DOI https://doi.org/10.30525/978-9934-26-686-7-14

ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ: ВИКОРИСТАННЯ ЕЛЕКТРОННИХ ДОКАЗІВ В ПРОЦЕСІ РОЗСЛІДУВАННЯ

Ряшко О. В.

ВСТУП

Ми живемо у світі, у якому специфіка сучасної злочинної діяльності призводить до необхідності знаходження особливого підходу щодо об'єкта криміналістичного пізнання. Наразі світова спільнота максимально залучена до інформаційного простору та перетворилася в окрему групу – інформаційне суспільство. Позитивні аспекти цього явища усім прекрасно відомі, але небезпечні його тенденції часом складно спрогнозувати. Серед цих тенденцій виділяються наступні: вплив на людську психіку та масштаб маніпуляцій, який постійно прогресує, використання сучасних інформаційних технологій для можливості проникнення я у приватне життя та в діяльність організацій, використання сучасних технологій для тотального контролю над життям людей, як в окремій державі, так і світової спільноти, поглиблення інформаційної війни між державами, що ворогують і як наслідок, неухильне зростання кіберзлочинів.

Якщо брати до уваги значення, то кіберзлочином виявляється будь-яке протиправне діяння, що здійснюється за допомогою електронних операцій, відповідно метою якого є подолання захисту комп'ютерних систем та даних, які ними обробляються. У ширшому сенсі це явище розглядається як будь-яке протиправне діяння, що вчинене за допомогою або з використанням комп'ютерної системи чи мережі, включаючи й такі злочини, як незаконне зберігання, пропозиція або поширення інформації за допомогою комп'ютерної системи чи мережі.

Важливим є факт, що предметами посягання у кіберпросторі першочергово виступають інформаційні продукти та ресурси. Майно, комп'ютери, комп'ютерні мережі, мережі електрозв'язку, документи виявляються другорядними (вторинними) об'єктами злочину.

Саме інформація, зафіксована в електронній формі, яка здатна задовільнити потреби чи інтереси користувачів кіберпростору і є інформаційним продуктом. Як будь яка інша інформація вона може бути вагомою, враховуючи залучення багатьох осіб для роботи над нею або бути необхідною умовою для виконання конкретного завдання. Цей інформаційний продукт повинен мати законного користувача, що абсолютно логічно пов'язане з певними відомостями щодо персональних даних чи авторського права чи банківської таємниці. Саме характер відомостей, зафіксованих у інформаційному продукті зумовлює його важливість, інтерес та цінність, а також сприяє обранню особою певної лінії злочинної поведінки.

За сучасного розвитку науки і техніки та швидкоплинних можливостей технологій, використання електронних доказів набуває важливого значення щодо доказуванні винуватості чи невинуватості підозрюваного (обви-

нуваченого) – яка становить головну дилему усього кримінального процесу. Зрозуміло, що роль цифрових доказів стрімко зростає і сьогодні переписки, записи з камер відеоспостереження та дані з мобільних пристроїв можуть бути використані для підтвердження або спростування версії сторони обвинувачення.

На відміну від скажімо стало традиційних доказів, електронні мають певні особливості. Сфера їх існування – цифрова, саме тому їх збирання, зчитування, аналіз та оцінка потребують відповідних знань та обладнання. Такі докази є дещо «крихкими», оскільки їх легше підробити, змінити, знищити, фальсифікувати. Саме тому їх використання у кримінальному провадженні стають додатковим тягарем для сторони обвинувачення, коли мова йде про їх відповідність умовам достовірності та допустимості.

1. Роль та місце електронних доказів у розслідуванні кіберзлочинів

Щодо правової природи електронних доказів – не дивлячись на недостатню врегульованість законодавством, це самостійний вид доказів. Коли мова заходить про основні проблеми та питання, що виникають у зв'язку з використанням електронних доказів, першочерговим завданням в ході судового розслідування виявляється необхідність доведення автентичності електронного доказу. Відповідно з цього правила витікає наступне та найголовніше – підтвердження допустимості його отримання та законного залучення до сфери кримінального судочинства. Не менш важливим є забезпечення незмінності та достовірності даних в ході їх збирання, зберігання та використання в кримінальному провадженні. Якщо звернути увагу на способи та механізми перевірки достовірності та належності таких доказів, то найпоширенішими виступають метадані – структурована інформація, яка дозволяє відстежити будь-які його зміни.

Особливе місце відводиться криптографічним методам – застосуванню цифрових підписів, хеш-функцій, електронних сертифікатів для забезпечення автентичності даних. На допомогу органам досудового розслідування приходить й цифрова експертиза – яка дозволяє за допомогою комплексу технічних заходів провести аналіз електронних доказів, включаючи відновлення видалених файлів, аналіз мережевого трафіку та ідентифікацію авторства[1]

Необхідно памятати, що залежно від обставин пристрої можуть бути зібрані як в увімкненому, так і у вимкненому стані. Надзвичайно важливо прийняти міри для запобігання знищення, псування або зміни оригінальних даних. Зрозуміло, що в ході транспортування можуть виникати ситуації, що сприятимуть пошкодженню або спотворенню даних, тому з метою недопущення необхідно використовувати захищене пакування.

