

АКТУАЛЬНІСТЬ ЦИФРОВОЇ КРИМІНАЛІСТИКИ В УМОВАХ ЦИФРОВІЗАЦІЇ СУЧАСНОГО СУСПІЛЬСТВА

БАРАНЯК Володимир Михайлович - кандидат хімічних наук, доцент
Навчально-науковий інститут права, психології та інноваційної освіти
Національного університету "Львівська політехніка", кафедра кримінального
права і процесу

ORCID ID: <https://orcid.org/0000-0001-6161-7862>

УДК 343.985

DOI 10.32782/LAW.UA.2023.4.17

Обґрунтовується актуальність цифрової криміналістики в умовах цифровізації сучасного суспільства, відзначено активне використання цифрових технологій у вирішенні найрізноманітніших видів протиправної діяльності у сфері комп'ютерної інформації, дано визначення поняття «цифрового сліду» та «цифрової криміналістики».

Наголошено на необхідності вироблення нових знань і напрацювань криміналістичної техніки, стандартів і принципів оцінки та перевірки зібраних доказів (цифрових слідів), проведенні обов'язкової стандартизації під час роботи з цифровою інформацією, розгляді та розробці відповідної методики для підготовки фахівців у сфері цифрової криміналістики.

Акцентовано увагу на етичних, правових та питаннях приватності, пов'язані із збором та використанням цифрових даних під час проведення розслідування, дотриманні конфіденційності та захисту особистої інформації осіб, що не мають відношення до кримінального правопорушення, відповідності збору і використання цифрових даних під час розслідування визначеним правовим нормам і стандартам (отримання судових ордерів для збору доказів, вимоги щодо збереження інформації, дотримання прав і свобод осіб, які перебувають під слідством), забезпеченні належного рівня захисту, збереження та передачі особистої інформації та обмеженні доступу до неї лише на визначених підставах.

Ключові слова: цифровізація, цифрові сліди, цифрова криміналістика, стандартизація, конфіденційність.

Постановка проблеми

Сьогодні розвиток передових цифрових технологій у сучасному суспільстві передбачає їх обов'язкове впровадження в найрізноманітніші напрямки суспільних відносин. Однак разом із розвитком цифрової економіки необхідно відзначити активне використання цифрових технологій у вирішенні найрізноманітніших видів протиправної діяльності з боку злочинців.

Дедалі частіше зустрічаються кримінальні правопорушення, що пов'язані з інформаційно-комунікаційними технологіями або у сфері комп'ютерної інформації. Саме тому за останні роки зросла питома вага кримінальних правопорушень, вчинених з використанням високих інформаційних технологій. Законодавцем передбачено XVI окремих розділ у Кримінальному кодексі України, що підкреслює актуальність та небезпечність кримінальних правопорушень у сфері цифрових технологій [1].

Стан дослідження проблеми

Питання теоретичних і методологічних аспектів цифрової криміналістики і судової експертизи в епоху діджиталізації досліджували такі вітчизняні вчені, як, Бузина С. О., Кравченко Р. В., Петрова І. А., Шепітько В. Ю., Голяш І. Д., Євдокіменко С. В., Рогатюк І. В., Авдєєва Г. К. та інші.

Мета і завдання дослідження полягає в обґрунтуванні актуальності цифрової кримі-

налістики в умовах цифровізації сучасного суспільства.

Виклад основного матеріалу

Правове регулювання цифрової трансформації України перебуває на початковому етапі розвитку. У той же час накопичений досвід, практичні результати цифрової трансформації, а також великий існуючий нормативний масив законодавчих норм у галузі інформаційних технологій дозволяють уже зараз дати оцінку поточному стану та перспективам розвитку права у сфері цифрової трансформації [2].

Електронні засоби платежу все активніше використовуються та забезпечують можливість здійснення фінансових транзакцій. Водночас, електронні грошові кошти є недостатньо захищеними від протиправних посягань з боку злочинців. Найбільш поширеним способом шахрайства є отримання злочинцями пароля електронного гаманця за допомогою несанкціонованого втручання в роботу електронно-обчислювальних машин.

У ситуаціях, коли вчиняють кримінальні правопорушення за допомогою віддаленого доступу, значно знижується доказова база, тобто наявність залишених трасологічних слідів, що відображають прикмети об'єкта, який їх залишив (відбитки пальців рук, сліди зламу, відбитки коліс тощо). Однак під час вчинення шахрайських дій із застосуванням цифрових технологій з'являється новий вид слідів – це цифрові сліди кримінального правопорушення. Під цифровим слідом слід розуміти унікальний набір дій, які були вчинені в інформаційно-телекомунікаційному просторі, а також інформація, що була залишена в результаті перегляду веб-сторінок [3].

