ЦИФРОВА КРИМІНАЛІСТИКА У ПЕРІОД ВІЙНИ В УКРАЇНІ: МОЖЛИВОСТІ ВИКОРИСТАННЯ СПЕЦІАЛЬНИХ ЗНАНЬ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Др., **Катерина Латиш,**
Національний юридичний університет імені Ярослава Мудрого,
Pushkins'ka St, 77, 61024 Kharkiv, Kharkiv Oblast, Ukraine,
<latysh78@gmail.com>

Анотація

Цифрова криміналістика набуває все більшої актуальності та стає однією з ключових складових традиційної криміналістики. Цифрові криміналістичні знання застосовуються під час проведення слідчих (розшукових) дій та у ході призначення відповідних судових експертиз не лише щодо кримінальних правопорушень у сфері інформаційних технологій, але й щодо розслідування широкого кола правопорушень, які вчиняються під час війни та окупації. За таких обставин правоохоронні органи все більше шукають та аналізують інформацію, отриману з відкритих джерел, через чат-боти («War Crime Bot», «STOP Russian War», «Стоп мародер», «Знайди зрадника»), у соціальних мережах та телеграм-каналах, що є новим для правозастосовчої системи України. Законодавець зреагував на нагальні потреби та впровадив до кримінально-процесуального законодавства України відповідні зміни стосовно особливостей збирання цифрових доказів, які й будуть розглянуті у межах цієї статті. Важливим інструментом верифікації та перевірки достовірності цифрової інформації залишається інститут судової експертизи, за допомогою якого й можуть проводитися криміналістичні дослідження цифрової техніки, вилучення з них і аналіз медіа-даних, переписки, телефонних книг, документів, відновлення та копіювання даних з усіх типів технічних носіїв. Необхідним вбачається й технічний супровід слідчих (розшукових) дій, в межах якого надається спеціальна комп'ютерно-технічна допомога у пошуку та фіксації слідів, залишених на місці події. Розглянуто інструменти цифрової криміналістики та запропоновано вимоги до цифрових доказів з урахуванням тенденцій, які висуває дія воєнного стану.

Ключові слова: кібервійна, спеціальні знання в ІТ-сфері, цифрова криміналістика, розслідування військових злочинів, цифрові докази.

Вступ

Збройна агресія Російської Федерації та бойові дії на території України оголили цифрові потреби криміналістики та продемонстрували нагальну необхідність впровадження дистанційних електронних інструментів пошуку, збору, фіксації та дослідження слідів кримінальних правопорушень. Традиційні криміналістичні науково-технічні засоби та форми використання спеціальних знань можуть працювати обмежено через небезпеку для всіх учасників слідчих (розшукових) дій, а також через неможливість безпосереднього доступу до місця події. Тому виникає потреба у пошуку в мережі Інтернет, соціальних мережах, телеграм-каналах та інших відкритих публічних середовищах інформації, відзнятої учасниками цієї події та викладеної у мережу, а також використання інших інструментів цифрової криміналістики. Більше того, є необхідність у розробленні методики відбору медіа-файлів з технічних носіїв приватних осіб, які ніде ці дані не розміщували у публічному просторі, але готові надати уповноваженим правоохоронним органам цю інформацію для огляду та подальшого дослідження. Для України така практика є новою та нетрадиційною, на відміну від країн Європейського Союзу, де цифрова криміналістика вже на високому рівні розвитку. Тому законодавчі та наукові розробки з цього приводу є критично важливими і у подальшому досвід такого впровадження з урахуванням триваючих складних воєнних умов в Україні може бути використаний також і іншими країнами.

Тому метою дослідження є виокремлення можливостей цифрової криміналістики, які можуть бути використанні під час розслідування кримінальних правопорушень у період воєнних дій, а також проаналізовані форми використання спеціальних знань у сфері інформаційних технологій та висунуто вимоги до цифрових (електронних) доказів.