Окрім цього, слід максимально забезпечити належні умови для зберігання цифрових носіїв (це і контроль вологості, і захист від магнітних полів) та документувати усі дії, пов'язані з обробленням доказів. З моменту збирання та фіксації доказів до їх представлення в суді, необхідно дотримуватися

[1] Аніщенко О. (2021). Збір і перевірка електронних доказів: проблеми та рішення. *Юридична практика*, 45(2). С. 14.

чіткості та послідовності щодо її документування. Документація повинна містити унікальний ідентифікатор доказу, дату та відомості про осіб, які мали до неї доступ. В першу чергу увага звертається на фіксацію даних, які можуть бути втрачені або є найменливішими за своєю природою, як вміст оперативної пам'яті до прикладу[2].

Основними умовами якісного збирання та аналізу цифрових доказів є ретельність процесу, перевірка та контроль доступу, чіткість процедури та правильність виконання кожного етапу з метою забезпечення подальшого успішного розслідування.

Саме дотримання принципів цілісності, автентичності та відтворюваності є основою застосування цифрової криміналістики, що надає можливості створення умов для максимально об'єктивного та неупередженого аналізу та мінімізує ризики спотворення чи втрати інформації. На жаль, кіберзлочинність, як феномен, постійно прогресує, набуває дедалі складніших форм, тому покращення ефективності методології збирання цифрових доказів є важливим кроком до зміцнення та збереження інформаційної безпеки з метою справедливого судового провадження.

На сьогоднішній день, дедалі в ході розслідування кіберзлочинів при проведенні слідчих (розшукових) дій перед слідчим постає питання щодо збирання, фіксації та використання електронної інформації, як джерела доказів у кримінальному провадженні. В своїй статті І. Г. Каланча зауважує, що під час слідчих (розшукових) дій фіксація доказів з електронних носіїв збирання інформації, що міститься на них, може здійснюватися двома способами: або вилученням носія або інформаційної системи, до якого він входить, або копіюванням інформації, що зберігається на відповідному електронному носії. Щодо вилучення, зрозуміло, що це класичний спосіб збирання доказів у формі матеріальних об'єктів, до яких належать електронні носії та інформаційні системи. Не дивлячись на певні плюси та переваги, неможливо оминути і деякі проблеми, на кшталт неефективності дослідження електронних носіїв після вилучення в разі загрози зупинення критично важливих функцій бізнес-процесів або наявності шифрування тощо. Погоджуємося, що в таких випадках альтернативою виступає збирання інформації, яка міститься в електронному носії шляхом виготовлення копії такої інформації[3].

Зараз ми живемо у світі, де практично щодня відбуваються терористичні акти, війни, що не вчухають, а відповідно зростає кількість кіберзлочинів та інших правопорушень, пов'язаних із військовою агресією. Тому саме цифрові (електронні) докази відіграють ключову роль у їх фіксації. Специфічні риси, якими вони володіють, наділяють їх як плюсами, так і мінусами. Навіть в ході безперервних бойових дій такі докази збираються за допомогою квадрокоптерів, які дозволяють побачити не тільки приміром масштаби руйнувань, але й зафіксувати деталі, не помітні з землі, фіксацією на смартфон за допомогою

[2] Івасишин, Т., Пірог, О. (2025). Порядок збирання цифрових доказів. *Криміналістика і судова експертиза.* Вип. 70. С. 376. DOI: 10.33994/ kndise.2025.70.28.

[3] Каланча І. Г. Копія електронної інформації як доказ у кримінальному про вадженні: процесуальний та технічний аспекти. *Юридичний науковий електронний журнал.* 2021. № 8. С. 337.

спеціального додатку, фото- і відеоматеріалами з місць обстрілів або перехопленими електронними комунікаціями окупантів, що є доказами вчинення злочинів проти цивільного населення.

Нематеріальна сутність цифрових даних робить їх надзвичайно крихкими саме в юридичному сенсі. На відміну від фізично існуючих речових доказів, електронна інформація дуже легко піддається різного роду трансформаціям: зміні, знищенню, виправленням, копіюванню, до того ж вкрай складно довести, що ці зміни відбулися внаслідок стороннього втручання[4]

Матеріали, незалежно від того, чи зібрані вони у момент вчинення злочину чи лише зафіксували його наслідки, стають доказами у судовому провадженні при умові підтвердження їх достовірності та допустимості. Коли мова заходить про оцінку таких даних в суді, то будь-які сумніви щодо цілісності, фіксації та зберігання будуть трактуватися на користь обвинуваченого (підсудного). Якщо сторона захисту переконає суд у неналежному зберіганні електронного доказу стороною обвинувачення або наведе доводи щодо сумнівності його автентичності, скоріш за все суд виключить його з процесу доказування, як такий, що не відповідає ознакам допустимості.

