Гальченко Вікторія Сергіївна,
ад'юнкт докторантури та ад'юнктури
Національної академії внутрішніх справ;
Мурзо Євгенія Олександрівна,
ад'юнкт докторантури та ад'юнктури
Національної академії внутрішніх справ

НАЛЕЖНІСТЬ І ДОПУСТИМІСТЬ ЕЛЕКТРОННИХ ДОКАЗІВ, ОТРИМАНИХ ПІД ЧАС РОЗСЛІДУВАННЯ КРИМІНАЛЬНОГО ПРАВОПОРУШЕННЯ ЗА СТ. 432 КК УКРАЇНИ

Використання електронних доказів стає все більш важливим при розслідуванні мародерства, оскільки сучасні технології та цифрове середовище мають значний вплив на злочини цього характеру. Зловмисники можуть залишати сліди у вигляді електронних даних на комп'ютерах або мобільних пристроях, таких як текстові повідомлення, електронна пошта, фотографії, відео, соціальні мережі тощо. Правоохоронні органи можуть аналізувати ці дані, щоб отримати важливі відомості про злочин та можливих осіб, які причетні до нього. Багато місць, де відбувається мародерство, оснащені системами відеоспостереження. Відеозаписи можуть слугувати важливими доказами, де можна бачити самі злочини, а також ідентифікувати зловмисників за їх зовнішнім виглядом або рухами. Правильне використання електронних доказів може значно збільшити ефективність розслідування та допомогти виявити та притягнути до відповідальності злочинців, що вчинили мародерство.

Проблематика даної теми полягає у специфіці вчинення мародерства, наявними слідами даного правопорушення, особливостями ідентифікації особи злочинця, недостатнім використанням технічних засобів тощо. Окрім цього, в умовах воєнного стану ускладнюється збір та фіксація доказів.

Важливого значення набуває один із нових напрямів криміналістики – цифрова криміналістика. Дана галузь дозволяє розробляти дієві інструменти для розслідування кримінальних правопорушень, особливо тих, які вчинені в умовах воєнного стану, окупації територій чи збройних конфліктів, коли є обмежений доступ до місця події або коли потрапити туди взагалі неможливо.

Кримінальний кодекс України (далі – ККУ) визначає мародерство військовим кримінальним правопорушенням, тобто його можуть скоїти лише військовослужбовці. Відповідно до ст. 432 ККУ, мародерство – це викрадення речей на полі бою, що знаходяться при вбитих чи поранених [1]. Стаття 432 ККУ визначає два чітких критерії кваліфікації мародерства як кримінального правопорушення: по-перше, існує чітка локація вчинення даного злочину – викрадення майна на полі бою (тобто, ділянка, на якій ведуться або колись велись бойові дії, також сюди відноситься зона, яка перебуває під обстрілом

військової техніки), по-друге, викрадення особистих речей, які знаходяться біля вбитих або поранених. Варто відзначити, що це стосується саме особистих речей, а не тих, які можуть в подальшому бути використані для ведення бойових дій.

Використання електронних доказів може бути важливим засобом при розслідуванні мародерства. Електронні докази – це інформація в електронній (цифровій) формі, що містить дані про обставини, що мають значення для справи: електронні документи (текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо); вебсайти (сторінки); текстові, мультимедійні та голосові повідомлення; метадані, бази даних та інші дані в електронній формі. Такі дані можуть зберігатися, зокрема, на портативних пристроях (картах пам'яті, мобільних телефонах тощо), серверах, системах резервного копіювання, інших місцях збереження даних в електронній формі (в тому числі в мережі Інтернет) [2].

Основними видами електронних доказів при розслідуванні мародерства можуть бути:

1. Відео- та фотодокази: відео та фотозаписи можуть засвідчити факти мародерства, показати осіб, задіяних у злочині, або зафіксувати інші подробиці. Такі докази можуть бути отримані з камер спостереження, мобільних пристроїв свідків або соціальних мереж.

2. Електронні комунікації: електронна пошта, повідомлення в соціальних мережах, SMS-повідомлення та інші форми електронної комунікації можуть містити важливу інформацію про злочинців, їх співучасників.

3. Інтернет-сліди: мародерство може мати електронний слід у вигляді активності на веб-сайтах, форумах, соціальних мережах тощо. Такі дані можуть надати важливу інформацію про дії та мотиви злочинців.

Варто зазначити, що для української правової системи отримання доказів з відкритих джерел інформації є чимось новим. Під час пошуку та фіксації такої інформації вона лише за певних умов може стати електронним доказом. 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» змінив правове регулювання використання цифрових доказів [3]. Одна із змін полягала в тому, що спеціаліст отримав право надавати пояснення, консультації та довідки. Чинний Кримінальний процесуальний кодекс України (далі – КПК) та вищезгаданий закон не описують вимог, яким має відповідати така довідка. Можна зробити висновок, що вона буде відноситись до документів, як джерело доказів.