Розвиток цифрової криміналістики відбувається у трьох основних напрямах: 1) формування окремої наукової галузі в криміналістиці; 2) застосування спеціальних знань під час роботи з цифровими доказами; 3) проведення судових експертиз (зокрема, комп'ютерно-технічної експертизи)[1]. Цифрову криміналістику можна визначити також в якості засобу протидії кібервійні, складовою якої є інформаційна війна (фейки), та в якості засобу збирання та фіксування інформації з відкритих та інших джерел, яка у подальшому може стати доказом.

У Стратегії кібербезпеки України, затвердженої Указом Президента України від 26.08.2021р. №447/2021,

1 Шепітько, В., Шепітько, М. (2021). Доктрина криміналістики та судової експертизи: формування, сучасний стан і розвиток в Україні. *Право України.* 8, С. 21.

визначено, що однією з загроз кібербезпеці України є гібридна агресія Російської Федерації проти України у кіберпросторі. Держава-агресор невпинно нарощує арсенал кіберзброї наступального призначення, застосування якої може викликати невиправні, незворотні руйнівні наслідки. Кібератаки Російської Федерації спрямовані, насамперед, на інформаційно-комунікаційні системи державних органів України та об'єкти критичної інформаційної інфраструктури з метою виведення їх з ладу (кібердиверсія), отримання прихованого доступу і контролю, здійснення розвідувальної та розвідувально-підривної діяльності. Кібератаки також активно використовуються державою-агресором як елемент спеціальних інформаційних операцій з метою маніпулятивного впливу на населення, втручання у виборчі процеси та дискредитації української державності[2]. Так, В. Ю. Шепітько зазначає, що досягнення стратегічних цілей (військових, політичних, економічних) окремих держав-злочинниць (їхніх керівників) відбувається за допомогою інформаційної війни (information war) – процесу сугестивного впливу на групи людей за допомогою спеціально підготовлених комунікативних технологій та інформаційних матеріалів[3].

Цифрова криміналістика розробляє дієві інструменти для розслідування злочинів, особливо під час війни, збройних конфліктів та окупації території, коли доступ до місця події обмежений або взагалі не доступний. Крім того, значний обсяг інформації знаходиться в Інтернет-мережі, яка потенційно, за певних умов, може бути використана в якості доказів вчинення воєнних та інших кримінальних правопорушень. Ці комп'ютерні дані, що відбиваються в електронному вигляді на різних ресурсах та носіях, стають джерелом криміналістично значущої інформації, отримання якої і стає завданням правоохоронних органів[4]. Однак, не достатньо дослідженими та нормативно закріпленими є правила збирання таких електронних доказів.

Серед інструментів цифрової криміналістики можна виділити, зокрема, такі:

- пошук за ключовими словами та хештегами, списки яких попередньо підготовлені,
- моніторинг радарів та системи офіційного моніторингу суден Marine Traffic,
- аналіз супутникових знімків,
- використання технології аналізу «великих даних» (Big Data);
- аналіз геолокаційних міток,
- дослідження фото- та відеоматеріалів у відкритому доступі та наданих слідству,
- використання програм для аналізу та обробки цифрових зображень,
- дослідження телефонних розмов,
- аналіз електронних пристроїв,
- аналіз ігрових систем,
- система розпізнавання облич і пошуку їх у відповідних базах даних (в Україні використовують додаток з розпізнавання облич Clearview AI для ідентифікації потенційних злочинців і загиблих).

Саме завдяки інструментам цифрової криміналістики та даних з відкритих джерел були встановлені факти застосування Російською Федерацією забороненої зброї у вигляді фосфорних, вакуумних та касетних бомб. Інший приклад, це масові вбивства та інші злочини, які були вчинені у містах Київської області у період з 27 лютого 2022р. по 31.03.2022р.. Збройні Сили України, звільнивши місто, знайшли велику кількість тіл цивільних громадян, що лежали на узбіччях. Після оприлюднення кадрів з цими тілами російська влада почала просувати ідею, що це «постанова» і тіла були підкинуті після звільнення міста. Проте супутникові знімки допомогли довести, що тіла з'явилися саме під час російської окупації. У цьому контексті не можна також забувати про масові поховання цивільних людей. Оскільки вони, здебільшого, знаходяться на тимчасово окупованих територіях і до них немає доступу – цифрова криміналістика, а саме аналіз та порівняння супутникових знімків, може суттєво допомогти у встановленні винних. Так відбулося і з масовим похованням біля церкви святого Андрія в Бучі, що було зафіксоване на супутникових знімках Maxar[5]. Також можуть використовуватися фото- та відеозаписи зі стаціонарних відеокамер, які розташовані на комерційних та приватних об'єктах. Так, на записах від 4 березня зафіксовано, як росіяни вишикували в колони полонених мирних мешканців перед тим, як убити їх[6].

