МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ
КОНСУЛЬТАТИВНА МІСІЯ
ЄВРОПЕЙСЬКОГО СОЮЗУ В УКРАЇНІ

ДОСВІД КРАЇН ЄВРОПЕЙСЬКОГО СОЮЗУ ЩОДО ВИЯВЛЕННЯ ТА РОЗСЛІДУВАННЯ ВІДМИВАННЯ ЗЛОЧИННИХ ДОХОДІВ ІЗ ВИКОРИСТАННЯМ ЦИФРОВОЇ ВАЛЮТИ (КРИПТОВАЛЮТИ)

Методичні рекомендації

Київ 2017

УДК 343.98:061.1ЄС
ББК Х629.4
Д70

Авторський колектив:

Чернявський С. С., доктор юридичних наук, професор, заслужений діяч науки і техніки України (Національна академія внутрішніх справ);

Кржечковськис І., радник високого рівня ЄС з питань протидії відмиванню коштів;

Тацієнко В. В., кандидат юридичних наук (Департамент захисту економіки Національної поліції України);

Запотоцький А. П., кандидат юридичних наук (Національна академія внутрішніх справ);

Лагодзінська Ю. М., перекладач І категорії (Національна академія внутрішніх справ)

Рецензенти:

Чубенко А. Г., доктор юридичних наук, професор, директор навчально-методичного центру Державної служби фінансового моніторингу України;

Василинчук В. І., доктор юридичних наук, професор, заслужений юрист України, професор кафедри спеціальної техніки та оперативно-розшукового документування Національної академії внутрішніх справ;

Вязмікін С. А., перший заступник начальника Департаменту захисту економіки Національної поліції України

Рекомендовано до друку науково-методичною радою Національної академії внутрішніх справ від 25 січня 2017 року (протокол № 5)

Д70 **Досвід** країн Європейського Союзу щодо виявлення та розслідування відмивання злочинних доходів із використанням цифрової валюти (криптовалюти) [Текст] : метод. рек. / [С. С. Чернявський, І. Кржечковськис, В. В. Тацієнко та ін.]. – Київ : Нац. акад. внутр. справ, 2017. – 86 с.

Розглянуто особливості функціонування ринку цифрової валюти, з огляду на матеріали міжнародних правоохоронних організацій. Охарактеризовано схеми відмивання злочинних доходів з використанням відповідних фінансових інструментів, виокремлено напрями розслідування правопорушень у цій сфері з урахуванням досвіду країн ЄС.

Для слідчих, співробітників оперативних підрозділів, працівників прокуратури, суду, адвокатів, а також науковців, викладачів і студентів.

УДК 343.98:061.1ЄС
ББК Х629.4

MINISTRY OF INTERNAL AFFAIRS OF UKRAINE
NATIONAL ACADEMY OF INTERNAL AFFAIRS
EU ADVISORY MISSION TO UKRAINE

EU MEMBER STATES EXPERIENCE IN AREA OF DETECTION AND INVESTIGATION OF CRIME PROCEEDS LAUNDERING USING VIRTUAL CURRENCIES

RECOMMENDATIONS

Kyiv 2017

УДК 343.98:061.1ЄС
ББК Х629.4
Д70

Authoring team:

S. Cherniavskyi, LLD, professor, Meritous worker of science and technology of Ukraine (National Academy of Internal Affairs);

I. Krzeckovskis, EU High Level Adviser in the field of Anti-Money Laundering (AML);

V. Tatsienko, PhD in Law (NPU Economic Security Department);

A. Zapototskyi, PhD in Law (National Academy of Internal Affairs);

Y. Lahodzinska, interpreter (National Academy of Internal Affairs)

Reviewers:

A Chubenko, LLD, professor, Director of Training Center of State Service of Financial Monitoring of Ukraine;

V. Vasylynchuk, LLD, professor of Special Equipment and Operative Recording Branch, National Academy of Internal Affairs;

S. Viazimkin, First Deputy Head of NPU Economic Security Department

Recommended for publishing by NAIA Scientific Board of January 25th 2017 (protocol № 5)

Д70 **EU member states experience in area of detection and investigation of the laundering of crime proceeds using virtual currencies**: recommendations / [S. Cherniavskyi, I. Krzeckovskis, V. Tatsienko etc]. – Kyiv : NAIA, 2017. – 86 p.

Peculiarities of virtual currencies use and market functioning are analyzed (on the basis of international organizations' materials and statistics). Popular schemes of crime proceeds laundering are presented along with best European practices of virtual currency fraud prevention and combating.

For investigators, operatives, prosecution staff, legal assistants, judiciary, scientists, teaching staff and students.

