УДК 349.2
DOI https://doi.org/10.32782/chern.v3.2022.20

М. Д. Денисовський
кандидат юридичних наук,
доцент кафедри права
Галицького фахового коледжу імені В'ячеслава Чорновола
orcid.org/0000-0002-2265-4190

РЕАЛІЇ ЗАСТОСУВАННЯ ЦИФРОВОЇ КРИМІНАЛІСТИКИ ПІД ЧАС ЗДІЙСНЕННЯ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ

З кожним роком інноваційні технології все більше впроваджуються в різні сфери людської життєдіяльності, і юриспруденція не є винятком. В останні роки як в загальну, так і в професійну лексику громадян увійшли нові терміни, такі як: інформатизація, цифрові технології, віртуальна реальність, інформаційно-комунікативний простір. А в професійній діяльності кожен з нас все частіше застосовує комп'ютери, різні гаджети, програми, що дозволяє прискорити процеси взаємодії, полегшити доступ, збір, зберігання, передачу і обробку інформації при мінімумі фізичних зусиль.

Ми добре усвідомлюємо, що суспільство під впливом комп'ютеризації змінилося і цифрова реальність стала виступати не міфом, не казкою, не далеким майбутнім, а нашим сьогоденням. Таким чином сучасні інформаційні технології вивели криміналістику на новий етап розвитку, внаслідок чого з'явилася нова галузь криміналістики – цифрова криміналістика.

У даній статті досліджується новітня галузь криміналістики-цифрова криміналістика, яка є прикладною наукою про розкриття кримінальних правопорушень, пов'язаних з комп'ютерною інформацією, про дослідження цифрових доказів, методи пошуку, отримання і закріплення таких доказів.

Автор статті проаналізував складові частини цифрової криміналістики, оцінив тенденції розвитку цієї науки на сучасному етапі та спрогнозував подальший розвиток цифрової криміналістики в Україні, надавши свої рекомендації.

Хоч в Національній поліції й було створено спецпідрозділ по боротьбі з кіберзлочинністю, проте вітчизняні правоохоронні органи не мають змоги використовувати весь спектр можливостей, що надають сучасні технології. А тому необхідно якомога швидше завершити процес інтеграції вітчизняних правоохоронних структур у європейський простір та чітко прописати у національних законодавчих актах процедуру збору, верифікації, зберігання та застосування електронних (цифрових) доказів.

Ключові слова: цифрова криміналістика, електронні (цифрові) докази, цифрові відбитки, кримінальне провадження, Протокол Берклі.

Denysovskyi M. D. **REALITIES OF APPLICATION OF DIGITAL FORENSICS DURING CRIMINAL PROCEEDINGS**

Every year, innovative technologies are increasingly introduced into various spheres of human life, and jurisprudence is no exception. In recent years, new terms such as: informatization, digital technologies, virtual reality, information and communication space have entered both the general and professional vocabulary of citizens. And in our professional activities, each of us increasingly uses a computer, various gadgets, programs, which allows us to speed up interaction processes, facilitate access, collection, storage, transmission and processing of information with a minimum of physical effort.

We are well aware that society has changed under the influence of computerization and digital reality has become not a myth, not a fairy tale, not a distant future, but our present. Thus, modern information technologies brought forensics to a new stage of development, as a result of which a new branch of forensics appeared – digital forensics.

This article examines the newest branch of forensics – digital forensics, which is an applied science about the disclosure of criminal offenses related to computer information, about the study of digital evidence, methods of finding, obtaining and securing such evidence.

The author of the article analyzed the components of digital forensics, assessed the trends in the development of this science at the current stage and predicted the further development of digital forensics in Ukraine, giving his recommendations.

Although a special unit for combating cybercrime was created in the National Police, domestic law enforcement agencies are not able to use the full range of opportunities provided by modern technologies. Therefore, it is necessary to complete the process of integration of domestic law enforcement structures into the European space as soon as possible and to clearly prescribe in national legislative acts the procedure for collecting, verifying, storing and using electronic (digital) evidence.

Key words: digital forensics, electronic (digital) evidence, digital fingerprints, criminal proceedings, Berkeley Protocol.