Погоджуємося з думкою Ханіна С., що сучасне кримінальне процесуальне законодавство, внаслідок своєї недосконалості фігурально висловлюючись, віддає м'яч на половину поля потенційного маніпулятора, аніж надає ефективні правові інструменти органам досудового розслідування, прокуратури та суду. Автором також дуже вдало підмічено, що цифрові докази, модифіковані через дії контрфорензіки, ускладнюють і сам об'єкт експертизи, оскільки експерт змушений не тільки аналізувати зміст даних, а ще й додатково брати на себе місію дослідника, спочатку відновлюючи та перевіряючи сам доказ, а вже потім роблячи висновки щодо його значення для кримінального провадження. Це досить виснажливо та вимагає від експерта не просто високої кваліфікації, доступу до сучасних інструментів, додаткового часу, але й нерідко і творчого підходу[5].

Кіберзлочинність постійно модернізується, практично щодня кіберзлочинці винаходять нові шахрайські схеми та вдосконалюють свої методи заради власного збагачення за рахунок інших громадян та підприємств по всьому світу з використанням мережі Інтернет. На сьогоднішній день ми не знайдемо конкретного переліку кіберзлочинів, окрім цього правове поле не послуговується і специфічними термінами, на кшталт смішингу, доксингу, фішингу, вішингу. Таке використання могло би допомогти в аналізі та синтезі інформації щодо відповідних тенденцій у кіберпросторі. Загрозливою виглядає тенденція до стрімкого поширення зараження комп'ютерів як окремих користувачів, так і підприємств, установ, організацій за допомогою розсилки електронних листів начебто від імені адміністраторів поштових сервісів, суду, банківських установ чи урядових інституцій.

[4] Метелев О.П. Цифрові докази у кримінальному процесі: видова характеристика. *Вісник кримінального судочинства.* № 1-2. 2023. С. 42 URL: https://vkslaw.com.ua/index.php/journal/ article/view/34.

[5] Ханін С. Електронно-цифрові докази під час виконання вимог ст. 290 КПК України. *Юридична газета.* 26 червня 2024. URL: https://yur-gazeta.com/dumka-eksperta/elektronnocifrovi dokazi-pid-chas-vikonannya-vimog-st-290-kpk-ukrayini.html.

Складність розслідування полягає ще й в тому, що кіберзлочини дуже часто є міжнародними, а тому не підпадають під єдину національну юрисдикцію, окрім цього непоодинокими є випадки, коли наприклад комп'ютери злочинця та його жертви знаходяться на територіях різних держав[6].

Якщо первинна інформація сприймається будь-якою людиною та є доступною для її розуміння, то для повної картини злочину та обставин його вчинення необхідно залучення експертом спеціальних засобів, спеціалізованих програм, які можуть допомогти розкодувати інформацію, яку намагалися приховати та відтворити її у тих версіях, які висунув слідчий в процесі розслідування.

Саме фахівець може відновити резервні копії системи, логфайли, дампи оперативної пам'яті, дампи мережевих трафіків, інші файли або їх частини (у разі пошкодження), як наявні, так і видалені, а також службову інформацію про ці файли. Після чого саме фахівець здатний проаналізувати сукупність знайдених цифрових слідів і вибудовати таймлайн шляхом структуризації інформації відносно діяльності користувача ЕОМ щодо операцій, які здійснювалися з певними файлами і програмами (встановлення, видалення, зміна), про роботу в локальній мережі або мережі Інтернет[7]

За загальноприйнятим правилом, збирання та використання доказів з відкритих джерел має здійснюватися за протоколом Берклі, яким рекомендовано мінімізувати дані щодо збирання лише необхідно пропорційної інформації, фіксувати щонайменше такі дані, як цільова вебадреса; вихідний код; захоплення всієї вебсторінки або зображення повідомлення крауд-месенджера взастосунку; вбудовані мультимедійні файли; вбудовані метадані; контекстуальні дані; хеш значення; дані про процес збирання інформації. Наприклад, у практиці правоохоронних органів Німеччини, Великобританії та США OSINT-фрагменти можуть входити до складу доказової бази за умови дотримання стандартів chain of custody (ланцюга збереження доказів) та цифрової фіксації із обов'язковим зазначенням джерела, дати та умов отримання[8]

У Сполучених Штатах Америки також використання у кримінальному провадженні цифрових доказів врегульовані правилами федерального доказового права, зокрема це положення про автентифікацію. Американський законодавець використовує напрочуд зрозумілий підхід про необхідність переконати суд у тому, що цифровий об'єкт є саме тим, за що він подається, а не зміненим чи підробленим артефактом. Таке переконання досягається через спеціалізовані експертизи, застосування криптографічних механізмів фіксації, надійних протоколів зберігання об'єкта та суворий контроль доступу до нього[9].