Однак, слід вказати, що для української системи права практика отримання доказів з відкритих джерел є новою та незвичною. На етапі пошуку, виявлення та фіксації знайдене має статус інформації, яка лише потенційно за умов відповідності певним критеріям зможе стати доказом. Разом з тим, у березні 2022 року Законом України «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам» (далі – Закон України №2137-IX) було змінено нормативно-правове регулювання відносно використання електронних доказів. Так, зокрема було надано спеціалісту право надавати «консультації, пояснення та довідки». Окремо доповнено перелік прав спеціаліста та надано право «надавати довідки з питань, що належать

2 Стратегії кібербезпеки України, затвердженої Указом Президента України від 26.08.2021р. №447/2021: <https://www.president.gov.ua/documents/4472021-40013>.

3 Шепітько, В.(2021). Вступ до актуальної теми. *Право України.* 8, С. 10.

4 Костенко, М. В. (2019). Особливості інноваційного процесу в сфері криміналістики. *Інноваційні методи та цифрові технології в криміналістиці, судовій експертизі та юридичній практиці: матеріали міжнар. «круглого столу».* С. 74.

5 Мамедов, Г. *Цифрова криміналістика. Як це допомогло зібрати докази злочинів у Бучі?*: <https://nv.ua/ukr/opinion/viyna-v-ukrajini-yak-cifrova-kriminalistika-vikrivaye-zlochini-rf-v-ukrajini-novini-ukrajini-50248411.html>.

6 *New Evidence Shows How Russian soldiers executed men in Bucha*: <https://www.nytimes.com/2022/05/19/world/europe/russia-bucha-ukraine-executions.html>.

до сфери його знань, у випадках, передбачених ч.3 ст. 245[1] КПК України». Чинний КПК України і положення Закон України №2137-IX не деталізують нормативних вимог до змісту такої довідки. Із цього можна зробити висновок, що вона як джерело доказів відноситиметься до документів[7].

Законодавець пішов прогресивним шляхом та впровадив можливість зняття показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису від особи, яка є власником або володільцем відповідних приладів або засобів, необхідних для з'ясування обставин, що мають значення для кримінального провадження, копій фото- або кінозйомки, відеозапису, здійснених у публічно доступних місцях, у тому числі в автоматичному режимі, за виключенням місць, що відносяться до приватних помешкань осіб. Таке зняття показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису здійснюється на підставі постанови слідчого, прокурора та, за необхідності, за участю спеціаліста. Також сформульовано вимоги до змісту такої постанови про зняття показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису повинна містити: 1) найменування кримінального провадження та його реєстраційний номер; 2) відомості про власника або володільця відповідних приладів або засобів; 3) період часу, за який має бути здійснено зняття показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису. Зняття показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису здійснюється у присутності слідчого, прокурора шляхом самостійного копіювання особою, яка є власником або володільцем відповідних приладів та засобів, або копіювання такою особою за участю спеціаліста відповідних записів на носії, які надаються слідчим, прокурором. Надання таких копій на носіях, особі, яка є власником або володільцем відповідних приладів та засобів, здійснюється за бажанням такої особи. За результатами здійснення зняття показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису складається протокол[8].