УДК 343.98:061.1ЄС
ББК Х629.4

ЗМІСТ

CONTENTS

1. КОНЦЕПЦІЯ ЦИФРОВОЇ ВАЛЮТИ (КРИПТОВАЛЮТИ)

1.1. Історія розвитку цифрової валюти

Цифрова (електронна) валюта не є новим явищем у сфері фінансів. Лише за останні десять років цей сегмент надзвичайно швидко популяризувався у багатьох країнах світу. Історія розвитку цифрової валюти була ознаменована появою в 1996 р. E-gold – платіжного засобу для миттєвої передачі коштів на інші рахунки E-gold за допомогою відкриття відповідного особового рахунку в одиницях, еквівалентних вказаній кількості золота чи інших дорогоцінних металів. За даними звітів, у 2005 р. було зареєстровано 2,5 млн клієнтів, а сукупна вартість активів у обігу становила 6,3 млн доларів США. Однак у 2007 р. E-gold припинила своє існування після низки судових позовів за звинуваченнями у відмиванні грошей, створенні загрози національній безпеці та інтересам, а також участі в тіньових схемах. У 1998 р. було створено платіжну систему WebMoney, яка успішно функціонує на світовому ринку (у 2014 р. система обслуговувала 25 млн користувачів). Принцип роботи WebMoney полягає в наданні клієнтам можливості користуватися індивідуальним правом власності на ресурси (цінності), які зберігають відповідні особи – гаранти. Liberty Reserve проіснувала сім років (2006–2013). Ключовим принципом цієї системи була спрощена процедура реєстрації (потрібно було вказати лише ім'я, електронну адресу і дату народження). У 2013 р. Департамент юстиції США висунув компанії обвинувачення у відмиванні грошей та фінансових махінаціях, результатом яких стало виведення з легального обігу понад 6 млрд доларів США.

Біткоїн (Bitcoin) – це електронна валюта, презентована у 2008 р. Сатосі Накамото. Для неї характерна відсутність централізованого управління та емітентів. Попри те, що біткоїни наділені основними функціями та властивостями звичайних грошей, тобто є засобами обміну та розрахунковою одиницею, насамперед вони – це криптовалюта. Монети в цій системі

представлено у вигляді унікальних криптографічних (математичних) хеш-кодів, які не можна використати декілька разів. Така функція забезпечує запобігання можливості витрачання чужих грошей або використання власних двічі (хронологічна фіксація).

Мережа Bitcoin функціонує за принципом ланцюга блоків (block chain), який є публічним колективним реєстром. Усі підтверджені транзакції включені до цього ланцюга. На засадах цієї інформації біткоїн-гаманці можуть автоматично розрахувати залишок балансу і перевірити, чи витрачаються біткоїни їх власником у наступних транзакціях.

Як саме здійснюється транзакція у системі? Обмін криптовалютою між біткоїн-гаманцями відбувається шляхом підтвердження факту обміну через секретний ключ – конфіденційну інформацію. Він слугує своєрідним підписом, який фіксує транзакцію й унеможливлює внесення будь-яких змін до операції після передачі до мережі. Зазвичай упродовж 10 хвилин мережа ретранслює і підтверджує фінансову операцію через так званий майнінг. Майнінг – це розподілена система, яку використовують для підтвердження транзакцій, що мають статус очікування, шляхом їх включення до ланцюга блоків. Майнінг забезпечує дотримання хронологічного порядку, балансу і забезпечення використання уніфікованого підходу до функціонування системи. Пакування транзакцій у блоки із використанням криптографічного ключа забезпечує валідність підтверджених операцій. До того ж, майнінг створює аналог лотереї, яка унеможливлює просте додавання блоків до ланцюга іншими користувачами. Таким чином, жоден користувач не може контролювати ланцюг блоків (принцип рівноправності клієнтів) або замінити його частини іншими для скасування здійснених транзакцій.

1.2. Термінологія та класифікація

Відсутність чіткого визначення термінів є проблемою, яка потребує якомога швидшого розв’язання, адже використання уніфікованих дефініцій дає змогу уникнути неоднозначності та

хибних інтерпретацій. Під час розслідування злочинів, пов'язаних із використанням цифрової валюти, експерти можуть стикнутися з низкою синонімічних термінів різного ступеня поширеності – «електронна валюта», «цифрова валюта» і «криптовалюта». Також у наукових колах активно обговорюють доцільність використання дефініції «валюта» для визначення електронних розрахункових одиниць і можливість їх віднесення до категорії товару.

Ми використали визначення, офіційно закріплене в нормативно-правових актах FATF (Групи з розробки фінансових заходів боротьби з відмиванням грошей). Отже, «*Цифрова валюта* – електронний ціннісний еквівалент, який може бути об'єктом мережевої купівлі/продажу і використовується як (1) конвертаційний засіб (2) розрахункова одиниця; (3) засіб збереження вартості, але немає закріпленого законодавством статусу платіжного засобу в будь-якій юрисдикції». «Електронний ціннісний еквівалент» представлений лише у цифровому форматі; будь-який фізичний об'єкт (USB-накопичувач чи біткоїн) може вміщувати певний об'єм такої валюти, однак сама валюта функціонує лише в кіберпросторі за умови підключення до Інтернет-мережі.