---

[6] Pohoretskyi M., Cherniak A., Serhieieva D., Chernysh R., Toporetska Z. Detection and proof of cybercrime. *Amazonia Investigaю*. 2022. Vol. 11, issue 53. P. 268. URL: https://doi.org/10.34069/AI/2022.53.05 (дата звернення: 09.10.2023).

[7] Колеснікова І.А. Цифрові сліди; поняття та їх значення при розслідуванні кримінальних правопорушень. *Юридичний науковий електронний журнал*. № 10. 2023. С. 473.

[8] Ліхтанська А. П., Михайлов В. О. (2024) Використання osint в кримінальному праві україни.» *DICTUM FACTUM* 1 (15). С. 110.

[9] Кутепов І.О. Роль цифрових доказів під час розслідування економічних злочинів. *Юридичний науковий електронний журнал.* № 2/2025. С. 629.

Якщо спробувати узагальнити характерні особливості кіберзлочинів, то виявиться, що для переважної більшості осіб, які їх вчиняють притаманна технократична раціональність мислення, яка базується на вмінні виявлення та використання в своїх цілях недостатню обізнаність та прогалини щодо цифрових систем, здібності оминати механізми контролю та створювати певні алгоритми з метою приховування каналів обігу ресурсів. Як влучно зазначає Кутепов І.О. в своїй статті, саме згадана форма раціональності дозволяє таким правопорушникам діяти в межах ретельно сконструйованого кримінального дизайну[10].

Щодо слідчої практики, то найбільш типовими діями є виявлення та збереження цифрових слідів у вигляді комп'ютерних даних. Вимоги ті самі що й відносно інших цифрових доказів. Але й водночас є певна специфіка, обумовлена бінарною природою (послідовність нулів та одиниць), що робить внесені зміни практично непомітними для людського ока. Саме тому, усі процедури щодо ідентифікації комп'ютерних даних у кримінальному провадженні повинні забезпечувати підтвердження їх цілісності та незмінності з істотно вищим рівнем достовірності, ніж це можливо при використанні традиційних методів виявлення цифрових слідів[11]

Якщо брати до уваги класифікацію кіберзлочинів, то за основними критеріями можемо розподілити їх за наступними групами: 1) крадіжка даних (незаконне отримання особистої, фінансової або іншої конфіденційної інформації); 2) фінансові махінації); 3) хакерські атаки; 4) поширення шкідливого програмного забезпечення; 5) кібертероризм[12].

Розслідування кіберзлочинів вимагає чітке розуміння методології та особливостей процесу збирання та аналізу доказової бази. В першу чергу, мова йде про залучення до досудового розслідування фахівців з кібербезпеки та забезпечення їх технічним обладненням. Цифрові докази визначаються як інформація, що є важливою для встановлення обставин кримінального правопорушення, яка зберігається, отримується або передається електронним пристроєм. Цифрові докази можуть існувати в латентному вигляді, на кшталт відбитків пальців, з легкістю перетинати юрисдикційні кордони, чутливість дозволяє змінювати, пошкоджувати або знищувати їх, не докладаючи зайвих зусиль[13].

Електронні сліди також утворюються внаслідок зовнішнього доступу до комп'ютерних систем з метою знищення або копіювання інформації, модифікації баз даних, блокування роботи системи. Такими слідами є видалення з каталогів

---

[10] Кутепов І.О. Кіберзлочинність у фінансовій сфері: предикатна роль, інструменти легалізації та проблематика доказування. *Юридичний науковий електронний журнал*. № 1/2025. С. 775

[11] Караман К.В. Виявлення цифрових слідів: особливості й алгоритм. *Вісник ХНУВС – Bulletin of KhNUIA.* 2025. № 3 (110). С. 145. DOI: https://doi.org/10.32631/v.2025.3.12

[12] Ларченко М.О. Деякі особливості розслідування кіберзлочинів. *Науковий вісник 3/2024 Львівського державного університету внутрішніх справ.* С. 72.

[13] Дунаєва Т.Є. Цифрові дані як доказ скоєння кіберзлочину в розслідуванні кримінальних правопорушень. *Використання цифрової інформації в розслідуванні кримінальних правопорушень: матеріали міжнар. наук.-практ. круглого столу,* м. Харків, 12 груд. 2022 р. / електрон. наук. вид., редкол.: В. Ю. Шепітько (голова), Г. К. Авдєєва, М. О. Со коленко ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України, Лаб. «Використання сучас. досягнень науки і техніки у боротьбі зі злочинністю». Харків : Право, 2022. С. 104 DOI: https://doi.org/10.31359/978-966-998-460-9.

імен файлів, видалення або додавання окремих записів, фізичне руйнування або розмагнічування носіїв, перейменування каталогів і файлів, зміна розмірів вмісту файлів, зміна атрибутів файлів, поява нових каталогів і файлів, зміна інформації про час останнього доступу до інформації, результати роботи антивірусних і тестових програм тощо. Вони можуть бути виявлені під час експертного дослідження комп'ютерного обладнання, протоколів роботи операційних систем, додатків, антивірусних програм, програмного коду[14].

