6. Міжнародні угоди та їх роль у кримінальному аналізі. (2022). Журнал міжнародних відносин, 15(1), с. 78–92.
7. ООН. (2023). Звіт про глобальні зусилля у боротьбі з міжнародною злочинністю. Нью-Йорк: ООН.
8. Ukraine: INTERPOL General Secretariat statement. Режим доступу: https://www.interpol.int/News-and-Events/News/2022/Ukraine-INTERPOL-General-Secretariat-statement
9. Secure Information Exchange Network Application (SIENA).
Режим доступу: https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/secure-information-exchange-network-application-siena
10. UNODC Office in Ukraine. Make Ukraine safer from drugs, organized crime and corruption. Режим доступу: https://www.unodc.org/poukr/uploads/documents/UNODC_in_Ukraine_Factsheet/UNODC_in_Ukraine_Factsheet_EN.pdf
11. Interpol. Data Protection in Interpol. Режим доступу: https://www.interpol.int
12. Europol. SIENA - Secure Information Exchange Network Application.. Режим доступу: https://www.europol.europa.eu
13. European Commission. European Criminal Records Information System (ECRIS). Режим доступу: https://ec.europa.eu
14. UNODC. International Cooperation Against Transnational Organized Crime. Режим доступу: https://www.unodc.org

Василинчук Віктор Іванович,
доктор юридичних наук, професор,
професор кафедри оперативно-розшукової діяльності Національної академії внутрішніх справ;
Поптанич Юрій Михайлович,
аспірант Національної академії внутрішніх справ

ВИКОРИСТАННЯ ІНФОРМАЦІЇ З МЕСЕНДЖЕРІВ ЯК ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

З впровадженням Всесвітньої павутини у 1990-х роках, а потім популяризацією соціальних медіа та смартфонів у 2000-х роках, кількість та якість інформації у відкритому доступі різко змінилися. Сьогодні будь-яка особа зі смартфоном

чи доступом до Інтернету може створювати та поширювати цифровий контент у всьому світі, хоча і різної якості, достовірності та прозорості. Зростаючий обсяг даних та швидкість передачі і обміну такими даними створили нові можливості для слідчих, що ведуть розслідування із використанням даних у відкритому доступі, збирати та аналізувати інформацію про міжнародні злочини та порушення прав людини. У той же час творці контенту тепер можуть поширювати дезінформацію та відносно легко маніпулювати цифровими даними.

Тому світова практика документування злочинів пішла іще далі та запровадила механізм фіксації цифрової інформації із відкритих джерел – протокол Берклі. Тобто документуванню підлягають не лише фактичні дані щодо спілкування між абонентами в месенджерах, а й інформація із відкритих джерел, з метою подальшої її використання в якості доказу для цілей правосуддя. [1, с. 21–22]

Особливо актуальним та дискусійним є питання використання у кримінальному провадженні в якості доказової бази інформації, яка передається абонентами за допомогою месенджерів (Viber, WhatsApp, Telegram, тощо).

Для фіксування слідів вчиненого або вчинюваного кримінального правопорушення правоохоронцям вкрай важливо оглянути вміст переписки месенджерів, які установлені на мобільному телефоні учасника кримінального провадження або іншому належному йому електронному пристрої.

Сама по собі переписка в месенджері не вважатиметься документом, оскільки це лише переписка між абонентами, яка за своїми ознаками тяжіє до звичайного спілкування (передачі інформації).

Для того, щоб переписка в месенджері набула ознак документу та могла слугувати доказом обставин вчинення кримінального правопорушення, її необхідно оформити процесуально правильно, так як того вимагає КПК України.

До процесуального оформлення виявлена на електронному пристрої інформація, що становить інтерес для органу досудового розслідування, може розглядатись лише як невід'ємна частина цього електронного пристрою, який, з огляду на вміст інформації, що в ньому зберігається, де-факто матиме статус речового доказу.

Відтак, для процесуального оформлення виявлених на електронному пристрої фактичних даних, які відображають

обставини вчинення кримінального правопорушення та можуть бути використані як доказ у кримінальному провадженні необхідно провести процесуальні дії із неухильним дотриманням вимог КПК України.

У відповідності до вимог ст. 86 КПК України доказ визнається допустимим, якщо він отриманий у порядку, встановленому цим кодексом [2].

Ст. 159 КПК України зазначає, що тимчасовий доступ до електронних інформаційних систем, комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку здійснюється шляхом зняття копії інформації, що міститься в таких електронних інформаційних системах, комп'ютерних системах або їх частинах, мобільних терміналах систем зв'язку, без їх вилучення [2].

У випадку якщо власник електронних інформаційних систем, комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку не обмежує доступ системою логічного захисту та надає добровільну на огляд вмісту інформації на його електронному пристрої, такий доступ може здійснюватися без ухвали слідчого судді.

Тимчасове вилучення майна також може відбутись під час обшуку чи огляду.

