УДК 343.13
DOI https://doi.org/10.32782/2524-0374/2023-2/113

# ПОРЯДОК ТА ОСОБЛИВОСТІ ВИЛУЧЕННЯ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ НЕЗАКОННО ЗДОБУТОЇ КРИПТОВАЛЮТИ

# PROCEDURE AND PARTICULARS OF REMOVING ILLEGALLY OBTAINED CRYPTOCURRENCY IN CRIMINAL PROCEEDINGS

**Козій В.В., к.ю.н.,**
**докторант кафедри оперативно-розшукової діяльності**
*Львівський державний університет внутрішніх справ*

Статтю присвячено дослідженню вилучення у кримінальному провадженні незаконно здобутої криптовалюти. Це є особливо актуальним у зв'язку із тим, що криптовалюти упродовж останніх років набули значного поширення. Водночас у цій сфері суспільних відносин вчиняється так само багато протиправних діянь, внаслідок чого потерпілі втрачають належну їм криптовалюту.

У процесі дослідження застосовано формально-логічний метод, а також методи системного та техніко-юридичного аналізу, що дозволило сформулювати підхід та правила вилучення викраденої у потерпілих криптовалюти. Наведено поняття криптовалюти та особливості її обігу. Проаналізовано процесуальний інструментарій, яким наділені слідчий та прокурор у контексті вилучення криптовалюти під час досудового розслідування злочинів, пов'язаних із некоконним заволодінням криптовалютою.

Зазначено про необхідність залучення спеціаліста до проведення відповідних слідчих (розшукових) дій. Запропоновано покроковий алгоритм вилучення криптовалюти та вказано способи її збереження. Сформульовано вимоги до того, яка інформація і в якій послідовності має відображатися у протоколах слідчих (розшукових) дій при вилученні криптовалюти. Зокрема відзначено, що у випадку отримання доступу до криптовалюти, її має бути невідкладно переведено на електронний гаманець, який контролюється слідчим або прокурором чи органом досудового розслідування або прокуратури.

Вказано про необхідність при вилученні криптовалюти зазначати у протоколі слідчої (розшукової) ідентифікаційних ознак гаджетів та встановленого на них програмного забезпечення для зберігання криптовалюти, а також вказувати чи обмежено доступ до гаджета системою логічного захисту та способу його подолання, у тому числі логінів та паролів. Також вказано про необхідність зазначення у відповідних протоколах назви криптовалюти, яка вилучається, її кількості, повних даних електронних гаманців, на яких вона знаходиться, зазначення публічних ключів, її балансу, хешів та інших даних всіх транзакцій. Запропоновано способи збереження приватних ключів від вилученої криптовалюти. Сформульовано практичні рекомендації щодо методики і тактики вилучення криптовалюти слідчим, прокурором.

**Ключові слова:** криптовалюта, блокчейн, злочини у сфері криптовалют, незаконне заволодіння криптовалютою, вилучення криптовалюти, розслідування незаконного заволодіння криптовалютою.

The article is devoted to the investigation of the seizure of illegally obtained cryptocurrency in criminal proceedings. This is especially relevant due to the fact that cryptocurrencies have gained significant popularity in recent years. At the same time, in this sphere of social relations, there are just as many illegal acts, as a result of which the victims lose their cryptocurrency.

In the process of research, the formal-logical method, as well as the methods of systemic and technical-legal analysis, were applied, which made it possible to formulate the approach and rules for the recovery of cryptocurrency stolen from the victims. The concept of cryptocurrency and features of its circulation are presented. The procedural tools available to the investigator and the prosecutor in the context of the seizure of cryptocurrency during the pre-trial investigation of crimes related to illegal acquisition of cryptocurrency have been analyzed.

It is noted that it is necessary to involve a specialist in conducting relevant investigative (search) actions. Methods of saving cryptocurrency are indicated and a step-by-step algorithm for its withdrawal is proposed. The requirements for what information and in what sequence should be displayed in the protocols of investigative (search) actions during the withdrawal of cryptocurrency have been formulated. In particular, it was noted that in case of gaining access to cryptocurrency, it should be immediately transferred to an electronic wallet controlled by an investigator or prosecutor or a pre-trial investigation body or prosecutor's office.