Варто зауважити, що валютою є саме оцифровані дані, які представляють електронний ціннісний еквівалент, а не носій інформації, на якому вони зберігаються. Причому їх можна копіювати чи переміщувати на інші носії, але операції з цифровою валютою не матеріалізуються.

Цифрову (нефіатну) валюту необхідно відрізняти від національної («традиційної», «справжньої» чи «паперової»). Вона представлена у вигляді паперових банкнот і металевих грошей, має офіційно закріплений правовий статус, перебуває у вільному обігу та використовується як розрахунковий та конвертаційний засіб на території визначеної держави. Також не варто плутати концепт цифрової валюти з електронними грошима. За визначенням Групи з розробки фінансових заходів боротьби з відмиванням грошей (FATF) «цифрова валюта не є аналогом електронних грошей, які представляють цифровий

еквівалент паперових і використовуються для електронного переказу визначеної вартості. *Електронні гроші* – це механізм передачі вартості визначеної суми паперових грошей через відповідні платіжні системи; вартість паперових грошей, відображена в електронному еквіваленті, має аналогічний правовий статус». Водночас «цифрова валюта може представляти еквівалент електронних грошей або іншої цифрової валюти...» Більшість проблем виникає на етапі використання оцифрованого ціннісного еквівалента, адже електронні гроші та цифрова валюта мають певну специфіку. Так, процес конвертації паперових грошей у цифрову валюту більш ускладнений, ніж електронних грошей, які є «відформатованими» банкнотами.

Незалежно від формату та наявності правового статусу в межах конкретної юрисдикції передусім треба розглядати сам цифровий ціннісний еквівалент (наприклад, явище «подвійного витрачання», тобто можливість неодноразового здійснення транзакції з використанням однієї й тієї самої вартості, яке є одним із ключових викликів для правоохоронних структур).

Класифікація цифрових валют

FATF класифікує всі наявні види цифрових валют, використовуючи два основних підходи.

1. *Конвертованість/не конвертованість цифрової валюти (у паперовий формат).* Цей підхід полягає в розподілі цифрової валюти на «конвертовану/відкриту», що передбачає обмін на паперові гроші та на «неконвертовану/закриту», що не передбачає обмін на паперові гроші. «*Конвертована (відкрита) цифрова валюта* має відповідний паперовий ціннісний еквівалент і є об'єктом обміну на реальну валюту (Bitcoin, E-gold (не функціонує), Liberty Reserve (не функціонує), Second Life Linden Dollars, WebMoney). *Неконвертована (закрита) цифрова валюта* закріплюється за конкретним доменом чи віртуальним простором (наприклад, MMORPG – масові багатокористувацькі рольові онлайн-ігри або торговельні майданчики типу Amazon) і, згідно з правилами, що регулюють

її використання, не є об'єктом обміну на реальну валюту (Project Entropia Dollars, Q Coins, World of Warcraft Gold)». Хоча у звіті FATF зазначено, що неконвертована валюта функціонує винятково в цифровому середовищі, криміналітет відшукує можливості для забезпечення обміну неконвертованої цифрової валюти на паперові чи електронні гроші (чорний ринок валюти). З огляду на вищевказане, під час розслідування фінансових злочинів такий принцип категоризації може мати незначну практичну цінність, тому більш доцільно використовувати другий підхід.

2. *Централізовані системи/децентралізовані системи (наявність чи відсутність центрального адміністративного органу).* Такий підхід до категоризації цифрових валют передбачає наявність чи відсутність центрального адміністративного органу, завданням якого є фіксація та контроль за здійсненням транзакцій. Усі неконвертовані валюти є централізованими – адміністративний орган контролює їх обіг та унеможливлює конвертацію в межах визначених процедур. Конвертована цифрова валюта може бути як централізованою, так і децентралізованою. Обіг централізованої віртуальної валюти контролює центральний адміністративний орган (адміністратор) – третя сторона, яка наділена відповідними повноваженнями (випуск валюти, встановлення правил обігу та користування, забезпечення функціонування платіжної системи та вилучення з обігу). Валютний курс може бути мінливим (визначається співвідношенням попиту і пропозиції на ринку цифрової валюти) або фіксованим (його визначає адміністратор з урахуванням вартості будь-якого матеріального ціннісного еквівалента – паперових грошей, цінних металів чи валютної корзини). У контексті цієї категоризації третя сторона представлена фізичною чи юридичною особою, яка є учасником фінансової операції, однак не відіграє ключової ролі та є посередником між користувачами (нейтральна сторона).

