Панченко Євгеній Вікторович,
начальник 4-го управління
Департаменту кіберполіції Національної поліції України

ДОСВІД КІБЕРПОЛІЦІЇ В РОЗСЛІДУВАННІ ЗЛОЧИНІВ, ПОВ'ЯЗАНИХ ІЗ ВІРТУАЛЬНИМИ АКТИВАМИ

Департамент кіберполіції, починаючи від часу створення як окремого структурного підрозділу в системі Міністерства внутрішніх справ, а потім Національної поліції України [3], почав стикатися з віртуальними активами (криптовалютами), що використовували у своїй діяльності представники злочинного світу, зокрема хакери, кібер-анархісти, послідовники ідей Сатоші Накамото [1, 2].

Досвід, здобутий за час роботи Департаменту, є важливим для обміну та поширення серед інших підрозділів Національної поліції України, правоохоронних органів та правозастосовних інституцій. Безперечно, важливим цей досвід буде і в наукових, навчальних посібниках, підручниках та інших матеріалах.

На сьогодні найбільшою проблемою, виходячи зі здобутих результатів практичної роботи, бачиться відсутність належного правового регулювання сфери віртуальних активів в України. Україна втрачає сотні мільйонів доларів доходів бюджету через відсутність регуляції [4], а правоохоронна ланка діє не системно та опирається на загальні норми, що містять відсилки до розуміння віртуальних активів як речей. Тому надалі мова піде саме про практики та підходи щодо вилучення та арешту віртуальних активів, що потребують негайної регуляції в Україні, а також запроваджені в інших країнах.

Арешт активів, що зберігаються на гаманцях сервісів, якими керують постачальники послуг віртуальних активів (VASP), наприклад, криптобіржі, може бути відносно простим, якщо правоохоронні органи мають необхідні законодавчі повноваження, суди, здійснюючи свої повноваження, ухвалюють унормовані рішення, а VASP визнають юрисдикцію цієї країни.

Проте активи, що зберігаються на особистих гаманцях, часто становлять більшу проблему. Їх успішне вилучення вимагає ретельної підготовки, коректного поводження з даними та їх аналізом. У зв'язку з чим, весь процес вилучення слід розділити на 6 етапів:

1. Підготовчий.
2. Ідентифікація.

3. Вилучення.
4. Арешт.
5. Зберігання.
6. Управління.

Розглянемо кожен з етапів окремо, опишемо його особливості та ризики, що можуть виникати.

Перший етап (підготовчий). Незалежно від того, йдеться мова про невідкладну слідчу (розшукову) дію чи заплановану, правоохоронні органи мають бути готові до можливого вилучення віртуальних активів. Це передбачає створення та керування стандартними операційними процедурами (інструкціями) і політиками, що регулюють підхід організації до арешту віртуальних активів, включаючи розуміння та пом'якшення фінансових, операційних, репутаційних і юридичних ризиків.

Урегульована та апробована правова політика повинна чітко визначати та регулювати наступне:

– законодавчі підстави та порядок вилучення й арешту активів;

– перелік мінімально необхідних для залучення осіб, зобов'язання кожного з них і відповідальність на кожному етапі;

– визначене та затверджене програмне та апаратне забезпечення;

– перелік кваліфікаційних вимог до працівників, залучених до проведення заходів із вилучення;

– процес надання внутрішнього схвалення планових і невідкладних заходів з вилучення віртуальних активів.

Усе програмне та апаратне забезпечення мають підтримувати найновіші політики безпеки, проходити тестування та, що не менш важливо, відповідати загальноприйнятим стандартам протоколу, такому як «BIP 39». Стандарт «BIP 39» є проектним документом для впровадження функцій або інформації в Bitcoin. Використання загальноприйнятих стандартів гарантує, що, якщо підтримку гаманця буде припинено, інший гаманець, що працює за стандартом протоколу, може бути використаний для відновлення доступу до активів [5].

Найважливішою частиною будь-якого підготовчого етапу є налаштування гаманців, що контролюються правоохоронними органами, і їх постійна готовність до використання: створення та налаштування гаманців на місці конфіскації завжди має бути останнім варіантом. Через їх граничну чутливість доступ до приватних ключів і початкових значень відновлення має бути суворо захищеним, але надаватися принаймні двом особам у

підрозділі, щоб запобігти єдиній точці компрометації. Резервні копії початкових фраз «Шаміра» служать подібній меті. Shamir – це процес протоколу безпеки, у якому від 12 до 24 початкових слів поділяються на три або більше окремо записаних колекцій, що можна зберігати в різних місцях. Щоб відновити гаманець, потрібно знову зібрати фрази разом [6].