It is indicated the need to indicate in the investigation protocol the identification features of gadgets and the software installed on them for storing cryptocurrency, as well as indicating whether access to the gadget is limited by a logical protection system and a way to overcome it, including logins and passwords. It is also indicated the need to indicate in the relevant protocols the name of the cryptocurrency to be withdrawn, its amount, complete data of the electronic wallets in which it is located, the indication of public keys, its balance, hashes and other data of all transactions. Ways to save private keys from cryptocurrency are proposed. Practical recommendations on the methodology and tactics of cryptocurrency withdrawal by investigators and prosecutors have been formulated.

**Key words:** cryptocurrency, blockchain, crimes in the field of cryptocurrencies, illegal possession of cryptocurrency, withdrawal of cryptocurrency, investigation of illegal possession of cryptocurrency.

У світі упродовж останніх років відбувся неймовірний розвиток сфери криптовалют. Практично будь яка особа може бути власником тієї чи іншої криптовалюти, маючи банківську картку та доступ до мережі Інтернет. Процес покупки криптовалюти на онлайн біржі чи обміннику і переведення її на власний електронний мультивалютний криптовалютний гаманець займає всього декілька хвилин і є достатньо анонімною операцією. Набули значного поширення торгівля криптовалютою на централізованих та децентралізованих (DeFi, DEX) онлайн-біржах та обмінних ресурсах; багато людей переводять у неї заощадження, сплачують за товари та послуги, дарують, передають у борг, спадок і т. ін. Також криптовалюту можна одержати внаслідок промислового та побутового майнінгу за допомогою потужної комп'ютерної техніки – процесорів та відеокарт або спеціалізованого обладнання – айсіків, які використовуються для здійснення складних обчислень, взятих за основу в системах криптовалют. Крім того, придбавши певну кількість криптовалюти, її можна використати для стейкінгу – отримання певних відсотків за її блокування у блокчейні по аналогії із банківським депозитом. Для цього електронний гаманець необхідно за допомогою програмного забезпечення синхронізувати із відповідними сервісами.

Відповідно до даних інтернет ресурсу CoinGeko, станом на 24.02.2023 на ньому містилася інформація про 12 309 монет (криптовалют) та 667 бірж, які здійснювали торгівлю криптовалютами, а загальна капіталізація ринку криптовалют становила понад 1 трильйон 143 мільярди доларів США [1].

Володіти криптовалютою легко і зручно, адже за її допомогою можна оплатити покупки та надані послуги у багатьох країнах світу, екстериторіально, перебуваючи за межами тієї чи іншої країни, і при бажанні залишаючись

при цьому анонімним. Проте такі властивості криптовалюти дозволяють використовувати її не тільки законослухняним громадянам, але й злочинцям. Також з кожним роком має місце все більше й більше випадків незаконного заволодіння криптовалютою внаслідок хакерських атак на онлайн біржі та викрадення криптовалюти внаслідок зламу криптовалютних гаманців її власників. Про масштаби проблеми свідчить повідомлення агентства Reuters від 01.02.2023 про те, що упродовж 2022 року хакери вкрали $3,8 млрд у криптовалюті, що є абсолютним рекордом. Найбільше викрали зловмисники з Північної Кореї. Хакери, пов'язані з Північною Кореєю, такі як синдикат кіберзлочинців Lazarus Group, були найактивнішими викрадачами криптовалют. За різними оцінками, вони викрали близько $1,7 млрд під час численних атак у 2022 році [2].

У зв'язку з цим перед слідчими правоохоронних органів та прокурорами постає багато викликів, які стосуються розслідування таких злочинів і особливо актуальним є питання вилучення у кримінальному провадженні незаконно здобутої криптовалюти та її повернення законному власнику або, за певних обставин, і конфіскації в дохід держави. Окремі питання, які стосуються правового регулювання криптовалют (віртуальних активів), а також розслідування злочинів у сфері криптовалют містяться у працях Р.Й. Бачо, В.Д. Іванюк, І.С. Карпюка та О.В. Кузьменко, Д.В. Казначеєвої та А.О. Дорош, О.В. Кремінського, А.В. Мовчана, А.Ю. Плюшкіна, В.О. Рядінської, Н. Хак Сіддікі та Р.О. Мовчана, В.В. Носова та І.А. Манжай, а також інших науковців.

Проте до цього часу в Україні немає ані відповідних наукових досліджень, ані науково-практичних посібників, ані методичних рекомендацій, які б стосуватися особливостей проведення слідчих (розшукових) дій щодо вилучення криптовалюти, якою незаконно заволоділи. Немає жодних роз'яснень і будь-яких орієнтирів щодо того яким чином слідчому (прокурору) діяти у випадку знаходження у злочинців гаджетів, на яких знаходиться незаконно здобута криптовалюта.