«*Децентралізована цифрова валюта* – це розрахунковий засіб, що функціонує в межах розподілених піринговых систем, які не контролює централізований адміністративний орган (Bitcoin,

LiteCoin, Ripple)». У децентралізованих системах транзакції здійснюються через пірингові мережі. Інформація про перекази фіксується і верифікується в тій самій розподіленій мережі.

1.3. Відмінності традиційної та цифрової валюти

У чому полягають основні відмінності цифрової валюти від традиційних для нас паперових грошей (або фіатної валюти, як її визначають експерти)?

Ми вже згадували, що існують специфічні вторинні ринки обігу неконвертованих цифрових валют (наприклад, онлайн-аукціони), які можуть послуговуватись різноманітними джерелами фінансування, зокрема з конвертованою цифровою валютою. Необхідно детальніше розглянути особливості фінансування первинних торговельних операцій з використанням цифрової валюти та можливі способи її конвертації в паперові гроші, товари, послуги та інші ціннісні еквіваленти віртуальних валют.

Зазвичай конвертовану цифрову валюту можна придбати на спеціальних обмінних ресурсах за різним курсом. Ця процедура передбачає комбіновану систему зняття комісії у вигляді визначеної суми та відсоткової ставки за надані послуги. Додаткову ставку можуть стягувати за розміщення або/та зняття коштів з обмінного рахунку. Основними джерелами фінансування таких транзакцій і кінцевими об’єктами обміну можуть бути інші види цифрової валюти, системи грошових переказів, платіжні картки, готівка, PayPal тощо. Також наявні інші моделі, які передбачають застосування конвертації не стільки для забезпечення обігу валюти, скільки для здійснення її купівлі з використанням нетрадиційних способів (наприклад, придбання біткоїнів за допомогою SMS). З огляду на слабку врегульованість процесу надання таких послуг існує високий ризик ускладнення процесу ідентифікації джерела фінансування (готівкового чи наданого третьою стороною). Нещодавно декілька держав публічно оголосили про плани щодо законодавчого врегулювання посередництва на ринку цифрової

валюти з метою ефективної протидії та профілактики її застосування в злочинних схемах із відмивання грошей.

Банківські рахунки можна використовувати як джерела фінансування для придбання цифрової валюти або спосіб її прямої конвертації в паперові гроші. Їх визначають об'єктом законодавчого регулювання, що передбачає можливість ужиття, за необхідності, визначених законом заходів. Однак їх ефективність може бути мінімізована шляхом використання нестандартних схем монетизації злочинних доходів – наприклад, залучення так званих грошових мулів (осіб, які погоджуються виконати роль посередників і використати власні рахунки для переказу коштів, вилучених у жертви, на рахунок зловмисника). Варто зауважити, що щороку з'являються нові можливості для використання цифрових обмінних ресурсів з метою розміщення та/або передачі паперових грошей.

Махінації з готівкою завжди були популярними серед шахраїв, тому злочинні схеми, що передбачають пряму конвертацію цифрової валюти в готівковий еквівалент, становлять особливий інтерес для представників правоохоронних структур. Беззаперечним лідером на ринку цифрової валюти є біткоїн. Саме ця платіжна система пропонує користувачам унікальний спектр послуг. Так, на території деяких країн діють спеціальні біткоїн-банкомати, через які за готівку можна придбати чи продати певну кількість цифрової валюти.

За останнє десятиліття кількість виданих у світі платіжних карток (особливо дебетових та prepaid) зросла майже вдвічі. Prepaid-картки можна використати як альтернативу традиційних банківських продуктів та послуг (дебетові та кредитні картки, дорожні чеки тощо), а також для здійснення й отримання виплат від третіх осіб, міжнародних переказів тощо. Використання таких карток забезпечує високий рівень анонімності, що надає можливість зняття операційного/кредитного ліміту.

Статистика підтверджує, що найчастіше для відмивання доходів, отриманих у результаті учинення кіберзлочинів, злочинці використовують системи грошових переказів. Оскільки більшість таких систем функціонує за принципом

передання електронного еквівалента готівки, то їх зручно використовувати для забезпечення легалізації злочинних доходів. У такому разі фіксування історії переміщення «легальних» готівкових сум у фінансовій системі є зручним засобом приховування їх походження на етапі розміщення. Платіжні системи часто є лише інструментом для реалізації комплексних схем зі здійснення мінімум однієї готівкової операції та одного «грошового мула», а саме через:

– розсилку фальшивих рекрутингових об'яв (спаму), здійснення телефонних опитувань тощо з пропозицією заробити гроші «не виходячи з дому»;

– переказ коштів на рахунок «грошового мула», який зобов'язаний зняти готівкою переказану суму і надіслати її через електронну систему визначеному бенефіціару. За надання таких послуг «грошові мули» зазвичай отримують свій відсоток – «комісійні». Реалізація такого механізму можлива також за використання цифрової валюти, джерелом фінансування якої є готівка;

– системи грошових переказів (прямий трансфер готівки на ім'я отримувача).