Також, даний закон визначив можливість знімати показання з технічних приладів та засобів, у яких функція фото- та відеозйомки у особи, яка є власником чи володільцем таких засобів або приладів, для з'ясування необхідних обставин справи. Зняття показань з даних

технічних пристроїв відбувається на підставі постанови слідчого або прокурора і за необхідності залучається відповідний спеціаліст. Ця постанова повинна містити такі дані: номер та найменування кримінального провадження, відомості про власника технічних пристроїв, період часу за який має здійснитись зняття показань з технічних засобів.

З урахуванням сучасних викликів, потрібно внести доповнення та зміни до глави 4 КПК, у якій варто передбачити визначення електронних (цифрових) доказів та його джерела. Також варто визначити критерії належності та допустимості електронних доказів. Крім цього, потребує регламентації порядок виявлення, пошуку, фіксації, вилучення та зберігання електронних доказів під час проведення слідчих (розшукових) дій.

Збираючи інформацію з відкритих джерел (соціальних мереж, новинних сайтів, блогів тощо), є можливість оглянути фото та відео випадків мародерства. Після огляду слідчому варто призначити судову портретну експертизу або експертизу фото-, відео-, звукозапису для того щоб ідентифікувати особу яка вчинила кримінальне правопорушення за голосом, обличчям тощо [4]. Щоб уникнути слідів монтажу та редагування фото-, відео- та звукозаписів варто призначати комп'ютерно-технічну експертизу. Щоб з'ясувати вартість предмету посягання необхідно призначити товарознавчу експертизу. Речами, які є предметом мародерства, можуть бути лише ті предмети матеріального світу, щодо яких виникають цивільні права та обов'язки і які пов'язані із забезпеченням сфери особистого життя людини. До таких речей можуть відноситись годинники, обручки, підвіски тощо [5]. Отже, однією з найбільш важливих процедур у кримінальному провадженні яке пов'язане з розслідуванням мародерства, є проведення вищезазначених експертиз.

Отже, електронні докази можуть включати в себе фотографії, відеозаписи, комунікаційні записи, метадані та інші цифрові дані, що можуть підтверджувати факт мародерства або ідентифікувати злочинців. Важливо забезпечити належне збереження електронних доказів, оскільки вони можуть бути використані в судовому процесі. Це включає правильне збереження метаданих, ланцюжок доведення та забезпечення недоступності для сторонніх осіб. Електронні докази можуть бути піддані експертизі, щоб підтвердити їх автентичність, цілісність та достовірність. Сюди може входити перевірка та аналіз метаданих, порівняння зразків, проведення комп'ютерно-технічної експертизи та інші технічні процедури. Важливо співпрацювати з відповідними службами безпеки, розвідки або військовими, для забезпечення належного збору та обробки електронних доказів. Це допоможе забезпечити правовий аспект розслідування мародерства.

Доказування мародерства вимагає збору та представлення переконливих доказів, що підтверджують наявність цього злочину.

Надійні докази і їх адекватне представлення допоможуть забезпечити справедливе розслідування та притягнення усіх винних злочинців до кримінальної відповідальності. Збір доказів мародерства на полі бою може бути складним і викликати певні труднощі. Звіти людей, які були свідками або потерпілими від мародерства, можуть бути важливим джерелом інформації. Ці свідчення можуть бути зібрані від мирних жителів, військових або журналістів, які перебували на полі бою.

Фотографії та відеозаписи можуть фіксувати моменти мародерства. Це можуть бути знімки зруйнованих будівель, пограбованого майна, фактів насильства або інших порушень прав людини. Важливо перевірити автентичність цих матеріалів та їх походження. Фотографії та відеозаписи можуть зіграти важливу роль у документуванні мародерства.

Список використаних джерел

1. Кримінальний кодекс України: Закон України від 05 квіт. 2001 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text.
2. Сабадин А. Як подати електронний доказ аби його прийняли? *Юридична газета* : веб-сайт. URL: https://yur-gazeta.com/publications/practice/sudova-praktika/yak-podati-elektronniy-dokaz-abi-yogo-priynyali.html.
3. 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: Закон України від 15 бер. 2022 р. № 2137-IX. URL: https://zakon.rada.gov.ua/laws/show/2137-20#Text.
4. Riekkinen J. Electronic Evidence in Criminal Procedure: On the Effects of ICT and the Development towards the Network Society on the Life-cycle of Evidence. *Digital Evidence and Electronic Signature Law Review*. 2019. № 16. P. 6–10. URL: https://journals.sas.ac.uk/deeslr/article/download/5014/4931.
5. Lasaka M. Ius Constituendum of Electronic Evidence Arrangement in Criminal Procedure Law. *Jurnal Legalitas*. 2023. Vol. 16, № 2. P. 154–166. URL: https://ejurnal.ung.ac.id/index.php/JL/article/download/20306/6663.