Водночас слідчі та прокурори все частіше і частіше стикаються при розслідуванні злочинів із незаконно здобутою криптовалютою, і такі випадки широко висвітлюються в засобах масової інформації. Наприклад, Вищий антикорупційний суд заарештував понад 57 тисяч доларів криптовалюти оперативного співробітника департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Служби безпеки України, якого підозрюють в одержанні неправомірної вигоди. Таке рішення ще 1 серпня 2022 ухвалив слідчий суддя ВАКС, і його залишила без змін Апеляційна палата ВАКС. Рішенням від 1 серпня 2022 року було накладено арешт на 25377,8 одиниць криптовалюти Tether на одному рахунку і 32 003 одиниць криптовалюти Tether – на іншому. Також на цих рахунках знайшли 10 доларів у криптовалюті Ethereum і 8 доларів у криптовалюті Tron. У сумі арешт наклали на 57 412 доларів. Адвокат підозрюваного працівника СБУ подав скаргу на це рішення, оскільки валюта нібито не належить його клієнту, попри наявність у нього ключів доступу до гаманців [3].

**Метою статті** є з'ясування порядку та особливостей вилучення у кримінальному провадженні незаконно здобутої криптовалюти та пошук і знаходження способів вирішення наявних проблем. Передусім потрібно з'ясувати що таке криптовалюта, які її види та основи функціонування і обігу, а також яким процесуальним інструментарієм КПК України наділяє слідчого, прокурора щодо вилучення криптовалюти. Це допоможе визначати покроковий алгоритм, порядок і спосіб вилучення криптовалюти та особливості відображення цього у відповідних процесуальних документах: протоколах обшуку, огляду та ін.

В Україні 17.02.2022 ухвалено Закон України «Про віртуальні активи», аналіз якого свідчить про те, що під віртуальним активом законодавець визнає у тому числі криптовалюту, і відповідно до п. 1 ст. 1 якого віртуальний актив – це нематеріальне благо, що є об'єктом цивільних прав, має вартість та виражене сукупністю даних в електронній формі. інші об'єкти цивільних прав [4].

Найпершою і найбільш відомою криптовалютою у світі є біткоїн (BTC), який являє собою цифровий електронний актив, обіг якого забезпечується електронною платіжною системою, заснованою на публічно доступній книзі обліку під назвою блокчейн, що в перекладі з англ. означає «ланцюг блоків». Всі інші криптовалюти, а їх наразі десятки тисяч, були створені після біткоїна, і їх називають альткоїнами. Деякі з них є форками біткоїна, тобто в основі їх функціонування закладено програмний код біткоїна, але з деякими відмінностями. Другою найвідомішою після Біткоїна криптовалютою є Ethereum (ефіріум). Він являє собою перший у світі програмований блокчейн, який дозволяє розробникам створювати і розгортати децентралізовані додатки (DApps), а також смартконтракти. Також криптовалюти поділяються на децентралізовані і стейблкоїни, тобто стабільні монети. Якщо курс децентралізованих криптовалют постійно змінюється, і іноді досить істотно у продовж короткого часу, то курс стейблкоїнів є стабільним і відповідає вартості активу, який його забезпечує, наприклад 1 долару США чи 1 Євро або вартості одинці виміру золота. Більшість криптовалют є децентралізованими, адже відсутній єдиний емісійний центр, яким у випадку емісії грошових коштів є центральні банки та уряди країн світу. Криптовалюта – це віртуальні електронні активи, які являють собою унікальні криптографічні коди. Будь-яка криптовалюта умовно складається із набору букв та цифр, і при цьому із цих самих символів складається адреса гаманця, так званий публічний ключ, який генерується системою і який потрібно знати тому, хто збирається переказати на нього певну суму тієї чи іншої криптовалюти. Проте є ще приватний ключ, який не можна передавати нікому, так як останній дозволяє у блокчейні тієї чи іншої криптовалюти підтвердити, що відповідна її кількість знаходиться на вказаному гаманці, тобто за вказаною адресою та за потреби перерахувати її на інший гаманець. Володіє криптовалютою лише той, хто має приватний ключ. Також є хеш транзакції, у якому містяться дані про транзакцію. При цьому приватний ключ розшифровує публічний ключ та хеш транзакції, але за допомогою хеша транзакції та публічного ключа не можна розшифрувати приватний ключ. Зазвичай будь-яку транзакцію, тобто відправлення криптовалюти із однієї електронної адреси (електронного гаманця) на іншу (інший електронний гаманець), за деякими винятками, скасувати неможливо.