Постановка проблеми. На сьогоднішній час цифрові технології, безперечно, проникають у всі сфери життєдіяльності людини, тай суспільства в цілому. Не є винятком і наука криміналістика. Оскільки не можливо уявити габітологію – без комп'ютерних засобів створення суб'єктивних портретів й відновлення зажиттєвого вигляду людини за кістковими залишками її черепу, дактилоскопію – без автоматизованого опрацювання й ідентифікації слідів пальців рук, зброє-

знавство – без комп'ютерних інструментів дослідження й ототожнення слідів пострілу на гільзах і кулях, документознавство – без комп'ютерних методів обробки й дослідження документів, а судову фотографію та відеозапис – без цифрової фото – і відеозйомки. У розслідуванні більшості кримінальних правопорушень безумовно застосовується так звана автоматизована методика розслідування. Вона являє собою технічний засіб у вигляді інформаційної системи, який ґрунтується на типовій комп'ютерній моделі відповідного кримінального правопорушення, виокремленого у певну групу за відповідними криміналістичними критеріями. За суттю, мова йде про цілісний напрям криміналістики – про так звану електронну (цифрову) криміналістику.

Оскільки використання даного напряму являється досить новітнім, то існує безліч як негативних, так і позитивних поглядів науковців – криміналістів та інших представників процесуальних наук, щодо визначення необхідності та доцільності вивчення цифрової криміналістики. Висновки аналітиків і становлення цифрової криміналістики, на даний час, невтішні, а можливості одержання й використання отриманої таким чином інформації у кримінально – судочинних напрямах більшості слідчим, прокурорам і суддям, на жаль, невідомі. В першу чергу це тому, що для дослідження, комп'ютерних засобів, систем, мереж та оброблюваної за їх допомогою інформації необхідно мати особливий набір криміналістичних знань, за допомогою яких можливо швидко та ефективно провести розслідування кримінального правопорушення. А для ефективного та правомірного застосування отриманої цифрової інформації – необхідно чітко закріпити процедуру її отримання в законодавчому рівні.

Стан дослідження теми. Цифрова криміналістика є відносно новою наукою, що зародилася лише у 80-ті роки XX століття, а тому її дослідженням в Україні займаються доволі небагато дослідників. Серед авторів, які торкаються окремих проблем цифрової криміналістики варто виокремити наступних: Бутузов В.М., Власова С.В., Іщенко Є.П., Нечаєва Н.Б. тощо. Щодо іноземних досліджень цифрової криміналістики, то однією із провідних науковців є Marie-Helen Maras.

Метою даної роботи є дослідження нової сфери криміналістики – цифрової криміналістики, зокрема висвітлення теоретичних та практичних реалій її застосування під час здійснення кримінального провадження, формулювання науково обґрунтованих пропозицій і рекомендацій з удосконалення законодавства України.

Викладення основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів. Ще в 70-ті роки минулого століття було помічено, що «стрімкі, динамічні зміни в соціальній структурі суспільства породжуються лавиноподібним процесом інновацій, матеріалізованих наукових ідей, наукових відкриттів, технічних винаходів і розробок, з принципово новими технологічними процесами [1, с. 7].

Так, дійсно в результаті науково-технічного прогресу, що зумовлений впливом світових інформаційних потоків, інтеграцією знань про можливості протидії злочинності за допомогою науково-технічних досягнень сучасного суспільства, запроваджуються різні інновації щодо застосування техніко-криміналістичних засобів і технологій в кримінальному провадженні. Тому в сучасних умовах у слідчій діяльності пропонується використання новітніх науково-технічних засобів і технологій при проведенні гласних та негласних слідчих (розшукових) дій, зокрема: інноваційних матеріалів роботи зі слідами, приладів, що дозволяють проведення експрес-аналізів, засобів аудіо-, відеоконтролю, систем спостереження, цифрової фототехніки та відеозапису, електронних контролерів, безпілотних літальних апаратів тощо.

Безперечно новітні технології використовуються не лише працівниками правоохоронних органів, а й безпосередньо правопорушниками при вчиненні кримінальних правопорушень, пов'язаних з використанням інформаційно – телекомунікаційної мережі Інтернет, кіберзлочинів, кримінальних правопорушень, пов'язаних з IT-технологіями і т.п. Саме тому, було виділено цифрову криміналістику, як одну із галузей дослідження науки криміналістики в цілому, яка «зосереджена на кримінально-процесуальному праві і доказах стосовно комп'ютерів і пов'язаних з ними пристроїв», такими, як мобільні пристрої (телефони, смартфони тощо), ігрові приставки та інші пристрої, що функціонують через Інтернет (пристрої для здоров'я та фітнесу та медичні прилади тощо) [2, с. 177].

Таким чином, цифрова криміналістика – це прикладна наука про розкриття кримінальних правопорушень, пов'язаних з комп'ютерною інформацією, що має відношення до процесу збору, отримання, збереження, аналізу та подання електронних доказів (також відомих як цифрові докази) з метою отримання оперативно-розшукових відомостей і здійснення розслідування та кримінального переслідування по відношенні до різних видів кримінальних правопорушень, включаючи кіберзлочини.