У цьому контексті важливим є питання допустимості даних, що містяться у джерелах з відкритим доступом, зокрема у соціальних мережах. Тут є проблеми пов'язані з встановленням джерела походження та автентичності таких даних. Лист-орієнтування Офісу Генерального прокурора від 28 серпня 2021 року стосовно питань збереження цифрової інформації, отриманої з відкритих джерел, відсилає до так званого Протоколу Берклі, що був розроблений школою права Університету Каліфорнії в Берклі разом з представниками ООН. Цей Протокол Берклі містить основні міжнародні стандарти дистанційного розслідування, криміналістичні засоби збирання, аналізу та зберігання електронних слідів та цифрової інформації з дотриманням професійних, правових та етичних принципів. У ньому запропоновано цикл розслідування з використанням даних у відкритому доступі, однак, підкреслено, що такі розслідування рідко бувають лінійними і часто вимагають повторення цього процесу з огляду на циклічність побудови. Так, до першого етапу відносяться процеси виявлення інформації шляхом здійснення онлайн-запитів у пошукових системах на індексованих веб-сайтах, на платформах соціальних мереж та у відкритих базах даних. Далі здійснюється інтерпретація даних, висновків та виявлення прогалин для подальшого дослідження («слідчий аналіз»), надається попередня оцінка шляхом визначення необхідності збирання, а також здійснюється перевірка процесів оцінки надійності джерел та контенту. Останні два етапи присвячені збору цифрових елементів з Інтернету та подальшого збереження[9]. Крім того, можуть бути використані принципи SWGDE по роботі з цифровими доказами.

Що стосується національного законодавства, то в Україні діють такі стандарти до зібраних інтернет-даних: 1) Національний стандарт України «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів», який стосується не лише цифрових доказів у відкритих джерелах, а й цифрових даних на конкретних пристроях (ДСТУ ISO/IEC 27037:2016 (ISO/IEC 27037:2012, IDT)). Цей стандарт був прийнятий з метою гармонізації національної нормативної бази з міжнародним законодавством і розроблений методом перекладу тексту з відповідного міжнародного стандарту ISO/IEC 27037:2012 «Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence», що був прийнятий спільним технічним комітетом Міжнародної організації зі стандартизації (ISO) та Міжнародної електротехнічної комісії (IEC) ще у 2012 році[10]. Відповідно до цього стандарту найбільш

7 Гловюк, І. Закон України «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам» № 2137–IX: аналіз новел кримінального провадження / Ірина Гловюк, Віктор Завтур // Вища школа адвокатури НААУ: <https://www.hsa.org.ua/blog/zakon-ukrayiny-pro-vnesennya-zmin-do-kryminalnogo-protsesualnogo-kodeksu-ukrayiny-ta-zakonu-ukrayiny-pro-elektronni-komunikatsiyi-shhodo-pidvyshhennya-efektyvnosti-dosudovogo-rozsliduvannya-za-garyach/>.

8 Закон України «Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам» від 15.03.2022р. №2137-IX: <https://zakon.rada.gov.ua/laws/show/2137-IX#Text>.

9 Berkeley Protokol on Digital Open Source Investigations: <https://www.ohchr.org/sites/default/files/2022-04/OHCHR_BerkeleyProtocol.pdf>.

10 *Використання електронних (цифрових) доказів у кримінальних провадженнях: метод. реком.* (2020). С. 70.

поширеним способом збирання і зберігання цифрових даних є спосіб архівації. Тобто, якщо якась інформація розміщена на інтернет-ресурсі, то необхідно застосувати будь-яку програму архівації і в такому вигляді можна подавати до суду. Це сприяє збереженню інформації в тому вигляді, у якому вона розміщена у відкритих джерелах[11]. 2) Національний стандарт України «Інформаційні технології. Методи захисту. Вибирання, розгортання та експлуатування систем виявлення та запобігання вторгнень (ДСТУ ISO/IEC 27039:2016 (ISO/IEC 27039:2015, IDT)); 3) Національний стандарт України «Інформаційні технології. Методи захисту. Настанова щодо забезпечення прийнятності та адекватності методів розслідування» (ДСТУ ISO/IEC 27041:2016 (ISO/IEC 27041:2015, IDT)); 4) Національний стандарт України «Інформаційні технології. Методи захисту. Настанови щодо аналізу та інтерпретації цифрового доказу» (ДСТУ ISO/IEC 27042:2016 (ISO/IEC 27042:2015, IDT))[12].