Нерідко на практиці виникають проблеми саме через нерозуміння між електронним документом та електронним доказом, хоча ці поняття тісно пов'язані, але не є аналогічними. Внаслідок такої неузгодженості на стадії судового провадження трапляються випадки відмови суду приймати до розгляду та дослідження скажімо то саме електронне листування, оскільки, приміром, йому не вистачає обов'язкових реквізитів. Не покращує ситуацію і відсутність чіткої регламентації відповідної процедури перевірки електронного документу перед поданням до суду. Чи то призначення відповідної судової експертизи чи то роздруківка інформації з бази даних? На наш погляд, ефективніше подавати електронні докази в електронній та паперових копіях, тому що такий підхід, однозначно, спрощує процедуру огляду електронних доказів судом.

Погоджуємося з думкою щодо необхідності чіткого визначення електронного доказу в КПК України та, додатково, в підзаконних нормативних актах узгодити порядок роботи з електронними доказами, зокрема окреслити необхідні носії інформації, доказову базу з яких суддя може аналізувати, програмне забезпечення для такого аналізу та обумовлення потреб, за яких виникає така необхідність, інші технічні та технологічні аспекти[15].

Цифрові сліди виникають внаслідок використання цифрових засобів та технологій. Важливим аспектом є те, що використання таких засобів і технологій може бути як безпосереднє, при фізичному, особистому застосуванні (пошук в мережі інтернет певної інформації або завантаження відео- файли в соціальну мережу), так і опосередкованим, коли дані утворюються без фактичного втручання особи (утворення метаданих при здійсненні фотографування певного об'єкту, фіксація камерами відеоспостереження пересування транспортного засобу тощо)[16].

2. Типові слідчі ситуації та характеристика особи кіберзлочинця

Типовими слідчими ситуаціями є ситуації, коли приміром відомості в ЄРДР вносяться в результаті отримання повідомлення особи про кримінальне правопорушення, яке містить інформацію щодо особи можливого злочинця та

[14] Лазебний А. М. Сутність та значення електронних слідів у криміналістиці. *Ірпінський юридичний часопис: науковий журнал.* 2023. Вип. 1 (10) С. 230. DOI 10.33244/2617-4154.1(10).

[15] В.Г. Хахановський. М.В. Гуцалюк. Особливості використання електронних (цифрових) доказів у кримінальних провадженнях. *Криміналістичний вісник.* № 1 (31), 2019. С. 16-17. С. 16-17 doi: 10.37025/1992-4437/2019-31-1-13

[16] Демидова Є.Є. Цифрові сліди кримінального правопорушення: поняття та особливості. *Науковий вісник Ужгородського Національного Університету,* 2024. С. 73. DOI https://doi.org/10.24144/2307-3322.2024.85.4.10

персоналізацію його даних. Таку особу можливо виявити за результатами внутрішньої перевірки під час моніторингу кіберпростору або в ході проведення аудиту.

Процес досудового розслідування буде ефективним у випадку максимального збереження документів, в яких зафіксована робота комп'ютерної мережі, встановлення усіх співучасників злочину та визначення ролі кожного з метою подальшої можливості забезпечення відшкодування цивільного позову. Перед слідчим постають такі типові тактичні завдання, як персоналізація особи злочинця, встановлення його місцеперебування та затримання, встановлення потерпілих осіб, забезпечення збереження віддалених електронних носіїв інформації, у яких зафіксовано роботу злочинця в мережі, накладення арешту на майно з метою відшкодування матеріальних збитків та можливої його конфіскації.

Інша слідча ситуація виникає, коли кримінальне провадження розпочинається на підставі отримання оперативної інформації та місить відомості, що персоналізують особу злочинця (злочинців). Як правило, таке розслідування стосується вчинення тяжких міжнародних кіберзлочинів, що включають розповсюдження дитячої порнографії або насильство, експлуатація та торгівля людьми.

В ході такого розслідування необхідно провести комплекс слідчих (розшукових) дій та негласних слідчих (розшукових) дій, надання доручення оперативному підрозділу на проведення оперативних заходів, спрямованих зокрема для зняття інформації з електронних комунікаційних мереж, з електронних інформаційних систем; особистий огляд затриманих; слідчий огляд вилученого майна; проведення обшуків за місцем проживання, перебування або роботи затриманих осіб.

Кримінальне провадження може бути розпочато в результаті перевірки оперативної інформації, але, на відміну від попередньої сприятливої слідчої ситуації, без жодних відомостей про особу злочинця. Така ситуація є характерною, коли мова йде про незаконну діяльність організованої злочинної групи, що пов'язана із заволодінням майном шляхом незаконних операцій з використанням електронно-обчислювальної техніки. В такому випадку на початок досудового розслідування слідчий володіє інформацією про потерпілих, йому відомий спосіб та механізм вчинення злочину, але практично нічого не відомо про безпосередніх замовників, виконавців чи спонсорів злочинних діянь.