Одним із основних принципів цифрової криміналістики являється принцип обміну Едмона Локара, який полягає у тому, що об'єкти і поверхні завжди вступають один з одним в контакт, а тому відбувається перехресне перенесення матеріалів. З цього випливає, що будь яка особа після використання інформаційно-комунікаційних технологій, залишають цифрові сліди (відбитки), за

допомогою яких можливо дізнатись інформацію про вік, стать, громадянство, расову та етнічну приналежність, думки, уподобання, звички, хобі, сексуальну орієнтацію, історію хвороби і проблеми зі здоров'ям, психологічні розлади, статус, зайнятість, приналежність до будь-якої спільноти, особисті відносини, геолокацію, розпорядок дня та інші активності.

Такі цифрові відбитки можуть бути активними або пасивними. Активний цифровий відбиток створюється даними, наданими користувачем, такими як персональні дані, відео, зображення і коментарі, що розміщуються в додатках, на веб-сайтах, електронних дошках оголошень, в соціальних мережах та інших онлайн-форумах. А пасивні – це дані, які особи залишають користуючись Інтернетом та цифровими технологіями без попереднього умислу (наприклад: історія переглядів в браузері).

Дані активних і пасивних цифрових відбитків в подальшому можуть використовуватись як доказ скоєння кримінального правопорушення або ж доведення або спростування твердження про певний факт, визначення причетності або непричетності підозрюваного до вчинення правопорушення тощо.

Джерелами доказів в електронній формі можуть бути: різноманітні носії інформації; моноблоки, мобільні пристрої (мобільні телефони, планшетні комп'ютери), цифрові камери, роутери, маршрутизатори, комп'ютерні мережі, глобальна мережа Інтернет, звуко- та відеозаписи тощо, тобто джерелом доказів може бути будь-який електронний пристрій, який знаходиться на місці обшуку. Варто також зазначити, що постійно з'являються нові види електронних пристроїв, які можуть містити електронні докази [3, с. 7].

Наприклад, одним з цифрових пристроїв, які накопичують значний обсяг даних про його користувачів, є Amazon Echo (з голосовим помічником Alexa). Дані, що накопичуються цим пристроєм, можуть містити цінні відомості про користувачів, зокрема: інформацію про їх інтереси, уподобання, запити, покупки і інші види активності, а також про їх місцезнаходження (щоб, наприклад, визначити, чи знаходяться вони вдома або поза будинком, шляхом перегляду міток часу і аудіозаписів взаємодії з мовним помічником Alexa). Даний пристрій вже використовувався в Сполучених Штатах Америки при розслідуванні справи про вбивство. Хоча звинувачення проти підозрюваного були в кінцевому підсумку зняті, це справа наочно продемонструвала, що дані, зібрані з використанням нових цифрових технологій, неминуче будуть представлені в суді як доказ.

у Китаї, на даний час, вагоме місце в цифровій криміналістиці посів штучний інтелект. За допомогою якого можливо із зображення з вуличної камери розпізнати обличчя та здійснити пошук особи у всіх відомих базах даних. Натомість в нашій державі, цей процес ще не є належно вдосконаленим, але для ідентифікації потенційних злочинців і загиблих, невелика кількість слідчих вже використовує додаток з розпізнавання облич Clearview AI.

Ідею щодо отримання доказів із відкритих джерел не всі одразу сприйняли всерйоз тому, що цифрові дані часто важко верифікувати і вони можуть бути дуже часто сфальсифіковані. Однак у європейських країнах, де цифрова криміналістика давно являється невід'ємним атрибутом розслідування кримінальних правопорушень, верифікація даних зазвичай прописана у законодавстві.

Всі вимоги щодо процедури збору, використання й збереження інформації з відкритих джерел передбачені у протоколі Берклі, над яким протягом трьох років працювало понад 150 експертів і представників Центру прав людини університету Берклі та Офісу Верховного комісара ООН з прав людини. Протокол Берклі являє собою практичний посібник з ефективного використання цифрової інформації з відкритим вихідним кодом при розслідуванні порушень міжнародного кримінального права, права людини та гуманітарного права.

Чому ж Протокол Берклі настільки важливий? А тому, що керуючись ним можна отримати доступ до великої кількості даних, зібраних з різних, незалежних одне від одного джерел, не обмежуючись територією, суб'єктом отримання та подачі інформації.