На підготовчому етапі також слід розглянути державно-приватне партнерство з VASP і постачальниками депозитарного (custodial) зберігання віртуальних активів, що нормативно визначені для допомоги в реалізації цілей конфіскації, що реалізовують правоохоронні органи. Правоохоронним органам може знадобитися придбати та утримувати різні активи, наприклад, Ethereum, щоб заплатити за газ (комісію), якщо гаманець підозрюваного містить великий портфель токенів, але не нативний (рідний) актив Ethereum. Державно-приватні партнерства також можуть допомогти правоохоронним органам проводити подальші продажі або аукціони конфіскованих віртуальних активів через авторитетну та регульовану компанію (VASP).

Другий етап (ідентифікація). Ідентифікація віртуальних активів на етапі правозастосування – це уміння, яким повинен володіти кожен працівник у правоохоронній структурі, принаймні на базовому рівні. Крім цього, потрібно мати навички щодо виявлення апаратних і паперових гаманців, ресурсів відновлення доступу до віртуальних активів, а також методів, за допомогою яких ці предмети можна приховати. Компактні та невибагливі гаманці для холодного зберігання можна легко сплутати з канцелярським приладдям і не помітити під час обшуку. Працівники також мають бути обережними у поводженні з ідентифікованими предметами: оскільки вони можуть містити надзвичайно конфіденційну інформацію, таку як необроблені приватні ключі чи початкові коди відновлення (seed-фрази). Їх слід поміщати в непрозору упаковку, щоб запобігти випадковому захопленню камерами, що носять на тілі, або іншими записуючими пристроями під час проведення обшуку, а також фіксації іншими залученими до процесуальної дії особами.

Технічний персонал і ті, хто має досвід цифрової криміналістики, повинні бути готові проводити огляд техніки (ноутбуків, настільних комп'ютерів і мобільних пристроїв) на місці, намагаючись зібрати дані та ідентифікувати програми, що можуть вказувати на використання віртуальних активів або

нещодавню історію доступу до VASP. Більш повні та ретельні цифрові криміналістичні експертизи згодом повинні проводитися в судово-медичних установах.

Третій і четвертий етапи (вилучення та арешт). Щодо віртуальних активів, вилучення фізичного об'єкта (флеш-накопичувач, спеціалізований холодний гаманець) не завжди означає наявність повного контролю над віртуальними активами, що зберігаються на них. Щоб конфіскація була завершена успішно, правоохоронні органи повинні підписати транзакції та отримати власні приватні ключі від віртуальних активів.

Місце конфіскації становить найбільший ризик: помилки, такі як відправка активів за неправильною адресою або помилкова плата за газ, можуть бути незворотними. Щоб запобігти таким ризикам, процес конфіскації має здійснюватися через «систему запобіжників», коли двоє співробітників узгоджують кожен крок із заздалегідь визначеним контрольним списком, як зазначено в політиці вилучення.

Процес конфіскації має бути ретельно зафіксований як у письмовій формі, так і, якщо це можливо, з використанням аудіо- та відеозаписувальних пристроїв, на що можна посилатися пізніше або використовувати як докази. Такі записи стануть у нагоді під час обґрунтування конкретних рішень. Через їх надзвичайну чутливість, запис фраз відновлення або приватних ключів варто здійснювати з дотриманням правил подальшої конфіденційності та чіткого управлінням доступом до зафіксованого матеріалу.

Незважаючи на те, що наведені вище принципи можуть бути широко застосовані до різних засобів зберігання віртуальних активів, не всі вилучення однакові, і використовувані процеси можуть суттєво відрізнятися залежно від типу ідентифікованого віртуального активу чи засобу його зберігання. Наприклад, пошук закритого ключа на паперовому гаманці вимагатиме іншого підходу до відновлення гаманця з вихідних кодів відновлення. Хоча спеціально підготовлені засоби для вилучення не можуть охоплювати всі поточні та майбутні варіанти зберігання віртуальних активів, вони повинні чітко визначити процеси, за допомогою яких віртуальні активи не можуть бути вилучені на місці події через технічні труднощі, і які доступні варіанти збереження ідентифікованих активів мають правоохоронці натомість.