Як правило, це багатоепізодні кримінальні провадження, нерідко виникають підстави для їх об'єднання в одне, тому основним завданням виступає скрупульозне документування усіх епізодів, встановлення суб'єктного складу щодо кожного з епізодів злочинної діяльності, визначення ролі кожного з учасників та встановлення механізмів легалізації незаконно отриманих доходів. З усіх слідчих ситуацій ця виглядає найскладнішою, оскільки, саме при її відпрацюванні слідчий змушений максимально реалізовувати весь арсенал тактичних операцій, в першу чергу спрямованих на подолання засобів конспірації, які використовують учасники мережевої злочинної групи.

Звернемо свою увагу на встановлення мотивів вчинення кіберзлочинів. Перше місце належить мотивації корисливій, оскільки дійсно чорний ринок даних, які викрадаються та простота їх монетизації сприяють постійній активізації цього мотиву, який надає можливість для швидкого фінансового збагачення. Політичні та інші ідеологічні мотиви народили так званий хактивізм – використання комп'ютерів, комп'ютерних мереж для просування політичних ідей, в тому числі й втручання у виборчі процеси країн через використання технологій фреймингу, сугестії, чорного піару. Метою хактивістів є приміром зрив діяльності організації, з якими вони перебувають в опозиції або навпаки, просування своїх власних політичних ідей шляхом злому.

Мотиві ігрові, які притаманні особам, що розглядають злом як виклик особистий, чи інтелектуальний, чи технічний. Такі особи намагаються доводити свою значимість, підвищувати авторитет у своєму колі спілкування або ж роблять це заради розваги, оскільки знаходяться в пошуку задоволення гострих відчуттів. Злочинець, що вчиняє кіберзлочин, фактично завжди прирівнюється до активного користувача комп'ютера. Фаховий рівень варіюється від користувача, упевненого користувача, досвідченого користувача до профі. Критеріями такої диференціації, в першу чергу, слугують кількість програм, які опанував користувач; ступінь опанування ним кожної з програм; рівень професійної самооцінки та бажання постійного самовдосконалення.

Абсолютно згідні з думкою, що така диференціація цілком підходить теорії, але є дещо формальною на практиці саме з позицій формулювання типових версій про особу злочинця. Наприклад, той самий професійний рівень не в змозі у повній мірі відобразити весь комплекс ознак злочинця, які він задіяє у процесі детермінації механізму злочину. Тут і психологічні особливості, і конкретна роль, якщо мова йде про злочинне угрупування, і його місце-знаходження в сенсі географічному, і соціальна мобільність[17].

Кіберзлочинці поділяються на так званих «одиночок», які працюють самостійно та переслідують матеріальну вигоду чи виявляють особисту зацікавленість до злому технологій; кіберзлочинні угруповання – це організовані групи, які об'єднують свої знання та ресурси для досягнення конкретних злочинних цілей; хакери, діяльність яких спонсоруються державою і які діють за підтримки або з дозволу держави, з метою шпигунства або завдання шкоди іншим країнам; і насамкінець, інсайдери – це працівники компаній або організацій, які можуть зловживати своїм доступом до конфіденційних даних[18].

Саме тому, банківські установи, ІТ-компанії, фірми охорони й технічного обслуговування, добираючи персонал, проводять тестування з метою визначення рівня професіональності, а також психотипу майбутнього

[17] [Кіберзлочинність та електронні докази = Cybercrime and digital evidence : навч. посібник / [Б. М. Головкін, О. І. Денькович, В. В. Луцик, Д. М. Цехан] ; за ред. канд. юрид. наук, доц. Ольги Денькович, д-р права, проф. Габріеле Шмельцер. – Електрон. вид. – Львів : ЛНУ ім. Івана Франка, 2022. С. 100. (Удосконалення магістер. програми з кримін. юстиції = Modernising Master's Training on Criminal Justice. CRIMHUM).

[18] Найченко А.М. Кіберзлочинність та оцінка судом електронних (цифрових) доказів в кримінальному провадженні. *Журнал «Наукові інновації та передові технології.* № 12 (40). 2024. С. 538

працівника. Результати такого роду тестувань можуть бути досить цінними для працівників кіберполіції під час первинної перевірки інформації та слідчого з позицій визначення кола підозрюваних в установі-жертві[19].

ВИСНОВКИ

На сьогоднішній день саме Інтернет відкриває надзвичайно великі можливості для спілкування, обміну інформацією будь-якого характеру та потенційною самореалізацією у багатьох сферах. Відповідно до цих можливостей, ми стали свідками та учасниками виникнення та функціонування абсолютно нового типу суспільних відносин – відносин у кіберпросторі, які вивели світову спільноту на зовсім інший рівень царину державного управління, наукові дослідження, мистецькі здобутки та економічні досягнення. Кожна монета має дві сторони, інша сторона інтернет-середовища лякає та жахає масштабами криміногенного характеру, від порушення авторських прав до розповсюдження та збуту творів, що пропагують культ насильства та жорстокості, порнографічних предметів, наркотичних засобів, вчинення вимагань та шахрайств.