Беручи до уваги все вищесказане, можна дійти висновку, що цифрова криміналістика включає виявлення, збір і аналіз електронних слідів з метою боротьби з кіберзлочинністю. Комп'ютер або смартфони можуть бути знаряддям або засобом вчинення протиправної дії, або предметом кримінального посягання, або призначатися для зберігання важливих електронних доказів кримінального правопорушення.

Сучасна криміналістика повинна пристосовуватися, адаптуватися до рівня розвитку сучасних технологій для можливості сприяння здійсненню правоохоронної діяльності. Станом на сьогодні часто став згадуватися термін «Цифрова криміналістика». Це пов'язано з тим, що вчинення кримінальних правопорушень з використанням цифрових пристроїв залишає в них електронні сліди, а по-друге, з тим, що органи досудового розслідування мають техніко-криміналістичні засоби (персональні комп'ютери), які дають змогу виготовляти процесуальні документи в електронній формі на електронних носіях інформації.

Виникнення поняття «цифрова криміналістика» дозволила виокремити самостійні напрямки судової експертизи. Залежно від джерела, для позначення цієї галузі також використовуються інші терміни, такі як «комп'ютерна криміналістика» або «криміналістика комп'ютерних систем». Водночас деякі вчені розглядають комп'ютерну криміналістику як прикладну науку для розслідування злочинів (інцидентів), пов'язаних з комп'ютерною інформацією, експертизи цифрових доказів, а також дослідження, отримання та фіксації цих методів доказів.

Крім того, криміналістика активно розвивається в контексті діджиталізації та розширення знань про діджиталізацію [4]. Цифрові докази вимагають нових способів збирання, зберігання, використання та перевірки доказів у кримінальному провадженні. Під час використання цифрових доказів слід дотримуватися принципів професійної підготовки, експертної допомоги та розумної обережності. Вони повинні бути перевірені та автентифіковані. Цифрові докази, зокрема, створюють унікальні виклики для перевірки автентичності порівняно з традиційними доказами через обсяг, швидкість, мінливість і вразливість наявних даних.

У сучасному світі цифрова криміналістика є новим видом діяльності, спрямованим на роботу з цифровими слідами правопорушень. Вироблення нових стандартів і принципів оцінки та перевірки зібраних доказів (цифрових слідів) потребує нових знань і напрацювань криміналістичної техніки [5].

Авдеева Г. К. зазначає, що цифрові сліди в криміналістиці – це непомітні матеріальні сліди, які містять важливу криміналістичну інформацію, збережену в цифровій формі на різних матеріальних носіях. Ці залишки можуть бути виявлені, зафіксовані та досліджені за допомогою спеціалізованих цифрових пристроїв.

Основними джерелами цифрових слідів є різноманітні матеріальні носії цифрової інформації, такі як комп'ютери, інтегральні мікросхеми, мікроконтролери, обладнання телекомунікаційних мереж, цифрові фотокамери, диктофони, пристрої для зчитування інформації з пластикових банківських карт, мобільні телефони та планшети. Окремі електронні компоненти цих пристроїв можуть навіть зберігати інформацію про місце та час їх використання. Наприклад, за допомогою системи геолокації можна точно визначити місцезнаходження комп'ютера, планшета або мобільного телефону в режимі реального часу, включаючи інформацію про їх власників. Дані геолокації також можуть бути використані для встановлення факту одночасної присутності двох або більше осіб в одному місці, що може свідчити про їх взаємодію [3, с. 91-92].

Основна проблема збору цифрових слідів полягає в тому, що вони можуть миттєво змінюватися, внаслідок чого стають візуально невидимими, а виявити їх і зафіксувати можна лише за допомогою спеціальних методів та спеціального комп'ютерного обладнання. Після проведеного збору комп'ютерної інформації її необхідно зберігати в незмінному вигляді, що є першочерговим завданням криміналістичного дослідження, лише при дотриманні цих правил інформація матиме доказову силу [5].

Під час вчинення кіберзлочинів часто проводяться прямі атаки на комп'ютери та інші подібні пристрої з метою їхнього відключення. Іноді атаковані комп'ютери використовують для поширення шкідливих програм, комп'ютерних вірусів, нелегальної інформації, різного роду зображень, кібербулінгу. У юридичній літературі виділяють такі види кіберзлочинів: корисливі кіберзлочини (включно з фішингом, кібер-вимаганням, фінансовим шахрайством тощо);

крадіжка персональних даних; кібершпигунство; порушення авторських прав та деякі інші.