Варто зазначити, що побічним ефектом популяризації біткоїнів є зростання кількості торговельних ресурсів і майданчиків, які приймають платежі в цифровій валюті. Ці платіжні засоби є актуальними з огляду на:

– незворотність транзакцій, адже після підтвердження операції з біткоїнами подвійне використання в мережі одного і того самого ціннісного еквівалента та інші шахрайські дії стають неможливими, на відміну від платіжних карток;

– плату за послуги з біткоїнами, яка є нижчою порівняно з аналогічною комісією за операції з платіжними картками.

1.4. Правове регулювання та міжнародний досвід

На сьогодні питання правового врегулювання операцій з цифровою валютою залишається актуальним. Зважаючи на відносну новизну цього явища та нестійкої динаміки його розвитку і функціонування як на міжнародному, так і на

національному рівні, досі не розроблено уніфікований стандарт – пакет нормативних актів. Однак неконструктивним є припущення стосовно того, що цифрова валюта функціонує в правовому «вакуумі», оскільки навіть за умови відсутності визначених правових норм існує певний узагальнений контекст, що визначає механізм обігу електронних грошей і цифрової валюти.

Бурхливий розвиток заходів у системі електронної торгівлі, вжитих на глобальному, регіональному і національному рівнях та спрямованих на посилення інноваційної складової й ефективності фінансових операцій, є позитивним явищем, оскільки вони постають основними інструментами, спроможними сприяти успішному її встановленню. Також необхідно враховувати деякі аспекти потенційного використання цифрових валют для відмивання грошей і вчинення кіберзлочинів, які досить часто є ланками одного ланцюга (у випадках незаконної діяльності з використанням цифрових валют).

Ураховуючи, що на цьому етапі немає уніфікованого визначення електронної торгівлі, його визначають як будь-який формат ділової угоди між фізичними та юридичними особами, які використовують технологію електронного зв’язку як еквівалент фізичного обміну товарами чи послугами. Вагомий вплив на становлення і розвиток механізмів електронної торгівлі мала пріоритезація Інтернету як комунікативного середовища для представників бізнесу (за статистикою, об’єми електронної торгівлі у 2014 р. становили приблизно 5 % від глобальних продажів).

У сфері електронної торгівлі основним документом є Типовий закон про електронну торгівлю від 16 грудня 1996 р., розроблений та ухвалений Комісією ООН з права міжнародної торгівлі (United Nations Commission on International Trade Law, UNCITRAL). Хоча цей акт не є міжнародним договором у традиційній інтерпретації міжнародного публічного права, його все одно активно використовують для розвитку національного законодавства в галузі електронної комерції. Він є міжнародним стандартом, який регулює електронну торгівлю. Секретаріат UNCITRAL веде реєстр країн, на території яких був прийнятий

та набув чинності закон про електронну торгівлю – нині цей перелік нараховує 54 держави.

Типовий закон UNCITRAL про електронну торгівлю визначає низку понять, які є ключовими для тлумачення стану поточної правової дискусії про статус цифрової валюти. Одним із таких понять є принцип **технологічного нейтралітету (медіанейтральності).** У контексті використання цифрової валюти він означає, що технології, застосовувані для здійснення операцій з такою валютою, можна використати як законно, так і для злочинної діяльності. Основну технологію не вважають протизаконною саму по собі лише за наявності потенційної можливості її незаконного використання. Так, прецедентне право підтримує концепцію технологічного нейтралітету і покладає відповідальність за протизаконне використання будь-якої технології на кінцевих користувачів.

Одним із найважливіших аспектів регулювання електронної торгівлі в контексті цифрових валют є **захист споживачів.** Ідеться про пакет норм, які захищають права споживачів (клієнтів) і визначають їхнє право на отримання товарів і послуг прийнятного стандарту, а також захищають їх від ризикових угод та операцій. Наприклад, у Директиві ЄС про електронну торгівлю чітко визначено високий рівень захисту прав споживачів як основний фактор, що сприяє безперешкодному руху послуг інформаційної спільноти. Оскільки наразі чимало актуальних питань пов'язано з захистом прав споживачів, то очевидно деякі з особливостей криптовалют – незворотність операцій з біткоїнами – можуть стати предметом окремої дискусії. Активне зближення сфер протидії кіберзлочинності та захисту даних сприяло виходу на передній план організацій з захисту прав споживачів як партнера та цінного джерела інформації про виявлені кіберзлочини.