Будь-які активи, вилучені безпосередньо з пристроїв, таких як настільні комп'ютери, ноутбуки та мобільні телефони,

смартфони тощо, вимагають особливої обережності. Зважаючи на важливість збереження цифрових доказів, з ними має працювати лише персонал, навчений сортуванню цифрових пристроїв у реальному часі. Баланс між захистом віртуальних активів і збереженням доказів необхідно контролювати та керувати ним з обережністю. Правова основа цього процесу має вирішальне значення як для встановлення винних осіб, так і для їх успішного затримання та арешту.

П'ятий етап (зберігання). Зберігання віртуальних активів під час процесу збору доказової бази та розгляду кримінального провадження пов'язане з певними ризиками. Значна частина дискусій щодо зберігання віртуальних активів обмежується програмним і апаратним забезпеченням для зберігання активу. Як такий, він не відображає унікальних вимог правоохоронних і державних органів, де організаційний контроль доступу, можливості аудиту та відшкодування цих активів є пріоритетними. Незважаючи на судові вимоги щодо правил ланцюга постачання, програмне та апаратне забезпечення споживчого рівня для роботи віртуальними активами часто створюються з єдиною точкою доступу, що викликає додаткові ризики втрати, відмови та зловживання.

Використання VASP і спеціалізованих зберігачів – організацій, що забезпечують безпечне довгострокове зберігання криптовалют від імені установ – може зменшити ці ризики. Зокрема, зберігачі часто мають надійні положення щодо роботи з інституційними інвесторами, чиї вимоги до постачальника послуг подібні до вимог правоохоронних органів або державних інституцій.

«Не ваші ключі, не ваша віртуальні активи» – це аксіома у світі криптовалюти, і використання кастодіальних послуг означає відмову від певного контролю над активами. Однак правоохоронні органи зазвичай покладаються на безпечних третіх сторін: адже автотранспорт, вилучений поліцією, зазвичай, зберігається на спеціальних майданчиках, а готівка, вилучена у великих розмірах, – у банках і фінансових установах.

Вибір методу зберігання не слід робити легковажно, і один варіант не підходить для всіх ситуацій. Організації знайдуть різні рішення, що добре підходять для їх цілей і юридичних зобов'язань. Але ключовим є те, що рішення про те, як зберегти віртуальні активи, приймаються на основі інформації від широкого кола зацікавлених сторін і як частина організаційної політики.

Шостий етап (управління).

Останній етап управління активами тісно пов'язаний з обраними умовами на п'ятому етапі (зберігання активів). Як вже відомо, на минулому етапі найбільше суперечок точиться між програмним та апаратним зберіганням, а також кастодіальним управлінням активами, що здійснюється третіми особами.

Обираючи будь-який з варіантів особистого зберігання (некастодіального), правоохоронні органи стикнуться з проблемами подвійної сплати комісії (газу) за транзакції під час вилучення активу, а також його подальшого переказу на гаманці, підконтрольні організаціям, що будуть здійснювати управління активами від імені держави, що є небажаним.

У випадку кастодіального зберігання, коли активи відразу переходять в управління VASP, потреба для подальшого переміщення може і не виникнути, коли VASP одночасно уповноважений на управління активами після їх вилучення.

Підсумовуючи викладене, на сьогодні найскладніше питання під час розслідування злочинів, пов'язаних з віртуальними активами, у проблемі відсутності належного регулювання цього інституту. Отже, описані вище етапи є власним баченням спільноти та автора щодо бажаного стану справ у роботі з віртуальними активами в правоохоронній схемі.

Список використаних джерел

1. The recording of crypto assets in the System of National Accounts – Interim guidance. Working paper 3.3. 8 July 2020. 22 p.

2. Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. 9 p.

3. Кіберполіція України. ВікіпедіЯ – Вільна енциклопедія. URL: https://uk.wikipedia.org/wiki/Кіберполіція_України.

4. Бюджет втратив 3 млрд грн податків від діяльності криптобірж // Бюро економічної безпеки: державний сайт України. 02.08.2023. URL: https://esbu.gov.ua/news/biudzhet-vtratyv-3-mlrd-hrn-podatkiv-vid-diialnosti-kryptobirzh.

5. Жидко А. А. Дослідження блокчейн технологій для обробки і передачі інформації з використанням криптографічних методів шифрування даних. 80 с.

6. P. Luo, A. Yu-Lun Lin, Z. Wang, M. Karpovsky. Hardware Implementation of Secure Shamir's Secret Sharing Scheme (англ.) // HASE '14 Proceedings of the 2014 IEEE 15th International Symposium on High-Assurance Systems Engineering : Proceeding. Washington, DC, USA: IEEE Computer Society, 2014. P. 193–200. doi: 10.1109/HASE.2014.34.