Важливою новелою у Кримінальному процесуальному кодексі України є те, що під час дії надзвичайного або воєнного стану надання дозволу на тимчасовий доступ до речей та документів, що містять окремі види охоронюваної законом таємниці, передається від слідчого судді прокурору та здійснюється на підставі постанови прокурора, погодженої з керівником прокуратури. Однак, це стосується лише щодо таких речей і документів, які містять: 1) відомості, які можуть становити лікарську таємницю; 2) відомості, які можуть становити банківську таємницю; 3) інформацію, яка знаходиться в операторів та провайдерів телекомунікацій, про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання тощо; 4) персональні дані особи, що знаходяться у її особистому володінні або в базі персональних даних, яка знаходиться у володільця персональних даних. Також цікавим є те, що під час дії воєнного стану не потребує дозволу слідчого судді установлення місцезнаходження радіообладнання (радіоелектронного засобу) за заявою його власника. Проте тут постає проблема з підтвердженням права власності на цей радіоелектронний засіб та ідентифікацію особи цього власника, адже в Україні відсутня обов'язкова ідентифікація власників номерів телефонів та відповідної реєстрації особи, яка придбала такий носій.

З урахуванням невпинного процесу євроінтеграції України, важливим є досвід країн Європейського Союзу. Так, Рада Європи надала «Керівні принципи щодо електронних доказів» з детальною інформацією про одержання і обробку електронних доказів. Вони охоплюють основні принципи, яких слід дотримуватись під час збирання і обробки електронних доказів. Серед цих принципів можна виділити такі: цілісність даних, контрольний журнал, спеціалізована підтримка, відповідна підготовка, законність[13]. З урахуванням цих настанов та вищевикладеного дослідження, пропонується виділити такі вимоги щодо цифрових (електронних) доказів.

По-перше, дані, які містяться на цьому електронному доказі, повинні мати безпосереднє відношення до обставин відповідного кримінального провадження, що розслідується.

По-друге, цифрові дані повинні бути релевантними (надійними) та автентичними, має бути проведена процедура верифікації даних. Метадані є важливим інструментом перевірки достовірності цифрової інформації. У сфері прав людини загальновживаним і рекомендованим є використання «Стандарту Дубліського ядра метаданих». Відповідно до цього набору з п'ятнадцяти «ядрових» елементів (для опису ресурсів розробники або одержувачі цифрової інформації повинні записувати такі дані про цифрову інформацію: 1) автор – особа, відповідальна за внесок до ресурсу; 2) охоплення – просторові чи часові характеристики інтелектуального змісту ресурсу, просторова застосовність ресурсу або юрисдикція, до якої належить ресурс; 3) створювач – особа, відповідальна за створення інтелектуального змісту ресурсу; 4) дата – відправна точка або період, пов'язаний із подією в життєвому циклі ресурсу; 5) опис – текстовий опис змісту ресурсу; 6) формат – формат файлу, фізичного носія або розміри ресурсу; 7) ідентифікатор – однозначне посилання на ресурс у певному контексті; 8) мова – мова інтелектуального контексту цифрового ресурсу; 9) видавець – особа, відповідальна за публікацію ресурсу; 10) стосунок – пов'язаний ресурс; 11) авторські права – інформація про авторські права на ресурс і об'єкти, пов'язані з ним; 12) джерело – інформація про відповідний ресурс, з якого «витягнено» поточний цифровий ресурс; 13) предмет – тема ресурсу; 14) назва – ім'я ресурсу; 15) тип – категорія чи жанр ресурсу[14].