У разі необхідності слідчий чи прокурор вилучає за допомогою апаратно-програмних комплексів копії інформації, що міститься в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, їх невід'ємних частинах. Копіювання такої інформації здійснюється із залученням спеціаліста.

У випадках, передбачених КПК України, хід і результати проведення процесуальної дії фіксуються у протоколі.

Тому після складення протоколу за результатами огляду переписки в месенджері установленого на електронному пристрої із дотриманням процедури визначеної КПК України (ухвала слідчого судді, обшук, добровільна згода, особистий обшук при затримані особи на підставі ст. 208 КПК України, інше) останній може використовуватись в суді, як окремий документ для встановлення необхідних обставин вчинення кримінального правопорушення, а не як речовий доказ.

Окрім процесуального закріплення переписки в месенджері за допомогою протоколу в арсеналі правоохоронних органів є можливість призначити судову комп'ютерно-технічну

експертизу. Під час проведення вказаної експертизи здійснюється відшукання, вилучення та систематизація необхідної інформації. Отримані внаслідок проведення експертизи фактичні дані фіксуються у висновку експерта та додатках до нього.

Зазначений спосіб збирання доказів є актуальним з огляду на те, що в практичній діяльності не завжди можливо детально оглянути кожен електронний носій за участю спеціаліста, наприклад у зв'язку з значною кількістю слідчих дій, що проводяться одночасно.

У подальшому, експерт може ефективно виконати завдання по аналізу даних по відповідним ключовим словам та відповідно до питань поставлених у постанові слідчого (прокурора).

Крім цього у випадках, якщо відомості про кримінальне правопорушення та особу, яка його вчинила, неможливо отримати шляхом проведення слідчих (розшукових) дій, слідчий за погодженням із прокурором або прокурор мають право звернутись до слідчого судді відповідного апеляційного суду із клопотанням про надання дозволу на проведення негласної слідчої (розшукової) дії у виді зняття інформації з електронних інформаційних систем, яка полягає у пошуку, виявленні і фіксації відомостей, що містяться в електронній інформаційній системі або їх частин, доступ до електронної інформаційної системи або її частини, а також отримання таких відомостей без відома її власника, володільця або утримувача лише в рамках розслідування тяжкого та особливо тяжкого злочинів. (3 ст. 264 КПК України) [2].

Результати проведеної негласної слідчої дії в даному випадку оформляються протоколом у відповідності до вимог КПК України.

Вказаний спосіб надає можливість отримати важливу для досудового розслідування інформацію (у вигляді аудіо-, відео-файлів, переписки) та документи (їх проекти), якими особи причетні до протиправної діяльності обмінювалися між собою під час підготовки, вчинення, приховування слідів кримінального правопорушень.

У подальшому отриману інформацію та доказову базу можна використати при проведенні слідчих (розшукових) дій (обшук, огляд, допит, тощо.), зокрема для виявлення та вилучення оригіналів документів, перевірки під час отримання показань свідка, потерпілого, підозрюваного, тощо.

Таким чином, до процесуального оформлення виявлена на електронному пристрої інформація, що становить інтерес для органів досудового розслідування, може розглядатись лише як невід'ємна частина цього електронного пристрою, який, з огляду на вміст інформації, що в ньому зберігається, де-факто матиме статус речового доказу.

Після складення протоколу за результатами огляду переписки в месенджері установленого на електронному пристрої із дотриманням процедури визначеної КПК України (ухвала слідчого судді, обшук, добровільна згода, особистий обшук при затримані особи на підставі ст. 208 КПК України, інше) чи відповідного протоколу, у разі проведення НС(Р)Д, чи отримання висновку експерта останні може використовуватись в суді, як окремий документ для встановлення необхідних обставин вчинення кримінального правопорушення, а не як речовий доказ.

Список використаних джерел

1. Протокол Берклі з ведення розслідувань з використанням відкритих цифрових джерел/ практичний посібник – 2020 р.: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf.

2. Кримінальний процесуальний кодекс України, URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text.

Демедюк Сергій Васильович
кандидат юридичних наук, заступник Секретаря Ради національної безпеки і оборони України

ОСОБЛИВОСТІ ОНЛАЙН ШАХРАЙСТВА В УКРАЇНІ

On-line шахрайство є найбільш поширеним видом кіберзлочину. У загальній сукупності злочинів, протидія яким є пріоритетом в діяльності кіберполіції, більше третини складають кримінальні правопорушення, пов'язані із шахрайством, при вчиненні яких використовуються сучасні інформаційні та телекомунікаційні технології. Водночас, 84% шахрайств вчиняються саме у формі діяльності передбаченої частинами 3 та 4 ст. 190 ККУ, що ще раз підкреслює надзвичайну поширеність on-line шахрайства в Україні.

За методологією Європол IOCTA, із врахуванням значної різноманітності способів та засобів, що використовуються при