Водночас різні нормативно-правові акти, що регулюють здійснення електронних платежів, є менш важливими в контексті саме цифрової валюти. Як міжнародні, так і регіональні документи відповідають такому принципу: електронні платежі здійснюють за допомогою встановлених фінансових механізмів через традиційні фінансові установи, що використовують фіатні

гроші. Проте на практиці цифрові валюти (централізовані чи децентралізовані) перебувають в обігу за межами цих установ і механізмів за винятком випадків конвертації цифрової валюти у фіатну і навпаки. Саме тому відмінності в механізмах здійснення транзакцій (серед іншого – застосування регулятивних норм) не мають суттєвого значення для правового аналізу і практичного використання цифрової валюти.

Відмивання грошей – це процес, спрямований на приховування зловмисниками джерел походження власності, контролю за доходами від злочинної діяльності та демонстрації їх «законності». На сьогодні є потужна база міжнародних інструментів та стандартів у сфері боротьби з відмиванням грошей. Насамперед треба згадати Конвенцію ООН про боротьбу з незаконним обігом наркотичних засобів і психотропних речовин від 20 грудня 1988 р., яка стала першим міжнародно-правовим документом, де було визначено елементи складу злочину з відмивання доходів, отриманих у результаті вчинення перерахованих у Конвенції злочинних діянь. Аналогічний підхід відображено у Конвенції ООН проти транснаціональної організованої злочинності від 15 листопада 2000 р. та Конвенції ООН проти корупції від 31 жовтня 2003 р., положення яких визначили подальший розвиток поняття відмивання злочинних доходів і конкретні вимоги та процедури боротьби з цим явищем. Міжнародна конвенція ООН про боротьбу з фінансуванням тероризму передбачає більш структурований підхід, встановлюючи спеціальні механізми з відслідковування, ідентифікації та арешту засобів і доходів, отриманих у результаті злочинної діяльності, пов’язаної з фінансуванням тероризму.

Для повноцінного огляду сучасних інструментів боротьби з відмиванням грошей необхідно згадати про FATF – міжурядовий орган, створений для розроблення стандартів і сприяння вжиттю правових, нормативних і оперативних заходів у межах протидії відмиванню грошей, фінансуванню тероризму та іншим загрозам цілісності міжнародної фінансової системи. Рекомендації FATF власне є зведенням обов’язкових вимог, дотримання контролюється FATF.

З урахуванням природи децентралізованих цифрових валют, ризик їх використання як засобу для координації кримінальних грошових потоків у Інтернеті є досить високим. Проте необхідно усвідомлювати, що актуальні з позицій відмивання грошей аспекти цифрових валют пов'язані не стільки із самою технологією (яка заслуговує на увагу з огляду на підвищену конфіденційність, складність відслідковування та наявність криптографічного захисту), скільки з відсутністю належного регулювання і контролю з боку компетентних органів за операціями з використанням цифрових валют.

Цифрові валюти можна використовувати як засіб учинення низки кримінальних правопорушень, а не лише для відмивання коштів. Вище зазначалося, що цифрові валюти постають об'єктом певних регулятивних норм, порушення яких в окремих випадках є підставою для встановлення кримінальної відповідальності. Наприклад, володіння цифровою валютою чи її використання в деяких країнах саме по собі визначають як кримінальне правопорушення, тобто «незаконне володіння неліцензованою валютою» чи «здійснення обміну неліцензованої валюти». Цифрову валюту також визначають як об'єкт злочину – у випадку її незаконного привласнення чи придбання в результаті шахрайських дій. Елементом складу злочину може бути також конвертація цифрової валюти в реальну.

До того ж, цифрова валюта може бути частиною *modus operandi* окремого злочину. Наприклад, у разі її використання для придбання заборонених товарів (зброї, наркотиків чи порнографічних матеріалів за участю неповнолітніх), а також для оплати послуг, надання яких є об'єктом посиленого регулювання чи криміналізації на території визначених держав (азартні ігри) цифрова валюта є *засобом* учинення злочину. Цифрова валюта також може бути представлена чи отримана з метою використання її в повному обсязі чи частково для: учинення злочинів, визначених універсальними міжнародно-правовими документами, які регулюють протидію фінансуванню тероризму; навмисного нанесення смертельних або тяжких поранень цивільним та іншим особам, які не беруть участь у воєнних діях під час збройного конфлікту; залякування

населення та застосування примусу до уряду чи міжнародної організації з конкретною вимогою (тероризм).

Кримінальним правопорушенням є використання цифрової валюти для конверсії та передачі майна (якщо відомо, що таке майно представлене злочинними доходами) з метою приховування джерела походження цих доходів, сприяння уникненню кримінальної відповідальності особою, причетною до вчинення вказаного злочину, або приховування будь-яких даних про істинне походження, розташування, спосіб розпорядження, переміщення та прав (охоплюючи право власності) на майно.

