УКРАЇНСЬКИЙ НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ СПЕЦІАЛЬНОЇ ТЕХНІКИ ТА СУДОВИХ ЕКСПЕРТИЗ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

ДЕРЖАВНА БЕЗПЕКА УКРАЇНИ В УМОВАХ РОСІЙСЬКОЇ АГРЕСІЇ: АКТУАЛЬНІ ПИТАННЯ ЕКСПЕРТНО-КРИМІНАЛІСТИЧНОГО ТА НАУКОВО-ТЕХНІЧНОГО ЗАБЕЗПЕЧЕННЯ

Збірник матеріалів Всеукраїнської науково-практичної конференції
Том 2

22 серпня 2023 року

м. Київ

УДК 351.746.1:351.86](477-651.2:470-651.1)(06)
Д36

Рекомендовано до друку Науково-технічною радою ІСТЕ СБУ
(протокол № 8 від 27 вересня 2023 року)

Д36 Державна безпека України в умовах російської агресії: актуальні питання експертно-криміналістичного та науково-технічного забезпечення: збірник матеріалів Всеукраїнської науково-практичної конференції, 22 серпня 2023 р.: Том 2. — Київ : ІСТЕ СБУ, 2023. — 212 с.

ISBN 978-617-8013-58-5

Збірник сформований за матеріалами доповідей та презентацій учасників Всеукраїнської науково-практичної конференції «Державна безпека України в умовах російської агресії: актуальні питання експертно-криміналістичного та науково-технічного забезпечення».

В тезах доповідей автори розглянули проблемні питання та перспективи розвитку експертно-криміналістичного забезпечення державної безпеки України; новітні розробки криміналістичних методик та напрями використання спеціальних знань у кримінальному судочинстві; актуальні аспекти забезпечення розроблення, виготовлення та модернізації спеціальних технічних засобів і спеціальної техніки в умовах протистояння російській агресії.

Розраховано на представників суб'єктів сектору безпеки й оборони, а також співробітників судових, правоохоронних органів і спеціальних служб, установ судової експертизи, науковців, викладачів, аспірантів, ад'юнктів та докторантів закладів вищої освіти.

ISBN 978-617-8013-58-5

УДК 351.746.1:351.86](477-651.2:470-651.1)(06)

ПИРІГ Ігор Володимирович
ЕКСПЕРТНЕ ЗАБЕЗПЕЧЕННЯ ДОСУДОВОГО РОЗСЛІДУВАННЯ В СИСТЕМІ ДЕРЖАВНОЇ БЕЗПЕКИ УКРАЇНИ В УМОВАХ РОСІЙСЬКОЇ АГРЕСІЇ 95

ПОЛІЩУК Сергій Миколайович
ДЕЯКІ АСПЕКТИ ТЕХНОЛОГІЇ КАМУФЛЯЖУ ПРИ СТВОРЕННІ СПЕЦІАЛЬНИХ ТЕХНІЧНИХ ЗАСОБІВ 100

ПОЛОВКО Альона Євгеніївна
ВИКОРИСТАННЯ СУДОВО-ЕКОНОМІЧНОЇ ЕКСПЕРТИЗИ В СПРАВАХ ПРО КОРУПЦІЮ: ВИКЛИКИ ТА ПЕРСПЕКТИВИ 105

ПОЛТАВСЬКИЙ Андрій Олександрович
ШЛЯХИ УНІФІКУВАННЯ СУДОВО-ЕКСПЕРТНОЇ ДІЯЛЬНОСТІ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ В КРАЇНАХ ІЗ РІЗНИМИ ПРАВОВИМИ СИСТЕМАМИ 108

ПРИМІРЕНКО Володимир Миколайович,
ДЕМ'ЯНЮК Андрій Володимирович
ПРОГРАМНИЙ ЗАСІБ ОПТИМАЛЬНОГО РОЗПОДІЛУ РЕСУРСУ ЦІЛЕСПРЯМОВАНОГО ПРОЦЕСУ 117

РЕЙТЕР Оксана Костянтинівна
МІЖНАРОДНО-ПРАВОВІ МЕХАНІЗМИ ПРИТЯГНЕННЯ АГРЕСОРА ДО ВІДПОВІДАЛЬНОСТІ 120

САВІНОВА Наталія Андріївна
ФОРМУВАННЯ КУЛЬТУРИ ЕЛЕКТРОННИХ ДОКАЗІВ В УМОВАХ ВІЙНИ 125

САНАКОЄВ Дмитро Борисович
ОКРЕМІ ПИТАННЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ РОЗСЛІДУВАННЯ ВОЄННИХ ЗЛОЧИНІВ В УМОВАХ РОСІЙСЬКОЇ ЗБРОЙНОЇ АГРЕСІЇ 130