В якості цифрового інструменту автоматичної фіксації метаданих можуть використовуватися різноманітні програми. Наприклад, може застосовуватися додаток для камери «eyeWitness to Atrocities», який дозволяє користувачам знімати фотографії та відео з вбудованими метаданими, які не можна змінювати. Ці метадані перевіряють, де і коли було знято відеоматеріал і чи було зображення змінено чи жодних змін не було. Як зображення, так і ме-

11 Яновська, О. (2022). *Процедура збору та фіксації е-доказів обов'язково має включати фахівців комп'ютерних технологій*: <https://advokatpost.com/protsedura-zboru-ta-fiksatsii-e-dokaziv-obov-iazkovo-maie-vkliuchaty-fakhivtsiv-komp-iuternykh-tekhnolohij-suddia-ianovska/>.

12 Наказ ДП «Український Науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 07.10.2016р. №307 «Про прийняття національних стандартів України, змін та поправок до національних стандартів України, гармонізованих з міжнародними нормативними документами»: <https://zakon.rada.gov.ua/rada/show/v0307774-16>.

13 Стефанів, Н. (2022). *Судова практика ККС Верховного Суду України щодо допустимості електронних доказів*: <https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/Prezentatsiia_Stefaniv.pdf>.

14 Принципи документування порушень прав людини: нотатки доповідача: <https://static1.squarespace.com/static/5900b58e1b631bffa367167e/t/617267b806a7863ad1316392/1634887608620/Digital+Information+-+Documentation+-+Speaker+Notes%28uk%29.pdf/>.

тадані зберігаються у безпечній галереї в програмі, де їх не можна редагувати. Потім користувач надсилає їх до бази даних, яка контролюється eyeWitness і розміщена в LexisNexis. LexisNexis Legal & Professional, у складі RELX Group, містить безпечне сховище, базу даних і систему резервного копіювання для зберігання та аналізу цих даних. Протоколи передачі та захищена серверна система, налаштована eyeWitness, створюють ланцюг зберігання, який дозволяє надавати цю інформацію в суді[15]. Важливим є приділення уваги формату зберіганню зібраної інформації, яка у подальшому може набути доказового статусу, оскільки російські службовці та найманці на всіх блокпостах, особливо у так званих «фільтраційних таборах» дуже ретельно перевіряють зміст медіа-файлів, список контактів, переписки та вимагають все видалити або фізично знищують телефон. При цьому, про такі випадки відомо не лише на окупованих територіях України, але й на території держави-агресора, через яку проїжджають примусово депортовані українці, намагаючись дістатися країн Європейського Союзу. Якщо телефон повністю очищений від медіа-файлів та іншої інформації, це викликає великі підозри та може призвести до затримання особи цими військовослужбовцями. Також може бути застосований додаток KoBo Toolbox. Це безкоштовний інструмент із відкритим вихідним кодом для збору інформації у польових умовах за допомогою мобільних пристроїв, планшетів, комп'ютерів тощо.

По-третє, електронний доказ повинен мати матеріально-фіксоване вираження, тобто бути зафіксованими на певному технічному носієві (комп'ютері, флешці, жорсткому диску, телефоні тощо), який може бути долучений до матеріалів провадження з подальшим відтворенням у відповідному процесі. Це є важливим для визначення джерела походження та встановлення процесу відеозйомки. Так, в одній справі захисник стверджував, що під час досудового розслідування не встановлено джерело походження відеозаписів, на яких зафіксовано підпали автомобіля і будинку, не перевірено їх на можливість фальсифікації, а тому, на його думку, вказані докази суд мав визнати недопустимими. Суд встановив, що наявні у справі CD-диски з відеозаписами підпалів автомобіля та будинку з камер відеоспостереження були добровільно надані потерпілим слідчому (справа № 677/2040/16-к, провадження №51-5738км19). Отже, завжди існує проблема джерела походження та отримання цих доказів, у зв'язку з чим постає питання визначення статусу: копія та оригінал. Наприклад, в одному кримінальному провадженні захисник скаржився на те, що до матеріалів кримінального провадження долучено не оригінальні записи вказаних слідчих (розшукових) дій, а їх копії на дисках, що, на думку сторони захисту, зумовлює їх недопустимість. На що суд вказав, що оскільки сторона захисту не оспорює достовірності відображення слідчих (розшукових) дій на вказаних записах, тому сам факт долучення до матеріалів провадження копії цих записів, зафіксованих на оптичних дисках, не суперечить вимогам кримінального процесуального закону[16].