Розглядаючи їх, слід враховувати, що в сучасних умовах у легальний економічний обіг активно входять «нетрадиційні» види власності, зокрема веб-сайти, криптовалюти, технології мобільного зв'язку, інтернет-власність тощо. Оскільки вони мають здатність генерувати високі доходи, кримінальне середовище реагує на них відповідним чином. Внаслідок чого з'являються нові види кримінальних посягань.

Проблеми та виклики, що виникають у сфері цифрової криміналістики, включають в себе етичні, правові та питання приватності, пов'язані із збором та використанням цифрових даних під час проведення розслідування. Етичні аспекти включають у себе обов'язок дотримуватися конфіденційності та захищати особисту інформацію осіб, які не мають відношення до кримінального правопорушення. Також важливо уникати зловживання цифрових даних для особистих цілей або політичної маніпуляції. Також збір і використання цифрових даних під час розслідування повинні відповідати чітко визначеним правовим нормам і стандартам. Це охоплює такі питання, як отримання судових ордерів для збору доказів, вимоги щодо збереження інформації, а також дотримання прав і свобод осіб, які перебувають під слідством. Недодержання правових норм може призвести до незаконного збору даних та порушення прав громадян. Збір і аналіз цифрових даних може порушити приватність та конфіденційність осіб, чії дані збираються. Важливо забезпечувати належний рівень захисту особистої інформації та обмежувати доступ до неї лише на визначених підставах. Це стосується також збереження та передачі цих даних, щоб забезпечити їхню безпеку.

Висновки

Отже, питання цифрової криміналістики в умовах цифровізації сучасного суспільства є актуальним. Сучасна криміналістика повинна пристосовуватися та адаптуватися до рівня розвитку сучасних технологій для можливості їх використання з метою здій-

снення правоохоронної діяльності. Вироблення нових стандартів і принципів оцінки та перевірки зібраних доказів (цифрових слідів) потребує нових знань і напрацювань криміналістичної техніки. У зв'язку з цим необхідно провести обов'язкову стандартизацію під час роботи з цифровою інформацією, а також розглянути та розробити відповідну методику для підготовки фахівців у сфері цифрової криміналістики.

Література

1. Кримінальний кодекс України: Закон України від 05.04. 2001 р. № 2341-III / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/2341-14#n2491>.
2. Полякова Т. А., Бойченко І. С., Троян Н. А. Інформаційно-правові механізми електронної взаємодії у сфері правової інформації в умовах цифровізації. Моніторинг правозастосування. № 1 (38). 2021. С. 24-27.
3. Авдеева Г. К. Сутність цифрових слідів у криміналістиці. Актуальні питання судової експертизи та криміналістики: Зб. матеріалів міжнар. науково-практ. конф., присвяч. 95-річчю створення Харків, м. Харків, 10–11 жовт. 2018 р. Харків, 2018. С. 90–93.
4. Діджиталізація кримінального процесу: в Україні планують перевести провадження в електронний формат. URL: <https://uazmi.org/news/post/bReTCc20Q04a1jCN6zj9y2>.
5. Коваль С. М. Стратегії розвитку безпеки цифрових комунікацій служби криміналістики. Юридичний науковий журнал, 2020. № 3. Т. 2. С. 83-87.

Volodymyr Baranyak

Candidate of Chemical Sciences, Associate Professor Educational and Scientific Institute of Law, Psychology and Innovative Education Lviv Polytechnic National University, Chair of Criminal Law and Procedure
e-mail: baranyakvm@gmail.com

RELEVANCE OF DIGITAL FORENSICS IN CONDITIONS DIGITALIZATION OF MODERN SOCIETY

The author substantiates the relevance of digital forensics in the context of digitalisation of modern society, notes the active use of digital technologies in solving various types of illegal activities in the field of computer information, and defines the concepts of «digital trace» and «digital forensics».

The author emphasises the need to develop new knowledge and developments in forensic techniques, standards and principles for evaluating and verifying collected evidence (digital traces), to carry out mandatory standardisation when working with digital information, and to consider and develop appropriate methodology for training specialists in the field of digital forensics.

Attention is focused on ethical, legal and privacy issues related to the collection and use of digital data during an investigation, confidentiality and protection of personal information of persons not involved in a criminal offence, compliance of the collection and use of digital data during an investigation with certain legal norms and standards (obtaining court orders for evidence collection, requirements for information storage, observance of the rights and freedoms of persons under investigation), ensuring an appropriate level of protection, storage and transmission of personal information and restricting access to it only on certain grounds.

Key words: *digitalisation, digital traces, digital forensics, standardisation, privacy.*