ТВЕРДОХЛІБОВ Володимир Віталійович,
КОВБАСЮК Олександр Васильович
ПРОБЛЕМИ СТВОРЕННЯ СУЧАСНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ СЕКТОРУ ОБОРОНИ КРАЇНИ 134

САВІНОВА Наталія Андріївна,
доктор юридичних наук, старший науковий співробітник,
директор навчально-наукового інституту
морського права та менеджменту
Національного університету «Одеська морська академія»;
головний науковий співробітник наукового сектору
прав і безпеки людини в інформаційній сфері
наукового відділу інформаційного суспільства і права
ДНУ «Інститут інформації безпеки і права
Національної академії правових наук України»

ФОРМУВАННЯ КУЛЬТУРИ ЕЛЕКТРОННИХ ДОКАЗІВ В УМОВАХ ВІЙНИ

«Повзуча» війна росії проти України з 2014 року і відкрите вторгнення 24 лютого 2022 року обумовили необхідність переосмислення всієї системи збирання та оцінювання релевантності доказів правопорушень, вчинених поза межами доступу органів дізнання та слідства.

Питання, здавалось би, майже не вирішуване. Хіба що за рахунок свідчень та окремих слідів, які вдається видобути після звільнення. Але в умовах інформаційного суспільства у правоохоронної системи виникає новий блок можливостей – розслідування на основі електронних доказів.

Сутність електронних доказів, з точки зору їх правового значення, де-факто не відрізняється від звичайних доказів: і ті, і інші демонструють певні ознаки, якості та інші особливості, котрі характеризують фактичні обставини вчинення правопорушення.

Більш того, світовий досвід видобування, фіксації та оцінювання доказів злочинів на окупованих територіях чи територіях супротивника існує, і факти збирання доказів, зокрема, за рахунок показань свідків, опитаних значно пізніше вчинених злочинів, відомий світу ще з часів Нюрнберзького трибуналу над фашистським ватажками, та, навіть, і раніше.

Отже, електронні докази в їх загальному розумінні – «докази, зафіксовані на електронних носіях», за змістом та характером використання майже нічим не відрізняються від інших доказів, і основні питання стосуються:

1) їхнього розуміння, визначення, класифікації;
2) оцінки /перевірки.

Вирізняються вони суто характером відображення та фіксації: «цифрові докази» (електронні докази) – будь-яка доказова інформація, котра зберігається або передається у цифровій формі, котру сторони можуть використовувати в суді» [1].

За визначенням Еогана Кейсі, визнаного експерта з цифрової криміналістики, електронні докази (англ. digital або electronic evidence) – «будь-

яка інформація, котра має доказове значення, зберігається або передається у цифровій формі та може бути використана стороною у судовому процесі» [2].

Цифрові докази мають суттєві переваги в порівнянні з традиційними доказами. Хоча перші мають тенденцію бути більш об'ємними, тим не менше, їх важче знищити, легко модифікувати і дублювати, потенційно вони є більш виразними та доступними.

Водночас, електронні докази частіше за інші докази піддаються сумніву дійсності через легкість можливості їхньої зміни, підробки, хоча у судів і є механізми відхиляти їх як неналежні або фальсифіковані. У більшості юрисдикцій США для арешту та дослідження цифрових пристроїв потрібен ордер. У цифровому розслідуванні це може створити проблеми, коли, наприклад, докази інших злочинів виявляються під час розслідування іншого. Наприклад, під час розслідування онлайн-домагань Кіта Шредера в 1999 році [3] слідчі знайшли на його комп'ютері порнографічні зображення дітей, і необхідно було отримати другий ордер, для підтвердження факту таких зображень, перш ніж докази змогли бути допущені до використання при звинуваченні Шредера.

Але такі обставини не утворюють об'єктивних вад для системного підходу для використання електронних доказів, тим більше, що наразі в доступі розслідування всіх країн світу є зброя Протоколу Берклі [4], котра надає чіткий принцип ведення розслідування з використанням електронних цифрових даних, з перевіркою таких за протоколом конкретних дій щодо електронних доказів.

У той же час, зокрема, у США та країнах Європи поступово формується єдине ставлення до електронних доказів. Стівен Мейсон та Уве Расмуссен [5], провівши опитування серед країн-членів Ради Європи, виділили три типи доказів, які можуть бути використані під час судового розгляду:

1) докази із сайтів з відкритим доступом, наприклад, дописи в блоги або фото, завантажені до соціальних мереж;

2) докази, що мають значення у справі, як-от електронне листування або документи у цифровому форматі, що не є публічно доступними та зберігаються на сервері;

3) обліковий запис (акаунт) користувача та дані про трафік (метадані), аби ідентифікувати особу за допомогою встановлення джерела передачі даних, а не їх змісту.