Проблемним моментом в ході розслідування кіберзлочинів можна назвати відсутність можливості дослідження електронних доказів, які зберігаються на віддалених серверах. Звичайно є можливість дослідження їх паперових аналогів. Маємо надію, що можливість дослідження таких доказів виведе досудове розслідування кіберзлочинів на абсолютно інший, якісно новий рівень.

Іншою проблемою, на наш погляд, виступає відсутність єдиної методики трактування одних і тих самих фактів сторонами кримінального провадження. Ми пов'язуємо це з використанням різних методів і процедур розслідування кіберзлочинів різними спеціалістами та експертними установами. Доцільно би було запровадити єдиний стандарт щодо методики, аналізу та синтезу інформації, принципів безпосереднього дослідження та оцінки в ході розслідування кіберзлочинів з метою недопущення помилкових висновків та неефективного використання ресурсів. Саме оцінка доказової інформації виявляє усі недоліки, які мають місце як в процесі збирання, так і в недостатньо якісному аналізу цифрових доказів на стадії досудового розслідування.

Констатуємо факт, що при характеристиці особи комп'ютерного злочинця, необхідно враховувати, що в електронну злочинність втягнуто надзвичайно широке коло осіб, яке варіюється від висококваліфікованих спеціалістів до дилетантів. До того ж правопорушники мають різний соціальний статус та різний рівень освіти. Зловмисники постійно вдосконалюють свої методи в обхід заходів безпеки, що надзвичайно ускладнює роботу органів досудового розслідування. Як правило, особам, що вчиняють кіберзлочини притаманний високий рівень інтелекту, професіоналізм, постійне залучення до новинок у сфері комп'ютерних технологій.

[19] Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі [Текст] : монографія / О. А. Самойленко; за заг. ред. А. Ф. Волобуєва. Одеса :ТЕС, 2020. С. 118

Цілком логічно, що більшість таких осіб знають декілька мов програмування, мають значний досвід роботи на комп'ютері, як правило раніше до кримінальної відповідальності не притягувалися, наділені розвиненим формально-логічним мисленням, використовують специфічну лексику, так званий компютерний сленг. Нерідко суб'єктом злочину є «білокомірцеві злочинці», які вчиняють злочини, пов'язані безпосередньо з їх службовою діяльністю, шляхом використання доступу до певних комп'ютерних інформаційних систем та електронних баз даних[20].

АНОТАЦІЯ

У статті досліджуються особливості збирання, перевірки та оцінки електронних доказів до розслідування кіберзлочинів. Наголошується на загрозі злочинності у кіберпросторі як основному чиннику негативного впливу, пов'язаними з багатьма сферами життя. Виокремлено й проаналізовано чинники, які ускладнюють процес досудового розслідування, зокрема обмежені можливості фіксації обстановки вчинення кіберзлочину та слідової картини. Визначено необхідність в подальшому розвитку забезпечення ефективності сфери кібербезпеки із врахуванням практики європейських партнерів, зокрема адаптації національного законодавства до міжнародних стандартів.

Література

1. Аніщенко О. (2021). Збір і перевірка електронних доказів: проблеми та рішення. *Юридична практика*, 45(2), 12–19.

2. Івасишин, Т., Пірог, О. (2025). Порядок збирання цифрових доказів. *Кримінал істика і судова експертиза.* Вип. 70. С. 371–381. DOI: 10.33994/ kndise. 2025.70.28.

3. Каланча І. Г. Копія електронної інформації як доказ у кримінальному провадженні: процесуальний та технічний аспекти. *Юридичний науковий електронний журнал.* 2021. № 8. С. 336-339. DOI https://doi.org/10.32782/2524-0374/2021-8/77

4. Метелев О.П. Цифрові докази у кримінальному процесі: видова характеристика. *Вісник кримінального судочинства.* № 1-2. 2023. С. 42-53 URL: https://vkslaw.com.ua/index.php/journal/ article/view/34.

5. Ханін С. Електронно-цифрові докази під час виконання вимог ст. 290 КПК України. *Юридична газета.* 26 червня 2024. URL: https://yur-gazeta.com/dumka-eksperta/elektronnocifrovi dokazi-pid-chas-vikonannya-vimog-st-290-kpk-ukrayini.html.

6. Pohoretskyi M., Cherniak A., Serhieieva D., Chernysh R., Toporetska Z. Detection and proof of cybercrime. *Amazonia Investigaю*. 2022. Vol. 11, issue 53. P. 259–269. URL: https://doi.org/10.34069/AI/2022.53.05 (дата звернення: 09.10.2023).

[20] Максимчук Ю. В. Особливості розслідування кіберзлочинів та протидії їх вчинення / Ю. В. Максимчук / Грані права: XXI століття : матеріали Всеукраїнської науково-практичної конференції (м. Одеса, 19 травня 2018 р.) У 2-х т. Т. 2 / за ред. Г. О. Ульянової ; уклад.: Ю. Д. Батан, М. В. Сиротко [та ін.] – Одеса : Видавничий дім «Гельветика», 2018. – С. 379-381.