Упродовж кількох останніх років у Кримінальному процесуальному законодавстві України відбулися певні зміни, які стосуються розслідування злочинів у сфері криптовалют. Зокрема, Законом № 2137-IX від 15.03.2022 «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» до ч. 10 ст. 170 КПК України внесено зміни та передбачено можливість накладення арешту на віртуальні активи, щодо яких ухвалою чи рішенням слідчого судді, суду визначено необхідність арешту майна. Слід звернути увагу і на положення ч. 6 ст. 236 КПК України, якою в тому числі передбачено право слідчого, прокурора під час проведення обшуку долати системи логічного захисту, якщо особа, присутня при обшуку, відмовляється їх зняти (деактивувати). Крім того, якщо під час обшуку слідчий, прокурор виявив доступ чи можливість доступу до комп'ютерних систем або їх частин, мобільних термі-

налів систем зв'язку, для виявлення яких не надано дозвіл на проведення обшуку, але щодо яких є достатні підстави вважати, що інформація, що на них міститься, має значення для встановлення обставин у кримінальному провадженні, прокурор, слідчий має право здійснити пошук, виявлення та фіксацію комп'ютерних даних, що на них міститься, на місці проведення обшуку [5].

Слід зауважити, що оскільки спеціальних норм, які стосуються тимчасового доступу до криптовалюти та її пошуку і вилучення КПК України не передбачає, то такі процесуальні дії мають здійснюватися згідно з положеннями глав 15 та 16 і у випадках, коли положення КПК не регулюють або неоднозначно регулюють питання кримінального провадження, підлягають застосовуванню загальні засади кримінального провадження, як це передбачено ч. 6 ст. 9 КПК України.

Передусім слідчий та прокурор повинні мати хоча б базові знання про те, що таке криптовалюта і як забезпечується її обіг, тому що без цього провести її пошук та вилучення просто неможливо. Більше того, непідготовленість може призвести до втрати криптовалюти, з урахуванням того, що різні блокчейни мають свої технічні особливості функціонування, і це може мати місце якщо здійснити транзакцію на неправильну адресу електронного гаманця або неправильне зазначення мережі, в якій здійснюється транзакція. У такому випадку у гаманці буде відображатися інформація про те що транзакція відбулася, але на новий гаманець криптовалюта так і не надійде і можливість її повернення за загальним правилом, у переважній більшості випадків, неможлива. Якщо йдеться про суму криптовалюти, еквівалент якої становить сотні тисяч або навіть десятки мільйонів доларів, негативні наслідки такої помилки можуть коштувати слідчому кар'єри, звільнення і навіть бути підставою для притягнення до кримінальної відповідальності, зокрема за службову недбалість. Тому у відповідних кримінальних провадженнях правильним при підготовці до проведення відповідних слідчих (розшукових) дій є їх покрокове планування, із врахуванням того, яка криптовалюта розшукується, на яких гаджетах може зберігатися, де можуть зберігатися паролі для доступу до облікового запису на криптовалютній біржі або сід-фрази та приватні ключі від криптовалютних електронних гаманців. Також слідчий, прокурор повинні попередньо визначитися, на які електронні гаманці органу досудового розслідування чи прокуратури або слідчого чи прокурора буде переведена криптовалюта, яке програмне забезпечення та гаджети будуть при цьому використовуватися і як буде забезпечено збереження приватних ключів, паролів та мнемонічних фраз, а також як процесуально це буде відображено у відповідних протоколах слідчих (розшукових) дій.

Отже для того, щоб самостійно провести вилучення криптовалюти, слідчий, прокурор повинні мати відповідний рівень підготовки та навички. Проте навіть і в такому випадку це не убезпечує від допущення помилок. Тому для проведення відповідних слідчих (розшукових) дій слід залучати спеціаліста, яким відповідно до вимог ст. 71 КПК України є особа, яка володіє спеціальними знаннями та навичками і може надавати консультації, пояснення, довідки та висновки під час досудового розслідування і судового розгляду з питань, що потребують відповідних спеціальних знань і навичок.