Виходячи з зазначеного, можна дати відповіді на обидва задекларовані на початку доповіді питання щодо особливостей легітимізації електронних доказів в порівнянні з традиційними:

Щодо розуміння / визначення та класифікації (1). Наявне станом на сьогодні визначення електронних доказів (за Еоганом Кейсі): будь-яка інформація, котра має доказове значення, зберігається або передається у цифровій формі та може бути використана стороною у судовому процесі. Наявна і класифікація електронних доказів (за систематизацією Стівена Мейсона та Уве Расмуссена), наведена кількома абзацами вище.

Щодо оцінки / перевірки (2). Найефективнішим є механізм перевірки доказів за схемою Протокола Берклі.

Важливим для розуміння вітчизняними дізнавачами і слідчими є те, що сьогодні, в умовах війни, коли безпосередній доступ до місця вчинення злочину нерідко буває неможливим, або потрапляння на нього несе характер невиправданого ризику, електронні докази набувають особливої цінності. За цих умов вади вітчизняного законодавства щодо визначення самих доказів, або способів доступу до них та їхньої фіксації не мають ставати перепонами. Збирання доказової бази щодо злочинів окупанта або злочинів, вчинених на окупованих територіях цивільним населенням України необхідне, і здійснюватися такі дії можуть саме через використання електронних доказів.

Якщо виходити з системи класифікації, котра взята мною вище за основу (класифікація С. Мейона та У. Расмуссена, підтверджена опитуванням працівників правоохоронних органів країн ЄС), то, на докази, розміщені в соціальних мережах, має сенс дивитися не лише як на підтвердження фактів, а й як «шлях» до свідків. Свідки можуть переміщатися, але їхня прив'язка до місця вчинення злочинів та можливість свідчення про факти правопорушень, виявлення інших свідків, даватимуть дізнанню та слідству значно більш вагому доказову базу для роботи.

На жаль, вітчизняне законодавство, не в усіх випадках встигає за сучасними світовими трендами, у т.ч. культурою роботи з електронними доказами. Хоча, сьогодні ми вже маємо і вітчизняні приклади належної оцінки вітчизняними судами електронної переписки. Наприклад, позиція Великої Палати Верховного Суду у справі № 916/3027/21 (провадження № 12-8гс23): «Якщо з урахуванням конкретних обставин справи суд дійде висновку про те, що відповідне електронне листування дає змогу встановити його учасників та може підтверджувати ті чи інші доводи сторін, наприклад, щодо наявності між ними відповідних відносин, ведення певних перемовин тощо, суд може прийняти таке листування як доказ і в такому разі надати йому оцінку сукупно з іншими доказами у справі» [6]. Але, все ж таки, поки що – не самостійний доказ, адже «може прийняти /…/ сукупно з іншими доказами».

Уявімо ж собі ситуацію, коли, крім електронних доказів, інших доказів просто нема. Такі ситуації можливі, і, зокрема, в кримінальних провадженнях як національного, так і міжнародного рівня. Чи здатні українські правоохоронці повністю побудувати розслідування на електронних доказах і чи здатні суди повною мірою провести судове дослідження таких?

На думку Н.М. Ахтирської, «електронними доказами» є дані, які підтверджують факти, інформацію або концепцію у формі, придатній для обробки за допомогою комп'ютерних систем, у тому числі програми виконання комп'ютерною системою або інших дій. Джерелами електронних доказів є електронні пристрої: комп'ютери, периферійні пристрої, комп'ютерні мережі, мобільні телефони, цифрові камери та інші портативні пристрої, мережа Інтернет [7, С.125]. А.М. Коваленко [8], О.І. Котляревський та Д.М. Киценко [9] вважають електронні докази – сукупністю інформації, яка зберігається в

електронному вигляді на будь-яких типах електронних носіїв та в електронних засобах.

Вітчизняні фахівці наділяють електронні докази такими ознаками:

– існують у нематеріальному вигляді;

– можуть бути створенні як людиною, так і бути результатом функціонування інформаційної системи;

– не можуть існувати поза межами технічного носія або каналу зв'язку;

– не мають нерозривного зв'язку з матеріальним носієм;

– вільно переміщуються в електронній мережі без технічного носія;

– їх не можна безпосередньо сприймати та досліджувати, тільки за допомогою технічних засобів і програмного забезпечення;

– потребують специфічного порядку збирання, перевірки й оцінки;

– мають здатність до дубляжу, тобто копіювання або переміщення на інший носій без втрати своїх характеристик;

– можливість дистанційного внесення змін до них та їх знищення [10, с.252].