7. Колеснікова І.А. Цифрові сліди; поняття та їх значення при розслідуванні кримінальних правопорушень. *Юридичний науковий електронний журнал*. №10. 2023. С. 472-474 DOI https://doi.org/10.32782/2524-0374/2023-10/114

8. Ліхтанська А. П., Михайлов В. О. (2024) Використання osint в кримінальному праві україни.» *DICTUM FACTUM* 1 (15). С. 105-111. DOI.ORG/10.32703/2663-6352-2024-1-15-105-111

9. Кутепов І.О. Роль цифрових доказів під час розслідування економічних злочинів. *Юридичний науковий електронний журнал.* № 2/2025. С. 626-630. DOI https://doi.org/10.32782/2524-0374/2025-2/151

10. Кутепов І.О. Кіберзлочинність у фінансовій сфері: предикатна роль, інструменти легалізації та проблематика доказування. *Юридичний науковий електронний журнал*. № 1/2025. С. 774-778. DOI https://doi.org/10.32782/2524-0374/2025-1/184

11. Караман К.В. Виявлення цифрових слідів: особливості й алгоритм. *Вісник ХНУВС – Bulletin of KhNUIA.* 2025. № 3 (110). С. 141-150. С. 145 DOI: https://doi.org/10.32631/v.2025.3.12

12. Ларченко М.О. Деякі особливості розслідування кіберзлочинів. *Науковий вісник 3/2024 Львівського державного університету внутрішніх справ.* С.70-77. DOI: https://doi.org/10.32782/2311-8040/2024-3-9

13. Дунаєва Т.Є. Цифрові дані як доказ скоєння кіберзлочину в розслідуванні кримінальних правопорушень. Використання цифрової інформації в розслідуванні кримінальних правопорушень: матеріали міжнар. наук.-практ. круглого столу, м. Харків, 12 груд. 2022 р. / електрон. наук. вид., редкол.: В. Ю. Шепітько (голова), Г. К. Авдєєва, М. О. Со коленко. ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України, Лаб. «Використання сучас. досягнень науки і техніки у боротьбі зі злочинністю». Харків : Право, 2022. 104 с. DOI: https://doi.org/10.31359/978-966-998-460-9.

14. Лазебний А. М. Сутність та значення електронних слідів у криміналістиці. *Ірпінський юридичний часопис: науковий журнал.* 2023. Вип. 1 (10) С. 226-233. DOI 10.33244/2617-4154.1(10).

15. В.Г. Хахановський. М.В. Гуцалюк. Особливості використання електронних (цифрових) доказів у кримінальних провадженнях. *Криміналістичний вісник.* № 1 (31), 2019. С. 13-19. С. 16-17 DOI: 10.37025/1992-4437/2019-31-1-13

16. Демидова Є.Є. Цифрові сліди кримінального правопорушення: поняття та особливості. *Науковий вісник Ужгородського Національного Університету*, 2024. С. 71-75. DOI https://doi.org/10.24144/2307-3322.2024.85.4.10

17. Кіберзлочинність та електронні докази = Cybercrime and digital evidence : навч. посібник / [Б. М. Головкін, О. І. Денькович, В. В. Луцик, Д. М. Цехан] ; за ред. канд. юрид. наук, доц. Ольги Денькович, д-р права, проф. Габріеле Шмельцер. – Електрон. вид. – Львів : ЛНУ ім. Івана Франка, 2022. 298 с. (Удосконалення магістер. програми з кримін. юстиції = Modernising Master's Training on Criminal Justice. CRIMHUM).

18. Найченко А.М. Кіберзлочинність та оцінка судом електронних (цифрових) доказів в кримінальному провадженні. *Журнал «Наукові інновації та передові технології.* № 12 (40). 2024.535544. DOI https://doi.org/10.52058/2786-5274-2024-12(40)-535-544

19. Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі [Текст] : монографія / О. А. Самойленко; за заг. ред. А. Ф. Волобуєва. Одеса: ТЕС, 2020. 372 с. Режим доступу: https://doi.org/10.32837/11300.13264

20. Максимчук Ю. В. Особливості розслідування кіберзлочинів та протидії їх вчинення / Ю. В. Максимчук / Грані права: XXI століття : матеріали Всеукраїнської науково-практичної конференції (м. Одеса, 19 травня 2018 р.) У 2-х т. Т. 2 / за ред. Г. О. Ульянової ; уклад.: Ю. Д. Батан, М. В. Сиротко [та ін.] – Одеса : Видавничий дім «Гельветика», 2018. С. 379-381. http://hdl.handle.net/11300/10643

Information about the author:
Ryashko Olena Vasylivna,
Candidate of Law, Associate Professor,
Associate Professor of the Department of Criminal Procedure and Criminology,
Lviv State University of Internal Affairs,
Ukraine, Lviv, Candidate of Law,
26, Horodotska St., Lviv, 79007 Ukraine