Зважаючи на електронну природу цифрових валют, майже всі типи злочинів можна охарактеризувати як кіберзлочини. Термін «кіберзлочинність» не має уніфікованого визначення, тому його доцільно розглядати як комплекс дій. Зазвичай кіберзлочинність інтерпретують як злочин проти комп'ютерних даних і систем (конфіденційності, цілісності та доступності даних і систем), злочини з їх використанням та злочини, пов'язані з контентом (комп'ютерне шахрайство, порушення авторських прав, розсилка і контроль за розсилкою спаму). В останньому випадку «традиційні» злочини (наприклад, підробка, виготовлення, поширення чи зберігання дитячої порнографії) кваліфікують за іншим принципом з відповідним ступенем тяжкості, якщо їх учиняють з використанням комп'ютерних систем (технології полегшують учинення та/або приховування таких злочинів та використовуються для оптимізації процесу розповсюдження негативних ефектів таких діянь).

Упродовж останнього десятиліття можна спостерігати позитивну динаміку імплементації в національне законодавство міжнародних інструментів у сфері боротьби з кіберзлочинністю, представлених як юридично зобов'язуючими, так і юридично не зобов'язуючими актами. Генеза, правовий статус, географія, предмет і механізми, визначені цими документами, є абсолютно різними (наприклад, Конвенція Ради Європи про кіберзлочинність, Угода про співробітництво держав-учасниць СНД у боротьбі зі злочинами у сфері комп'ютерної інформації, Угода між урядами держав-учасниць Шанхайської організації

співробітництва про взаємодію у сфері забезпечення міжнародної інформаційної безпеки, Конвенція про злочини в галузі інформаційних технологій Ліги арабських держав).

Варто зауважити, що «основні» кіберзлочини (несанкціонований доступ до комп'ютерної системи) можуть бути вторинними відносно таких злочинів, як крадіжка цифрової валюти. Наприклад, хакерське проникнення в особистий гаманець з метою незаконного привласнення біткоїнів може бути кваліфіковане як крадіжка, причому кіберзлочин матиме статус вторинного (учиненого з метою фасилітації основного). Злочини з неправомірним доступом також можуть мати пряме відношення до відмивання грошей через використання цифрових валют. Прикладом такого може бути ситуація, коли рахунки третіх осіб використовують для здійснення операцій без отриманої від них згоди.

Інші види кіберзлочинів, зокрема комп'ютерне шахрайство, можуть мати статус основних. У такому разі цифрова валюта буде об'єктом учинення злочину (особливо одержана шляхом обману). Злочини, пов'язані з даними контенту, та інші форми кіберзлочинності (забезпечення зберігання чи поширення матеріалів жорстокого поводження з дітьми з використанням комп'ютера чи продаж наркотиків онлайн) можуть бути або предикатними відносно відмивання грошей із використанням цифрових валют (якщо ці матеріали були продані), або бути основним злочином із використанням валюти як засобу (якщо матеріали були придбані). Також варто згадати про характеристики злочинних діянь, які зазвичай кваліфікують як кіберзлочини. З правової точки зору вони є аналогічними щодо злочинів, учинених з використанням цифрової валюти. Кіберзлочинність має яскраво виражений транснаціональний характер і об'єднує декілька юрисдикцій, що значно ускладнює проведення розслідувань у межах надання взаємної правової допомоги. Також незаконне використання, перехоплення або втручання в комп'ютерні системи чи дані часто майже неможливо відстежити, оскільки однією з головних проблем залишається своєчасне інформування компетентних органів про такі випадки. До того ж, кіберзлочини залишають

специфічні сліди, які є електронними доказами. Аналіз цих доказів є надзвичайно складною процедурою в правовому та технічному контексті.

На відміну від міжнародного контексту, питання щодо регулювання використання віртуальних валют декілька держав вирішили в межах чинного законодавства про процедуру надання звітності, реєстрації, оподаткування та можливих зловживань з метою відмивання грошей. Водночас тестування різних підходів до регулювання цифрової валюти в умовах очікуваного зростання кількості операцій, а також визнання досягнень у галузі розвитку технологій засвідчує потенціал розвитку відповідної правової бази.

З огляду на зростання популярності електронної торгівлі, **Сполучені Штати Америки** є активним учасником дискусії про цифрові валюти. Американські політики та регулятивні органи використовують підхід, який полягає в усуненні заборони на використання такої валюти за умови застосування встановлених правил до конкретних гравців ринку електронних фінансових послуг. На засадах цього підходу в березні 2013 р. Комісія з боротьби з фінансовими злочинами (FinCEN) опублікувала інструкцію FIN-2013-G00199 з роз'ясненнями щодо застосування законодавства США до визначених категорій провайдерів електронних фінансових послуг із використанням цифрової валюти (пункти обміну, адміністратори тощо), які зобов'язані відтепер дотримуватися вимог щодо реєстрації, зберігання документів тощо (як і всі інші провайдери фінансових послуг). Ця інструкція чітко розмежовує користувачів цифрової валюти (за винятком провайдерів фінансових послуг) та адміністраторів і пункти обміну, що мають провайдери фінансових послуг (надання послуг з «переміщення грошей»). Окрім того, Служба внутрішніх доходів США (IRS) опублікувала Інструкцію 2014-21100, де подано відповіді на запитання щодо статусу цифрової валюти в США з точки зору оподаткування.