Очевидно що такими особами можуть бути фахівці у сфері ІТ, а також інші особи, які, наприклад, мають сертифікати чи свідоцтва про проходження тренінгів або навчальних курсів у сфері криптовалют та блокчейну. І консультування із спеціалістом слід здійснювати ще на етапі планування та підготовки до проведення вилучення криптовалюти, а не безпосередньо під час її вилучення.

А.Д. Марушев, досліджуючи консультаційні форми використання спеціальних знань під час розслідування злочинів дійшов до висновків про те, що консультації спеціалістів належать до основних форм використання спеціальних знань під час розслідування злочинів. Консультативна діяльність спеціаліста складається не тільки з усного роз'яснення особливостей використання технічних засобів, але й з попереднього дослідження окремих об'єктів, надання письмових довідкових даних, складання письмових висновків спеціаліста, які є джерелом орієнтуючої інформації для слідчого (оперативного працівника) в пошуку знаряддя злочину, злочинця, предметів його одягу та взуття, транспортного засобу та ін. Комплексне використання таких форм забезпечить об'єктивність, повноту і всебічність досудового розслідування та сприятиме оперативному розкриттю злочинів [6].

Також слідчий та прокурор можуть скористатися послугами АРМА – Агентства з розшуку та менеджменту активів. Так, згідно з ч. 1 ст. 9 Закону України «Про Національне агентство України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів», однією з основних функцій АРМА є здійснення заходів з виявлення та розшуку активів за зверненням слідчого, детектива, прокурора, суду (слідчого судді), надання роз'яснень, методичної та консультаційної допомоги слідчим, детективам, прокурорам та суддям з питань, пов'язаних з виявленням, розшуком активів [7].

На сайті АРМА міститься типовий зразок звернення правоохоронних органів до вказаного органу [8].

Крім того, певну інформацію, яка може допомогти спланувати проведення слідчих (розшукових) дій із подальшим вилученням криптовалюти, зокрема інформацію про підозрілі транзакції у випадку обміну криптовалюти на біржах та переведення грошових коштів на банківські рахунки підозрюваного можна отримати від Держфінмоніторингу України, до повноважень якого відноситься збір, обробка, аналіз інформації про фінансові операції, що підлягають фінансовому моніторингу, інші фінансові операції або інформація, що може бути пов'язана з підозрою у легалізації (відмиванні) доходів, одержаних злочинним шляхом, або фінансуванні тероризму. Обов'язки, права, функції та повноваження Держфінмоніторингу визначені Законом України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» та Положенням про Державну службу фінансового моніторингу України, затвердженим постановою Кабінету Міністрів України від 29.07.2015 № 537 [9, 10].

Але передусім вилучення криптовалюти можливо під час проведення слідчих (розшукових) дій слідчим, прокурором. І перше питання, яке підлягає вирішенню: що саме слід шукати? До гаджетів, на яких може зберігатися програмне забезпечення для доступу до наявної криптовалюти відносяться: 1) смартфони; 2) ноутбуки; 3) комп'ютери; 4) апаратні криптовалютні мультивалютні гаманці (Trezor, ledger Nano); 5) смарт – годинники. Крім того, криптовалюта може зберігатися на паперових носіях, являючи собою набори символів (букв та цифр), а також на QR-кодах, на яких зашифровуються набір цифр та букв (публічний і приватний ключі).

Потрібно враховувати і те, що у будь-якому місці і будь-де та будь-яким способом можуть бути записані також логіни і паролі або тільки паролі чи тільки логіни для доступу до криптовалютних онлайн-бірж чи гаманців, а також мнемонічні або як їх ще називають seed-фрази, за допомогою яких на будь-якому гаджеті можна відновити доступ до криптовалютних мультивалютних гаманців і швидко, упродовж кількох хвилин перерахувати криптовалюту на будь-який інший електронний гаманець, і таким чином завадити її вилученню слідчим чи прокурором. Якщо логінами та паролями зазвичай є букви та символи, то мнемонічна або seed-фраза – це група слів, яка

забезпечує доступ до ваших активів і є резервною копією для вашого крипто-гаманця (її часто також називають Seed-фразою або BIP39). Фраза може містити 12, 18, 24 слова. Найчастіше зустрічаються фрази на 12 та 24 слова [11].

Якщо під час огляду чи обшуку слідчий виявляє апаратний криптовалютний гаманець, то мають бути вжиті заходи до знаходження паролю для доступу до нього. Те саме стосується і смартфонів, планшетів та ноутбуків чи смарт-годинників підозрюваного. Для доступу може знадобитися також подолання системи логічного захисту.

