

Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні : наказ МВС України від 07.07.2017 № 575.

5. Про затвердження Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні : наказ ГПУ, МВС, СБУ, АДПС, МФ, МЮ України від 16.11.2012 № 114/1042/516/1199/936/1687/5.

6. Про оперативно-розшукову діяльність : Закон України від 18 лютого 1992 р. № 2135–ХІІ // ВВРУ, 1992. № 22. Ст. 303.

7. Спеціальна техніка: основні поняття, терміни та визначення : навчальний посібник / М.В. Кобець, Б.В. Жуков, П.П. Артеменко. Київ : Аванпост-Прим, 2013. 192 с.

Козій Василь Васильович,

докторант кафедри оперативно-розшукової діяльності Львівського державного університету внутрішніх справ, кандидат юридичних наук

КОПИЮВАННЯ, АРХІВУВАННЯ ТА ГЕШУВАННЯ ФАЙЛІВ ПРИ ЗДІЙСНЕННІ ФІКСАЦІЇ ДАНИХ З МЕРЕЖІ «ІНТЕРНЕТ» ПІД ЧАС РОЗСЛІДУВАННЯ ЗЛОЧИНІВ У СФЕРІ КРИПТОВАЛЮТ

Починаючи із появи у 2008 році першої у світі криптовалюти біткоїна, і по наш час відбувся бурхливий розвиток криптовалют. Наразі ринок криптовалют являє собою десятки, якщо не сотні тисяч ресурсів, які надають можливість будь-кому, практично в бідь-якій точці світу, всього за декілька хвилин за допомогою грошових коштів із банківської карти придбати ту чи іншу криптовалюту, NFT-токени, або стейблкоїни. Так, відповідно до даних ресурсу CoinMarketCap, станом на 16.03.2023 на ньому наявна інформація про 22 940 криптовалют та 5870 онлайн бірж, на яких здійснюється торгівля криптовалютою, а капіталізація ринку криптовалют становить понад трильйон доларів США, при цьому добовий обсяг торгів перевищує 78,5 мільярди доларів США [1].

Ресурс Coin Gecko станом на 16.03.2023 містить інформацію про 11 393 монети, які на ньому відстежуються [2].

У багатьох країнах світу криптовалюта стала звичним явищем у житті мільярдів людей.

В Україні криптовалюту законодавцем віднесено до віртуальних активів. Так, 17.02.2022 ухвалено Закон України «Про віртуальні активи», який проте до цього часу не набрав чинності. Згідно з п. 1 указанного Закону віртуальний актив – це нематеріальне благо, що є об'єктом цивільних прав, має вартість та виражене сукупністю даних в електронній формі [3].

Ринок криптовалют являє собою потужну індустрію, до нього все частіше й частіше проявляють інтерес злочинці. Крім незаконного заволодіння криптовалютою шляхом зламу електронних гаманців потерпілих, криптовалюту використовують для покупки заборонених речей в мережі Даркнету, а також для фінансування тероризму.

За повідомленням Transparency International, в РФ масово використовують криптовалюти для виведення коштів в обхід санкцій. В Москві виявлено як мінімум вісім позабіржових брокерів, які можуть продавати десятки тисяч доларів у стейблкоїнах, а потім обмінювати їх у Великобританії на фунти стерлінгів. Вони будуть обробляти криптовалюту на суму від 10 000 доларів: Pridechange, Bitokk, Alfa. exchange, Finex24, Mychange, 24ExPay, Trust-exchange і OTC Suex, що знаходяться під санкціями, але продовжують працювати [4].

За допомогою криптовалюти здійснюється і фінансування війни проти України. За даними компаній з відстеження криптовалюти Chainalysis, Elliptic і TRM Labs, а також відділу розслідувань найбільшої у світі криптовалютої біржі Binance, головними бенефіціарами були воєнізовані групи, які постачають боєприпаси та спорядження, військові підрядники та виробники зброї. Фахівці з'ясували, що за перші 8 місяців повномасштабної війни Росії проти України групи, які підтримують окупантів, завдяки криптовалюти зуміли зібрати для них понад 4 мільйони доларів [6].

Зазвичай при вчиненні такого виду злочинів злочинці залишають після себе електронні цифрові сліди, якими можуть бути повідомлення на різних ресурсах в мережі «Інтернет», повідомлення, фото та відеозаписи на каналах у різних месенджерах для спілкування (Телеграм, Вотс Ап, Вайбер та ін), контент із соціальних мереж (Фейсбук, Ютуб, Тік Ток та ін). Це може бути реклама в інтернеті, інтерв'ю із певними особами і таке ін. Загалом це може бути інформація або у вигляді фото чи відеозаписів або текстових повідомлень.

Випадки незаконного заволодіння та використання криптовалюти вимагають відповідної уваги оперативних працівників, слідчих, детективів та прокурорів. У цьому контексті важливе значення має фіксування злочинної діяльності за допомогою як процесуального так і технічного інструментарію.

Одним із способів, які покликані допомогти у фіксації такої злочинної діяльності є огляд документів в електронній формі (з інтернету) та її копіювання, архівування і гешування файлів.