Саме в ньому передбачено основоположні міжнародні стандарти для проведення онлайн-розслідування порушень, методи і процедури збирання, аналізу, перевірки та зберігання контенту із соціальних мереж та відкритих джерел з дотриманням професійних, правових та етичних принципів. При цьому, такими джерелами можуть бути, як контент створений користувачами у соціальних мережах, таких як YouTube, Facebook, Instagram, так і дані супутникових знімків, що зможуть бути використанні в рамках різних кримінальних проваджень.

З точки зору роботи правоохоронних органів, такі джерела можуть слугувати додатковою доказовою базою по справі і надаватимуть слідчим ширше уявлення про осіб або події. Але з іншого боку, таким особам варто досить уважно перевіряти інформацію з відкритих джерел, оскільки вона може бути неправдивою, неточною або хибною. Це полягатиме у витрачанні більшого обсягу часу на досудове розслідування і відповідно, на судовий розгляд, оскільки потенційно можуть існувати сотні тисяч фотографій, відео та публікацій, які мають бути перевірені та дослідженні всіма сторонами процесу.

На мою думку, в реаліях сучасного світу «рамки визначення» правдивої чи неправдивої інформації настільки стерлись, що в будь-якому випадку збір та використання інформації з відкритих джерел, є вигідним для всіх сторін, оскільки допоможе підвищити стандарти розслідування та судового розгляду справи. В сучасному світі цифрова криміналістика суттєво доповнює традиційні методи розслідування, адже практично все має свій цифровий слід, знищити який майже неможливо.

Як би це прикро не звучало, на жаль, багато прикладів нам надає саме український досвід. Тому що саме зараз ця процедура використовується українськими неурядовими громадськими організаціями та журналістами у розслідуванні злочинів, вчинених російськими військовослужбовцями та високопосадовцями на території України. Так, на сьогоднішній час, Протоколом Берклі уже керуються в Офісі Генерального прокурора разом з українськими та міжнародними партнерами під час збору доказів про злочини російської армії (https://warcrimes.gov.ua/), а також відома організація Bellingcat, яка веде спеціальний портал воєнних злочинів Росії в Україні https://bit.ly/3tvHMvb.

Не можливо не згадати події у місті Буча Київської області, що тривали від 27.02.2022 р. до 31.03.2022 р., в результаті яких було знайдено велику кількість тіл вбитих цивільних громадян. Після оприлюднення кадрів російська влада почала просувати ідею, що це сфальсифікована ситуація, а тіла були підкинуті після звільнення міста. І тільки супутникові знімки допомогли довести, що тіла з'явилися саме під час російської окупації [4].

Однак зараз виникає питання, чи будуть дані цифрові докази допущені як докази у судових провадженнях в нашій державі. Адже інститут електронних доказів в КПК України не деталізований та не врегульований на достатньому рівні, саме тому питання внесення відповідних змін до КПК України є нагальним, в тому числі щодо чіткого визначення поняття та видів електронних доказів, а також доповнення переліку процесуальних джерел доказів, і розмежування поняття електронного документа як офіційного документа та інших документів, які подаються в електронній формі.

Щодо особливостей поводження з цифровими доказами, то ще у 2012 році Міжнародна організація зі стандартизації (ISO) і Міжнародна електротехнічна комісія (МЕК) опублікували міжнародні стандарти, що стосуються поводження з цифровими доказами (ISO / IEC 27037 Керівництво по ідентифікації, збирання, одержання і збереження свідчень, представлених в цифровій формі [5]).

Даними стандартами пропонуються чотири етапи поводження з цифровими доказами, а саме:

Ідентифікація – включає в себе пошук і розпізнавання відповідних доказів, а також їх документування. На цьому етапі пріоритетні завдання збору доказів визначаються на основі цінності і мінливості доказів. У порівнянні з традиційними доказами (наприклад, паперовими документами, зброєю, контрольованими речовинами і т.д.), цифрові докази створюють унікальні складності при аутентифікації через обсяг доступних даних, їх швидкості (тобто швидкості, з якою вони створюються і передаються), нестійкості (вони можуть швидко зникнути при перезапису або видаленні) і уразливості (їх легко можна обробити, змінити або пошкодити).

Збір – передбачає збір всіх цифрових пристроїв, які можуть містити дані, що мають доказову цінність. Ці пристрої згодом транспортуються в лабораторію судової експертизи або іншу установу для збору і аналізу цифрових доказів. Цей процес називається збором даних в статичному режимі. Однак бувають випадки, коли збір даних в статичному режимі є практично нездійсненним. У таких ситуаціях здійснюється збір даних в реальному часі.