Не завжди у слідчого чи прокурора у наявності може бути інформація про те, яка саме криптовалюта знаходиться у володінні підозрюваного та яким чином до неї можна отримати доступ. Адже умовно кажучи сьогодні підозрюваний може володіти біткоїнами, а взавтра обміняти їх на ефуруім чи солана. Те ж саме стосується і електронних гаманців. Сьогодні це може бути паперовий або апаратний носій, а взавтра мультивалютний гаманець, доступ до якого здійснюється за допомогою смартфона. Залежно від наявності тієї чи іншої інформації і залежить порядок та особливості слідчих (розшукових) дій щодо вилучення криптовалюти. Кожна ситуація по своєму унікальна, і наприклад, у криптовалютному мультивалютному гаманці ATOMIC DEX є функція підробленого балансу, тобто його можна так налаштувати, що, у програмі буде показано лише 10% від кількості наявної криптовалюти. Крім того, деякі електронні гаманці можуть мати нестабільне з'єднання із блокчейнами і тоді баланс буде показувати нуль у той час як насправді на ньому можуть зберігатися мільйони доларів. Звідси слідує надзвичайно важливе правило про те, що адреси гаманців, які відображаються у електронному програмному забезпеченні, встановленому на гаджеті підозрюваного слід перевіряти у блокчейні відповідної криптовалюти у режимі реального часу, що має вказуватися у протоколі обшуку чи іншої слідчої (розшукової) дії. І тут все можуть вирішувати хвилини або навіть секунди, адже доступ до криптовалютних гаманців можуть мати спільники підозрюваного, які територіально можуть перебувати у протилежному куточку світу, взагалі поза дією юрисдикції країни розслідування, а отже будь-яка повільність у вжитті заходів щодо переведення виявленої криптовалюти на криптовалютні гаманці, які контролюються слідчим або прокурором чи органом досудового розслідування або прокуратури може мати фатальні наслідки, адже спільникам може бути достатньо кількох хвилин для того, щоб перевести криптовалюту із одного електронного гаманця на інший.

Іншим важливим правилом є те, шо у протоколах огляду, обшуку мають бути чітко зазначені наступні дані: який вилучений гаджет оглядається, які його повні ідентифікаційні дані (IMEI, номери сім-карт, яке програмне забезпечення для зберігання криптовалюти на ньому встановлено, чи обмежено доступ до нього системою логічного захисту, якщо так то яким способом отримано доступ до криптовалюти, тобто які логін та пароль знайдено та введено, які назва криптовалюти, яка її кількість, повні дані електронних гаманців, на яких вона знаходиться, баланс та дані всіх транзакцій, зокрема час їх здійснення та хеші.

У випадку, якщо вдалося отримати доступ до криптовалюти, то її має бути переведено на електронний гаманець, який контролюється слідчим або прокурором чи органом досудового розслідування або прокуратури. Відповідно у протоколі мають бути вказані публічні ключі (публічні адреси) криптовалюти, хеші транзакцій та час їх проведення, а також її кількість (баланс). Ні в якому разі у протоколі не можна вказувати приватні ключі, та паролі доступу і мнемонічні фрази від криптовалютних гаманців слідчого та прокурора, адже тоді будь-хто зможе упродовж кількох хвилин викрасти криптовалюту.

Це без перебільшення найважливіший етап слідчої (розшукової) дії, адже це таїть у собі ризики випадкової втрати вилученої криптовалюти або й умисного заволодіння нею самими слідчими та прокурорами, які можуть просто не встояти перед спокусою у кілька десятків чи сотень мільйонів доларів США.

Як засвідчило опитування 220 прокурорів – процесуальних керівників у кримінальних провадженнях з приводу того, на які електронні гаманці має переводитися вилучена при проведенні слідчих (розшукових) дій криптовалюта, чи на створені ними, і від яких у них же і знаходяться приватні ключі (мнемонічні фрази, паролі для доступу) чи на електронні гаманці органу досудового розслідування чи прокуратури або ж іншого спеціально визначеного органу 92% опитаних вказали, що криптовалюта має переводитися на електронні криптовалютні гаманці, які не повинні контролюватися ними особисто.