Так, ч. 1 ст. 237 КПК України наділяє повноваженнями слідчого, прокурора проводити огляд місцевості, приміщення, речей, документів та комп'ютерних даних з метою виявлення та фіксації відомостей щодо обставин вчинення кримінального правопорушення. При цьому ч. 2 цієї статті встановлює, що огляд комп'ютерних даних проводиться слідчим, прокурором шляхом відображення у протоколі

огляду інформації, яку вони містять, у формі, придатній для сприйняття їх змісту (за допомогою електронних засобів, фотозйомки, відеозапису, зйомки та/або відеозапису екрана тощо або у паперовій формі).

Отже, для фіксації слідів злочинної діяльності у вказаних вище випадках можливо проводити огляд документів в електронній формі, які містять відповідні відомості, зокрема відомості з електронних інформаційних систем, доступ до яких не обмежується її власником, володільцем або утримувачем та не пов'язаний з подоланням системи логічного захисту. При цьому з метою одержання допомоги з питань, що потребують спеціальних знань, слідчий, прокурор для участі в огляді можуть запросити спеціалістів, у даному випадку у галузі ІТ, комп'ютерних технологій.

Зокрема, в процесі огляду можливо використовувати такі програми як Mozilla Firefox із розширенням Easy Youtube Video Downloader Express, а також такі програми як MediaInfo, RapidCRC Unicode.

Так, залежно від того, що саме фіксується, у процесі огляду можливо використовувати функцію «Знімок екрана» браузера «Mozilla Firefox», та зберігати на носій інформації знімок екрана всієї сторінки. Також за допомогою програмного забезпечення може бути здійснене копіювання фото чи відеофайлів. З метою фіксації метаданих скопійованого файлу можна використовувати програму MediaInfo. За допомогою програми RapidCRC Unicode проводиться обчислення геш-кодів файлів, результати чого мають бути зазначені у протоколі. Веб-ресурси, які підлягають архівації, можуть бути заархівовані із використанням веб-сервісу архівування «Internet Archive» (цифрова бібліотека), який доступний за посиланням <https://web.archive.org>.

Відповідно до вимог ч. 4 ст. 99 КПК України, дублікат документа (документ, виготовлений таким самим способом, як і його оригінал), а також копії інформації, у тому числі комп'ютерних даних, що містяться в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, їх невід'ємних частинах, виготовлені слідчим, прокурором із залученням спеціаліста, визнаються судом як оригінал документа.

Підбиваючи підсумки наведеному вище слід відзначити, що здійснення фіксації даних з мережі «Інтернет» за допомогою відповідного програмного забезпечення і можливостей веб-сервісів та з дотриманням вимог КПК України і в передбаченому ним порядку дозволяє зафіксувати сліди злочинної діяльності та використати їх в суді як належний та допустимий доказ з метою доведення вини осіб, які вчинили злочинні діяння.

Список використаних джерел

1. CoinMarketCup [Електронний ресурс]. – Режим доступу: <https://coinmarketcap.com/uk>.

2. CoinGeko. [Електронний ресурс]. – Режим доступу: <https://www.coingecko.com/uk>.

3. Про віртуальні активи: Закон України від 17 лютого 2022 року № 2074-ІХ. офіц. текст: / Офіційний веб-сайт Верховної Ради України [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/2074-20#Text>.

4. В рф масово використовують криптовалюти для виведення коштів в обхід санкцій [Електронний ресурс]. – Режим доступу: <https://sprotyv.info/ekonomika/v-rf-masovo-vikoristovuyut-kriptovalyuti-dlya-vivedennya-koshtiv-v-obhid-sankcij>.

5. Цифрова небезпека: що відомо про боротьбу з фінансуванням війни в Україні через криптовалюти: [Електронний ресурс]. – Режим доступу: https://financy.24tv.ua/kriptovalyuti-vikoristovuyut-dlya-finansuvannya-viyni-rosiyi_n2240031.

Коломієць Світлана Ігорівна,

начальник Відділу організації кінологічної діяльності Національної поліції України

Злагода Ольга Валеріївна,

доцент кафедри оперативно-розшукової діяльності Національної академії внутрішніх справ, кандидат юридичних наук, доцент

НАПРЯМИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАСТОСУВАННЯ СЛУЖБОВИХ СОБАК НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ ДЛЯ ПОШУКУ ВИБУХОНЕБЕЗПЕЧНИХ ПРЕДМЕТІВ

З початку повномасштабного вторгнення збройних сил російської федерації на територію України у лютому 2022 року, сили безпеки і оборони нашої держави зіштовхнулися з небаченим досі масштабом загроз широкого спектру, вчасне і результативне реагування на які стало справжнім викликом для відповідних державних суб'єктів та їх посадових осіб, оскільки безпосередньо пов'язано зі збереженням життя і здоров'я людей, як найважливішої соціальної цінності [1, ст. 3]. Конкретизуючи актуальні загрози, які безпосередньо пов'язані із веденням бойових дій, слід акцентувати увагу на значному збільшенні використання і розповсюдження вибухових пристроїв, боєприпасів агресором. У зв'язку з цим, роль засобів і алгоритмів вчасної протидії такій загрозі набула нового і особливого значення. На цьому тлі практика підготовки і застосування службових собак як спеціального засобу підтверджується не тільки у якості унікального процесу, спрямованого на виявлення вибухонебезпечних предметів, а й являється своєрідним «середовищем» у площині якого доцільно знаходити нові можливості використання потенціалу службової кінології у напрямі пошуку вибухонебезпечних предметів.