org/wp-content/uploads/2019/06/2001_USA_a_road_map_for_digital_forensic_research.pdf [in English]
15. Digital forensics. Interpol. Retrieved from: https://www.interpol.int/en/How-we-work/Innovation/Digital-forensics#:~:text=Digital%20forensics%20is%20a%20branch,crucial%20for%20law%20enforcement%20investigations [in English]
16. Nosov V.V. Vykorystannya tsyfrovoyi kryminalistyky pry rozsliduvanni kiberzlochyniv. [The use of digital forensics in the investigation of cybercrimes.]. Retrieved from: https://univd.edu.ua/science-issue/issue/959 [in Ukrainian]
17. How Well Do You Know Digital Forensics? EC-Council. Retrieved from: https://www.eccouncil.org/what-is-digital-forensics/#phase-ix---testify-as-an-expert-witness [in English]
18. What Is Digital Forensics: Applications, Processes, and Real-World Scenarios. J.S. Held. Retrieved from: https://jsheld.com/insights/articles/what-is-digital-forensics-applications-processes-and-real-world-scenarios [in English]
19. Guide to Integrating Forensic Techniques into Incident Response. National Institute of Standards and Technology U.S. Department of Commerce. Retrieved from: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-86.pdf [in English]
20. Kryminal′nyy protsesual′nyy kodeks Ukrayiny. Kodeks. Zakon Ukrayiny № 4651-VI vid 13 kvitnya 2012 r. [Criminal Procedure Code of Ukraine. Code. Law of Ukraine No. 4651-VI of April 13, 2012.]. Baza danykh «Zakonodavstvo Ukrayiny». VR Ukrayiny. Retrieved from: https://zakon.rada.gov.ua/laws/show/4651-17#Text [in Ukrainian]
21. Postanova vid 11.02.2020 № 761/33311/15-k. [Resolution of February 11, 2020 No. 761/33311/15-k.]. Verkhovnyy Sud. Kasatsiynyy kryminal′nyy sud. Retrieved from: https://verdictum.ligazakon.net/document/87672462 [in Ukrainian]
22. Kodeks administratyvnoho sudochynstva Ukrayiny. Kodeks. Zakon Ukrayiny N 2747-IV vid 06 lypnya 2005 r. [Code of Administrative Procedure of Ukraine. Code. Law of Ukraine N 2747-IV of July 6, 2005.]. Baza danykh «Zakonodavstvo Ukrayiny». VR Ukrayiny. Retrieved from: https://zakon.rada.gov.ua/laws/show/2747-15#Text [in Ukrainian]
23. Hospodars′kyy protsesual′nyy kodeks Ukrayiny. Kodeks. Zakon Ukrayiny N 1798-XII vid 06 lypnya 1991 r. [Economic Procedural Code of Ukraine. Code. Law of Ukraine N 1798-XII of July 6, 1991.]. Baza danykh «Zakonodavstvo Ukrayiny». VR Ukrayiny. Retrieved from: https://zakon.rada.gov.ua/laws/show/2747-15#Text [in Ukrainian]
24. Breß Sebastian, Kiltz Stefan, Schäler Martin (2013). Forensics on GPU Coprocessing in Databases – Research Challenges, First Experiments, and Countermeasures. pp. 115–130. Retrieved from: https://dl.gi.de/bitstream/handle/20.500.12116/17423/115.pdf?sequence=1&isAllowed=y [in English]
25. Manes Gavin W., Downing Elizabeth, Watson Lance, Thrutchley Christopher (2007). New Federal Rules and Digital Evidence. pp. 31–40. Retrieved from: https://core.ac.uk/download/pdf/217157581.pdf [in English]
26. Improving the Collection of Digital Evidence. National Institute of Justice. Retrieved from: https://nij.ojp.gov/topics/articles/improving-collection-digital-evidence [in English]
27. Adam Chris (2020). Cyber toolkit a ‘complete package’ for detectives, companies to follow a criminal’s digital footprint. Retrieved from: https://www.purdue.edu/newsroom/releases/2020/Q1/cyber-toolkit-a-complete-package-for-detectives,-companies-to-follow-a-criminals-digital-footprint1.html [in English]
28. Baker Pam (2020). Purdue University Launches Open Source, All-in-One Network Forensics Toolkit. Retrieved from: https://www.channelfutures.com/mssp-insider/purdue-university-launches-open-source-all-in-one-network-forensics-toolkit [in English]
29. Arshad Shoaib (2020). Computer Forensics Field Triage Process Model (CFFTPM). Retrieved from: https://medium.com/@shoaib629/computer-forensics-field-triage-process-model-cfftpm-67cb678ffbe8 [in English]
30. FileTSAR Final Summary Overview. Purdue University. 2019. Retrieved from: https://www.ojp.gov/pdffiles1/nij/grants/254635.pdf [in English]