Тому нагальним є створення в Україні спеціально уповноваженого органу, який у тому числі буде забезпечувати створення електронних гаманців криптовалюти та передачу до органів досудового розслідування та прокуратури публічних ключів, тобто публічних адрес електронних гаманців, на які при проведенні слідчих (розшукових) дій слідчий чи прокурор і будуть переводити вилучену криптовалюту. Відповідно приватні ключі будуть знаходитися у цього органу і він буде здійснювати збереження вилученої криптовалюти та в подальшому відповідно до рішення прокурора, слідчого судді чи суду займатися подальшим переведенням криптовалюти потерпілому чи звертати в дохід держави. Альтернативою може бути створення відповідних підрозділів у кожному з правоохоронних органів, але тут ризики зловживань та втрати вилученої криптовалюти видаються значно вищими.

Конфісковану в дохід держави криптовалюту можна продавати на аукціонах, що вже не перший рік практикує Міністерство Юстиції США.

Ранній продаж біткоїна став збитковим для уряду США: втратили $10 млрд. Якби уряд США продавав біткоїни по $50 000, він би заробив понад $10 млрд, однак прибуток склав лише $151,4 млн. Починаючи з 2014 року, уряд США продавав конфісковані біткоїни, які були продуктом шахрайства. Однак, за інформацією від одного з інженерів біткоїну Джеймсона Лоппа, зараз вони могли б заробити набагато більше. Лише з відомого анонімного вебсайту Silk Road було конфісковано біткоїнів на суму близько $1 млрд (за яким саме курсом біткоїна не уточнюється – ред.). Засновник цієї платформи – американець Росс Ульбріхт був засуджений до довічного позбавлення волі за звинуваченнями в наркоторгівлі, хакерських атаках та відмиванні грошей. Платформа стала ринком для всього незаконного, включаючи продаж героїну. Служба маршалів США, підрозділ Міністерства юстиції США, почала продавати активи BTC з усіх джерел ще в червні 2014 року, отримавши перший виторг в розмірі $18,740 за 29 657 BTC від визнаного переможця торгів Тіма Дрейпера. Друга партія аукціонів в тому ж році включала 50 000 BTC, які були віддані за $19 млн. [12].

Проте наразі слідчий та прокурор при пошуку та вилученні криптовалюти можуть розраховувати лише на себе, оскільки жодних органів чи спеціальних підрозділів, на гаманці яких можна було б відправляти вилучену криптовалюту не існує. Загалом є три варіанти куди слідчому чи прокурору перераховувати і як зберігати вилучену криптовалюту – апаратні гаманці (Trezor, Ledger Nano та ін.), мобільні додатки (Trust Wallet, Wia Wallet, Coinomi, Atomic Dex та ін.) та паперові гаманці (з QR-кодом). І зберігання криптовалюти кожним із цих способів має свої переваги та недоліки. Тут слід зупинитися лише на окремих з них. Так, у випадку використання апаратних гаманців, вони мають бути придбані органом досудового розслідування чи прокуратурою і знаходитися на балансі відповідного органу, що вимагає додаткових витрат, також їх слід зберігати у надійному та захищеному місці. У випадку вико-

ристання мобільних додатків має бути визначено перелік таких додатків, рекомендованих до застосування з тим, щоб не скористатися шкідливим програмним забезпеченням, вони мають періодично оновлюватися і т. ін. Тому надзвичайно важливим є питання про те, як слідчому та прокурору зберігати приватні ключі від вилученої криптовалюти та мнемонічні або seed-фрази від криптовалютних гаманців, а також паролі для входу до апаратних криптовалютних гаманців. З урахуванням реалій сьогодення очевидно що такі паролі, фрази та паперові коди мають як додатки до протоколу відповідної слідчої (розшукової) дії бути надійно опечатаними та зберігатися у надійному місці (сейфі) з тим, щоб унеможливити до них несанкціонований доступ сторонніх осіб.