Отримання – цифрові докази необхідно отримувати без шкоди для цілісності даних. Таке отримання даних без їх зміни здійснюється шляхом створення копії вмісту цифрового пристрою (процес, відомий як створення неспотвореного образу) з використанням пристрою (блокувальника запису), який призначений для запобігання зміни даних в процесі копіювання. Для того щоб визначити, чи є дублікат точною копією оригіналу, значення хешфункції розраховується з використанням математичних обчислень; тут для отримання значення хешфункції використовується криптографічна хешфункція. Якщо значення хешфункції для оригіналу та копії збігаються, то вміст копії є точно таким же, що і в оригіналі.

Збереження – цілісність цифрових пристроїв і цифрових доказів – «процес, за допомогою якого слідчі забезпечують охорону місця кримінального правопорушення (або події) і збереження доказів протягом всього періоду провадження у справі. У журнал реєстрації записують інформацію про те, хто здійснював збір доказів, де і яким чином вони були зібрані, які особи отримали ці докази, і коли вони їх отримали. Ретельне документування процесу цифрової судової експертизи на кожному етапі має важливе значення для забезпечення допустимості доказів у суді.

У країнах Європи, Америці та, зокрема, у Міжнародному кримінальному суді вже існує практика залучення цифрових доказів до справ. Ці норми регулюються місцевим законодавством та здебільшого опираються на Протокол Берклі й принципи SWGDE по роботі з цифровими доказами. Проте питання цифрових доказів та їхньої допустимості у контексті українського законо-

давства залишається відкритим, тому процедура їхнього збору, верифікації, зберігання та застосування має бути чітко прописана у національних законодавчих актах.

Висновки з даного дослідження. На даний час доказовою базою достатньої частки кримінальних правопорушень є електронні (цифрові) докази, оскільки сучасні правопорушення все більше здійснюється в кіберпросторі та за допомогою інформаційних технологій і систем.

Динаміка вчинення кримінальних правопорушень з використання інформаційно-телекомунікаційних технологій постійно зростає. Вбачається, що, вдосконалення та застосування даної науки на практиці, в умовах активного розвитку можливостей мережі Інтернет, новітніх технологій, криміналістичної техніки, нових способів вчинення правопорушень, сприятиме не тільки розвитку окремих теоретичних положень криміналістичної науки, але й позитивно відобразиться на практичному використанні даних знань при розкритті та розслідуванні кримінальних правопорушень.

Хоч цифрова криміналістика в розвинутих країнах розвивається стрімкими темпами та гідно протистоїть поширенню кіберзлочинності, наша держава також не є пасивною в цьому впровадженні.

Після створення в складі національної поліції спеціального підрозділу з боротьби з кіберзлочинністю, працівники правоохоронних органів активно використовують можливі техніки та прилади новітньої цифрової криміналістики.

Проте для того, щоб вітчизняні правоохоронні органи дійсно могли використовувати весь спектр можливостей, які надають сучасні технології, необхідно якомога швидше завершити процес інтеграції вітчизняних правоохоронних структур в європейський простір.

Зараз інститут електронних доказів в КПК України не деталізований та не врегульований на достатньому рівні, саме тому питання внесення відповідних змін до КПК України є нагальним, в тому числі щодо чіткого визначення поняття та видів електронних доказів, а також доповнення переліку процесуальних джерел доказів, і розмежування поняття електронного документа як офіційного документа та інших документів, які подаються в електронній формі.

Література

1. Лазар М.Г., Лейман И.И. НТР и нравственные факторы научной деятельности. Ленинград, «Наука». 1978. 156 с.

2. Колодіна А.С., Федорова Т.С. Цифрова криміналістика: проблеми теорії і практики. Київський часопис права. 2022. № 1. С. 176-180. URL: http://kyivchasprava.kneu.in.ua/index.php/kyivchasprava/article/view/151/139.

3. Гуцалюк М. В., Гавловський В. Д., Хахановський В. Г. та ін. за заг. ред. Корнейка О. В. Використання електронних (цифрових) доказів у кримінальних провадженнях: методичні рекомендації. Київ : Видавництво Національна академія внутрішніх справ. 2020. Вид. 2. 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.

4. Гюндуз Мамедов. Цифрова криміналістика. Як це допомогло зібрати докази злочинів у Бучі? (08 червня 2022 р.) *Електронний журнал «НВ Погляди»*, 2022. URL: https://nv.ua/ukr/opinion/viyna-v-ukrajini-yak-cifrova-kriminalistika-vikrivaye-zlochini-rf-v-ukrajini-novini-ukrajini-50248411.html.

5. ISO/IEC 27037:2012 Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. URL: https://www.iso.org/standard/44381.html.