Відповідно до статті 7 Закону України від 22 травня 2003 року №851-IV «Про електронні документи та електронний документообіг» у випадку зберігання інформації на кількох електронних носіях кожний з електронних примірників вважається оригіналом електронного документа. Однак, відповідно до практики Верховного Суду України, матеріальний носій - це лише спосіб збереження інформації, який має значення тільки тоді, коли електронний документ виступає речовим доказом. У провадженні №51-3124км20 суд зазначив, що головною особливістю електронного документа є відсутність жорсткої прив'язки до конкретного матеріального носія. Один і той же електронний документ (відеозапис) може існувати на різних носіях. Усі ідентичні за своїм змістом примірники електронного документа можуть розглядатися як оригінали та відрізнятися один від одного тільки часом та датою створення.

Слід погодитися з цією точкою зору, але необхідно зазначити, що для проведення відповідної судової експертизи має бути оригінал самого запису та сам технічний носій, за допомогою якого його було створено, адже за копією встановити технологічні властивості відеограми за відсутності оригіналу та оригінального пристрою неможливо. Отже, у матеріалах кримінального провадження мають бути відповідні процесуальні документи, на підтвердження існування та дослідження у встановленому законом порядку оригіналу цього запису і самого технічного пристрою.

Цифрові докази вимагають новітніх підходів до їх збирання, зберігання, використання та дослідження під час доказування у кримінальному провадженні. У роботі з цифровими доказами необхідно дотримуватись таких принципів: наявність фахової підготовки, експертна підтримка і розумна обережність. Цифрові докази потребують верифікації (перевірки) й аутентифікації (процедури перевірки справжності). Зокрема, порівняно із традиційними доказами, цифрові докази створюють унікальні складнощі під час аутентифікації через обсяг доступних даних, їх швидкості, нестійкості та вразливості[17].

Під час дослідження цифрових зображень необхідно враховувати вплив технології на відтворення ознак зовнішності. Найчастіше експертові надходить диск або карта пам'яті із записом в електронній формі. Сучасні програмні засоби дають змогу здійснювати певні маніпуляції із зображеннями, а саме: покращувати умови зіставлення зображень, змінювати контраст і масштаб, повертати на необхідний кут, працювати із фрагмента-

15 Перевірка фактів: хто ми: <https://www.eyewitness.global/documents/who-we-are-UA.pdf>.

16 Стефанів, Н. (2022).*Судова практика ККС Верховного Суду України щодо допустимості електронних доказів*: <https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/Prezentatsiia_Stefaniv.pdf>.

17 Шепітько, В., Шепітько, М. (2021). Доктрина криміналістики та судової експертизи: формування, сучасний стан і розвиток в Україні. *Право України.* 8, С. 20.

ми зображення, відбирати кадри відеозапису, на яких найбільш інформативно відображено певні ознаки особи. Також використовувати прийом накладення зображень одне на одне, що дасть змогу якнайповніше зіставити зображення[18].

Отже, через постійну діджиталізацію світу та невпинний розвиток інформаційних технологій збільшується роль цифрової криміналістики як сучасного інструмента розслідування кримінальних правопорушень. Епідемія Covid-19, кіберзагрози та збройна агресія лише загострили необхідність інтенсивного розвитку цифрової криміналістики та необхідність синергії зусиль міжнародного альянсу. Традиційні криміналістичні науково-технічні засоби мають бути оновлені та модернізовані відповідно до технологічних потреб сучасності, але з урахуванням вимог чинного кримінально-процесуального законодавства та міжнародної практики, яка уособлює досвід збирання та аналізу доказів під час військових та збройних конфліктів у різних країнах. Особливо це стосується інформації, яку збирають та отримують з відкритих джерел, соціальних мереж та платформ. Такі цифрові дані повинні бути релевантними та автентичними, для чого необхідно дотримуватися ряду вимог, які описані вище.