Отже, дослідивши порядок та особливості вилучення у кримінальному провадженні незаконно здобутої криптовалюти доходимо до таких висновків. Слідчі та прокурори повинні мати базові знання у сфері криптовалют та блокчейну. При плануванні і підготовці до проведення, а також при проведенні відповідних слідчих (розшукових) дій слід залучати спеціаліста. Покроковий алгоритм та особливості вилучення криптовалюти такі: пошук гаджетів, на яких знаходиться програмне забезпечення, за допомогою якого можна отримати доступ до криптовалюти; пошук паролів для доступу до акаунтів на криптовалютних біржах чи до програмного забезпечення, за допомогою якого надається доступ до криптовалюти; пошук мнемонічних (seed) фраз, за допомогою яких можна відновити доступ до електронних гаманців, на яких зберігається криптовалюта; пошук публічних та приватних ключів, за допомогою яких можна отримати доступ до криптовалюти; за потреби і в разі технічної можливості подолання системи логічного захисту, які встановлена на гаджетах підозрюваних осіб з метою одержання доступу до криптовалюти; безпосередній доступ до криптовалюти, тобто введення логінів, паролів, мнемонічних фраз та іншої необхідної інформації, що надає можливість контролювати електронні гаманці з криптовалютою чи облікові записи на криптовалютних біржах; вилучення виявленої криптовалюти, тобто її перерахування на не електронні гаманці, які контролюються слідчим чи прокурором або органом досудового розслідування чи прокуратури; вжиття заходів до таємного збереження приватних ключів, паролів та мнемонічних фраз від криптовалюти, що унеможливлює доступ до неї будь-яких сторонніх осіб; відображення у відповідному протоколі слідчої (розшукової) дії відомостей про її хід та результати. У протоколах огляду, обшуку мають бути чітко зазначені наступні дані: який вилучений гаджет оглядається, які його повні ідентифікаційні дані (IMEI, номери сім-карт, яке програмне забезпечення для зберігання криптовалюти на ньому встановлено, чи обмежено доступ до нього системою логічного захисту, яким чином її подолали, назва криптовалюти, її кількість, яким способом отримано доступ до криптовалюти, тобто які логін та пароль чи мнемонічні фрази введено, повні дані електронних гаманців, на яких знаходиться криптовалюта, її баланс та дані всіх транзакцій, тобто публічні ключі (публічні адреси) криптовалюти, хеші транзакцій та час їх проведення, а також її баланс. При цьому в жодному разі у протоколі не вказуються приватні ключі, мнемонічні фрази та паролі, за допомогою яким можливо отримати доступ до криптовалюти. Також після завершення вилучення криптовалюти слідчий, прокурор повинні визнати вилучені криптовалюту речовим доказом та звернутися до слідчого судді з клопотанням про її арешт, а також, за наявності підстав, вжити заходів до її повернення потерпілому.

**ЛІТЕРАТУРА**


1. CoinGeko. URL: https://www.coingecko.com/uk
2. Crypto hacks stole record $3.8 billion in 2022, led by North Korea groups – report. URL: https://www.reuters.com/technology/crypto-hacks-stole-record-38-billion-2022-led-by-north-korea-groups-report-2023-02-01
3. ВАКС заарештував криптовалюту підозрюваного оперативника СБУ. URL: https://www.slovoidilo.ua/2022/10/07/novyna/polityka/vaks-zaareshtuvav-kryptovalyutu-pidozryuvanoho-operatyvnyka-sbu
4. Про віртуальні активи: Закон України Закон України від 17 лютого 2022 р. № 2074-IX. / *Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/2074-20#Text (дата звернення: 23.02.2023).
5. Кримінальний Кодекс України: Закон України від 5 квітня 2001 р. № 2341-III / *Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 24.02.2023).
6. Марушев А.Д. Консультація як одна з форм використання спеціальних знань у кримінальному провадженні. *Юридичний науковий електронний журнал. Електронне наукове фахове видання.* № 4. 2020., с. 307–310. URL: http://www.lsej.org.ua/index.php/dovidnik/2-uncategorised/126-4-2020
7. Про Національне агентство України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів: Закон України від 10 листопада 2015 р. № 772-VIII / *Верховна Рада України*. URL: https://arma.gov.ua/n/1 (дата звернення: 24.02.2023).
8. Типовий зразок звернення правоохоронних органів до АРМА. URL: https://arma.gov.ua/spivrobitnytstvo
9. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення. Закон України від 06 грудня 2019 р. № 361-IX / *Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/show/361-20#Text (дата звернення: 24.02.2023).
10. Положення про Державну службу фінансового моніторингу України, затверджене постановою Кабінету Міністрів України від 29 липня 2015 № 537. Мінітерство фінансів України. URL: https://mof.gov.ua/uk/state-service-for-financial-monitoring (дата звернення: 24.02.2023).
11. Д. Караченцов Що таке мнемонічна фраза? Словник BIP39. URL: https://lwallet.com.ua/22505-що-таке-мнемонічна-фраза-словник-bip39/?lang=uk
12. Ранній продаж біткоїна став збитковим для уряду США: втратили $10 млрд. URL: https://nachasi.com/crypto/2021/03/23/bitkoyin-dlya-ssha