Грабчук О.В.,
кандидат наук з державного управління,
доцент кафедри права та правоохоронної діяльності,
Державний університет «Житомирська політехніка», м. Житомир

МОЖЛИВОСТІ ЦИФРОВОЇ КРИМІНАЛІСТИКИ В УМОВАХ ВІЙНИ

Цифрові технології в умовах сьогодення стали невід'ємною частиною повсякденного життя та професійної діяльності. Не винятком в даному питанні стають і специфічні сфери, зокрема криміналістика: протягом останніх років зросла важливість цифрової криміналістики як напрямку криміналістичної науки. Причому незважаючи на її зв'язок саме з цифровізацією, вона відіграє важливу роль у розслідуванні не тільки кіберзлочинів, а також традиційних злочинів, які залишають цифрові сліди.

Крім того, в умовах воєнної агресії, яку проводить російська федерація на території нашої країни, значно зросла роль цифрових технологій у військових та розвідувальних операціях. Це, у свою чергу, підвищило актуальність цифрової криміналістики як інструменту для виявлення, аналізу та документування цифрових доказів воєнних злочинів та кіберзлочинів. Цифрова криміналістика стає все більш важливою для національної безпеки, правоохоронної діяльності та міжнародного правосуддя.

В умовах сучасних збройних конфліктів цифрова криміналістика набуває особливого значення. Війни та збройні конфлікти, які відбуваються в XXI столітті, ведуться не лише на полі бою, але й у цифровому просторі. Робота з цифровими доказами в умовах війни ставить перед фахівцями з цифрової криміналістики низку специфічних завдань.

На думку Д.М. Назаренко, основними напрямами цифрової криміналістики в умовах воєнного стану є такі: 1) аналіз інформаційного простору; 2) виявлення та розслідування кіберзлочинів; 3) моніторинг соціальних мереж; 4) кіберзахист [3, с. 144]. В цілому погоджуючись з представленими напрямами, вважаємо, що з них можна було б деталізувати та розширити, зокрема щодо:

– виявлення та розслідування кіберзлочинів. Адже сфера застосування цифрової криміналістики не обмежується виключно кіберзлочинами;

– перейменування «Аналіз інформаційного простору», оскільки в такому трактуванні воно охоплює також і «Моніторинг соціальних мереж».

Таким чином, можливості цифрової криміналістики в умовах війни передбачають:

– виявлення та документування воєнних злочинів. Аналіз цифрових доказів дозволяє встановити факти порушення міжнародного гуманітарного права. Журналісти вже тривалий час використовують інформацію з цифрових джерел в своїх розслідувань. Так, в 2018 р. в ході розслідування вбивства волонтера під час протестів в Газі журналісти зібрали понад 1000 фото і відеозаписи з місця події, за допомогою дрона відзняли весь район та створили 3D-модель у відповідному програмному забезпеченні [5]. Проте «надання доказів для судового провадження й співпраця з прокуратурою щодо ймовірних воєнних злочинів не належать до обов'язків редакції або журналіста» [1]. Для покращення взаємодії між журналістами та правоохоронними органами у контексті розслідування воєнних злочинів варто розробити чіткі протоколи та механізми передачі цифрових доказів, зібраних журналістами, зберігаючи при цьому журналістську незалежність та захист джерел інформації. Важливо організувати навчання для журналістів щодо правильного збору та документування цифрових доказів, які можуть бути використані в судових процесах, а також створити захищені платформи для анонімної передачі інформації від журналістів до правоохоронних органів;

– ідентифікація учасників бойових дій. За допомогою аналізу цифрових слідів можливо встановити особи комбатантів та їх приналежність до військових підрозділів. Так, в нашій країні під час військової агресії «близько 400 слідчих використовують додаток з розпізнавання облич Clearview AI для ідентифікації потенційних злочинців і загиблих» [2];

– розкриття схем незаконного фінансування та постачання зброї. Саме завдяки методам цифрової криміналістики досягається можливість виявлення каналів нелегального постачання зброї та фінансування незаконних збройних формувань. Крім аналізу електронних банківських транзакцій, криптовалютних операцій, експерти з цифрової криміналістики вивчають електронне листування, повідомлення

в месенджерах та дані з соціальних мереж для виявлення зв'язків між учасниками незаконних схем та відстеження логістичних ланцюгів постачання зброї;

– протидія інформаційним операціям та пропаганді. Аналіз цифрових доказів дозволяє викривати факти дезінформації та маніпуляцій. Після подій в Бучі та оприлюднення кадрів з тілами загиблого місцевого населення російська сторона почала просувати ідею про постановку та розміщення цих тіл вже після звільнення. «Проте супутникові знімки допомогли довести, що тіла з'явилися саме під час російської окупації. У цьому контексті не можна також забувати про масові поховання людей» [2]. Крім того, СБУ з початку повномасштабного вторгнення російських військ на територію України постійно виявляє ботоферми, діяльність яких спрямована на те, щоб підірвати авторитет держави і органів влади, і послабити обороноздатність країни. Так, одні з останніх були виявлені в червні 2024 р.: «Служба безпеки нейтралізувала дві ботоферми, які діяли у Коростені (Житомирщина) та у Дніпрі. Фігуранти допомагали російським спецслужбам зламувати телефони українських захисників та поширювати кремлівську пропаганду» [4].

Вищенаведене підтверджує важливість цифрової криміналістики у фіксуванні та розслідуванні кіберзлочинів та воєнних злочинів в умовах сучасної війни. Проте наразі в Україні для підвищення її ефективності необхідно забезпечити виконання певних кроків, зокрема: розвивати нормативно-правову базу у даній сфері, впроваджувати сучасні технології та методи аналізу цифрових доказів, посилювати міжнародну співпрацю у сфері цифрової криміналістики, а також проводити навчання та підвищення кваліфікації фахівців з цифрової криміналістики.

Список використаних джерел:

1. Майкл М. Розслідування воєнних злочинів: Збирання й архівування доказів та інформації. Global Investigative Journalism Network. 1 Грудня 2023 р. URL: https://gijn.org/ua/resurs-ua/rozsliduvanna-voennih-zlociniv-zbiranna-j-arhivuvanna-dokaziv-ta-informacii/

2. Мамедов Г. Цифрова криміналістика. Як це допомогло зібрати докази злочинів у Бучі? New Voice. 8 червня 2022 р. URL: https://nv.ua/ukr/opinion/viyna-

v-ukrajini-yak-cifrova-kriminalistika-vikrivaye-zlochini-rf-v-ukrajini-novini-ukrajini-50248411.html

3. Назаренко Д.М. Напрями використання цифрової криміналістики в умовах воєнного стану. Інформаційні моделюючі технології, системи та комплекси (ІМТСК-2024): V міжнародна науково-практична конференція (м. Черкаси, 18-19 квітня 2024 р.). Черкаси: Черкаський національний університет імені Богдана Хмельницького, 2024. С. 143-145

4. Поліковська Ю. СБУ викрила дві ботоферми, які «розганяли» російські фейки. 12 червня 2024 р. URL: https://ms.detector.media/sotsmerezhi/post/35211/2024-06-12-sbu-vykryla-dvi-botofermy-yaki-rozghanyaly-rosiyski-feyky/

5. Faure G. My Favorite Tools: Malachy Browne. Global Investigative Journalism Network. 25 November 2019. URL: https://gijn.org/stories/my-favorite-tools-malachy-browne/