DIGITAL FORENSICS DURING THE WAR IN UKRAINE: POSSIBILITIES OF USING SPECIAL KNOWLEDGE IN THE FIELD OF INFORMATION TECHNOLOGIES

Kateryna Latysh

Summary

War has long gone beyond classical understanding and includes itself and cyberwar. After all, the failure of critically important facilities infrastructure is possible not only through physical destruction with the help of various types of weapons, but also by destroying information systems that manage such facilities. That is why a decision was made in Ukraine creation of cyber troops and the National Coordination Center with cyber security. Such units are already operating in Germany, Poland, Estonia, Israel.

In addition, a significant amount of information is available on the Internet, which can potentially, under certain conditions, be used as evidence committing war crimes. However, not enough researched and the rules for collecting such evidence are normatively fixed. In this sense it is the so-called Berkeley Protocol developed by the law school is known of the University of California in Berkeley together with representatives of the United Nations. Protocol Berkeley contains basic provisions on international standards of remote investigation, forensic means of collection, analysis and storage electronic traces and digital information in compliance with professional, legal and ethical principles.

At the same time, it is very important to have synergy between the Ukrainian and European experience in matters of criminal investigation offenses during military operations on the territory of Ukraine. Especially in the context of the expansion of the jurisdiction of the International Criminal Court, of the European Court of Human Rights and other international institutions criminal offenses committed on the territory of Ukraine during war.

Keywords: Cyberwar, special knowledge in the IT-sphere, Digital Forensics, Investigation of war crimes, Digital Evidence.

SKAITMENINĖ KRIMINALISTIKA UKRAINOS KARO METU: SPECIALIŲJŲ ŽINIŲ PANAUDOJIMO GALIMYBĖS INFORMACINIŲ TECHNOLOGIJŲ SRITYJE

Kateryna Latyš

Santrauka

Karas jau seniai peržengė klasikinį supratimą ir apima vykstantį kibernetinį karą. Juk itin svarbių objektų infrastruktūros naikinimas galimas ne tik fiziškai naikinant įvairių rūšių ginklus, bet ir sunaikinant tokius objektus valdančias informacines sistemas. Būtent todėl Ukrainoje buvo priimtas sprendimas sukurti kibernetines pajėgas ir Nacionalinį kibernetinio saugumo koordinavimo centrą. Tokie padaliniai jau veikia Vokietijoje, Lenkijoje, Estijoje, Izraelyje.

Be to, internete yra daug informacijos, kuri tam tikromis sąlygomis gali būti panaudota kaip karo nusikaltimų įrodymas. Tačiau nepakankamai aiškios tokių įrodymų rinkimo taisyklės, nėra aprašytos norminiuose dokumentuose. Šioje situacijoje turime taip vadinamą Berklio protokolą, kurį sukūrė Kalifornijos universiteto Berklyje teisės mokykla kartu

18 Чашницька, Т. Г. (2021). Сучасні тенденції ідентифікації особи за матеріалами відеозапису. *Актуальні питання судової експертизи і криміналістики*: зб. Матеріалів міжнар. наук.-практ. конф. полілогу (м. Харків, 15-16 квіт. 2021р.). С. 276.

su Jungtinių Tautų atstovais. Protokole pateikiamos pagrindinės nuostatos dėl tarptautinių nuotolinio tyrimo standartų, kriminalistinių elektroninių pėdsakų ir skaitmeninės informacijos rinkimo, analizės ir saugojimo priemonių, laikantis profesinių, teisinių ir etinių principų.

Straipsnyje kalbama apie tai, kad itin svarbu vertinti ir pažinti Ukrainos ir Europos besiklostančią kriminalinių nusikaltimų tyrimo praktiką karinių operacijų Ukrainos teritorijoje metu. Ypač plečiant Tarptautinio baudžiamojo teismo, Europos žmogaus teisių teismo ir kitų tarptautinių institucijų jurisdikciją karo metu Ukrainos teritorijoje padarytų nusikalstamų veikų kontekste.

Raktiniai žodžiai: kibernetinis karas, specialios žinios informacinių technologijų srityje, skaitmeninė kriminalistika, karo nusikaltimų tyrimas, skaitmeniniai įrodymai.