Це важко, навіть, коментувати. Просто приклад.

Однак, серед вітчизняних наукових підходів є і прогресивні. Наприклад, позиція О.В. Сіренка, котра полягає у необхідності визнання на нормативному рівні електронними доказами даних про обставини, що мають значення для кримінального провадження й існують у нематеріальному вигляді в межах технічного носія чи каналу зв'язку та сприйняття і дослідження яких можливе за допомогою технічних засобів і програмного забезпечення [11, с. 211]. Така позиція не дисонує зі світовим баченням електронних доказів і, в цілому, найбільш точна і абстрактна, і тому не «вибиватиме» з числа реальних електронних доказів тих, котрі, в дійсності, є корисними для розслідування.

В цілому, на даному етапі розвитку культури електронних доказів в Україні, і, особливо – в умовах війни, необхідно переосмислити відношення як до цінності доказів, так і до цінності світового досвіду роботи з ними. Вірогідно, що запозичення світової моделі бачення електронних доказів якнайширше, і перевірки їх якнайретельніше, суттєво підвищуватимуть результативність розслідування злочинів, доступ до місця вчинення котрих сьогодні для нас обмежений.

Невідворотність покарання винних у вчиненні злочинів на окупованих територіях має переважати вади вітчизняного законодавства. Крім того, в перспективі, робота з електронними доказами стане рутинною для дізнання, слідства та суду, і результати такої роботи повинні бути перевірені, коректні та прозорі. В цьому і полягає сутність культури електронних доказів, котру, на жаль, у нашій країні зрушила з місця війна, а мав би зрушити здоровий глузд і розуміння невідворотності прогресу, у тому числі і в доказуванні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Casey, Eoghan (2004). Digital Evidence and Computer Crime, Second Edition. Elsevier. ISBN 0-12-163104-4. URL:

https://books.google.com.ua/books?id=Xo8GMt_AbQsC&q=Digital+Evidence+and+Computer+Crime,+Second+Edition&redir_esc=y#v=snippet&q=Digital%20Evidence%20and%20Computer%20Crime%2C%20Second%20Edition&f=false (дата звернення: 22.08.2023).
2. Eoghan Casey (ed.). Handbook of Digital Forensics and Investigation. Academic Press. p. 567. ISBN 978-0-12-374267-4. Retrieved 2 September 2010. URL: https://books.google.com.ua/books?id=xNjsDprqtUYC&redir_esc=y (дата звернення: 22.08.2023).
3. STATE v. SCHROEDER (2000) Court of Appeals of Wisconsin. STATE of Wisconsin, Plaintiff-Respondent, v. Keith SCHROEDER, Defendant-Appellant. Nos. 99-1292-CR, 99-2264-CR. Decided: May 24, 2000 URL: https://www.wicourts.gov/ca/opinions/99/htm/99-2264.html (дата звернення: 22.08.2023).
4. Berkeley Protocolon Digital Open Source Investigations URL: https://www.ohchr.org/sites/default/files/2022-04/OHCHR_BerkeleyProtocol.pdf (дата звернення: 22.08.2023).
5. Stephen Mason and Daniel Seng, editors, Electronic Evidence and Electronic Signatures (5th edition, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2021) URL: https://ials.sas.ac.uk/publications/electronic-evidence-and-electronic-signatures (дата звернення: 22.08.2023).
6. Постанова ВП ВС від 21 червня 2023 року у справі № 916/3027/21 (провадження № 12-8гс23). URL: https://reyestr.court.gov.ua/Review/112088045 (дата звернення: 22.08.2023).
7. Ахтирська Н. М. До питання доказової сили кіберінформації в аспекті міжнародного співробітництва під час кримінального провадження. Науковий вісник Ужгородського національного університету. 2016. Вип. 36(2). С. 123–125.
8. Коваленко А. М. Особливості, тактики огляду електронних документів під час досудового розслідування посягань на життя та здоров'я журналіста. Вісник Національної академії правових наук України. 2017. № 1 (88). С. 182–191.
9. Котляревський О. І., Киценко Д. М. Комп'ютерна інформації як речовий доказ у кримінальній справі. Інформаційні технології та захист інформації : збірник наукових праць. 1998. № 2. С. 70–79.
10. Алєксєєва-Процюк Д. О., Брисковська О. М. Електронні докази в кримінальному судочинстві: поняття, ознаки та проблемні аспекти застосування. Науковий вісник публічного та приватного права. 2018. Випуск 2. С. 247–253.
11. Сіренко О. В. Електронні докази у кримінальному провадженні. Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика). 2019. Вип. 14. С. 208-214. URL: http://nbuv.gov.ua/UJRN/muvnudp_2019_14_24 (дата звернення: 22.08.2023).