Велика Британія застосувала аналогічний підхід до регулювання ринку цифрових валют, затвердивши Податковий та митний бюлетень 09/14 «Податковий режим діяльності з

використанням біткоїнів та іншими криптовалютами». У тексті цього документа визнають потужну динаміку розвитку ринку послуг, наданих із використанням децентралізованих цифрових валют. Також у бюлетені біткоїни визначають не повноцінною валютою, а платіжним засобом, до якого застосовують механізми індивідуального (ПДВ, сума якого залежить від категорії користувачів) та корпоративного оподаткування (податок на доходи і приріст капіталу, отриманого від операцій з біткоїнами).

У **Китаї** віддають перевагу введенню заборони на використання біткоїнів та інших криптовалют державними фінансовими установами. У грудні 2013 р. Народний банк Китаю та п'ять міністерств опублікували циркуляр «Попередження ризиків, пов'язаних з використанням біткоїнів», де чітко визначено, що біткоїни не є еквівалентом грошей і не можуть бути використані як законний платіжний засіб та об'єкт конвертації, виплати іпотечного кредиту, інвестиційні та страхові платежі тощо. Водночас заборона не є абсолютною, адже цифрову валюту можна використовувати в Інтернет-мережі як товар на власний страх і ризик. Однак сайти, які надають можливість здійснення торгових операцій з використанням біткоїнів, відповідно до закону про боротьбу з відмиванням грошей підлягають реєстрації регулятивними органами з питань контролю за наданням телекомунікаційних послуг.

Підхід уряду **Канади** до цього питання також є виваженим – біткоїни не мають статусу законного платіжного засобу на території держави, проте на відміну від Китаю, в Канаді залишається відкритою можливість перегляду цього питання в майбутньому залежно від розвитку подій. Було враховано такі фактори, як фінансова стабільність, високий ризик, зручність і простота використання, вартість, безпека і зручні механізми компенсації.

Інший підхід було застосовано в **Сингапурі.** Влада не накладає обмежень на використання цифрової валюти як платіжного засобу в межах національної фінансової системи, але встановлює досить жорсткі вимоги щодо функціонування пунктів обміну та автоматів з продажу біткоїнів з метою

забезпечення обов’язкової ідентифікації особи клієнта та прозорості операцій з біткоїнами.

2. РИНОК ЦИФРОВОЇ ВАЛЮТИ: СУЧАСНІ ВИКЛИКИ І ЗАГРОЗИ

2.1. Цифрова валюта в злочинних схемах

У сучасних умовах цифрова валюта може стати зручним засобом для зловмисників, які використовують типові схеми з відмивання коштів. Одним з ключових факторів для злочинців є швидкість електронних транзакцій та їх незворотність.

Для сучасних платіжних систем характерна надзвичайно висока швидкість, тобто будь-яку суму можна зняти з одного рахунку і поповнити інший за лічені хвилини. У контексті розслідування фінансових злочинів технологізація банківських операцій і популяризація електронних платіжних систем є істотним фактором ризику, який призвів до ускладнення процедури моніторингу та накладення арешту (особливо в разі використання цифрової валюти).

Незворотність є відносною характеристикою – все залежить від конкретної платіжної системи і типу електронної валюти. Так, після підтвердження транзакції біткоїнів внесення будь-яких змін є неможливим, оскільки система – децентралізована. Єдиним варіантом постає переведення еквівалентної суми отримувачем на рахунок відправника. Централізовані системи відрізняються наявністю адміністратора – контролюючого елемента. Більшість операцій із цифровою валютою в таких системах також здійснюють за принципом невідворотності, однак адміністратор може прийняти рішення про відміну транзакції в разі потреби.

На цей час існує три найпоширеніших види транзакцій:

– конвертація паперової валюти в цифрову і в зворотному напрямі;

– конвертація різних видів цифрових валют;

– переказ цифрової валюти на рахунок (електронний гаманець).

Паперову валюту конвертують у цифрову двома способами: придбання чи продаж цифрової валюти у адміністраторів (доступно для централізованих систем; формат є близьким до депозитного вкладу) або шляхом обміну цифрової валюти за встановленим курсом (деякі централізовані та всі децентралізовані системи). Процес конвертації в такому разі

може бути забезпечено через ресурси банківських рахунків і вкладів, системи грошових переказів, платіжні картки, готівкові розрахунки та електронні платіжні системи, зокрема PayPal.

Конвертацію (купівля/продаж) різних видів цифрових валют, де як операційний ресурс не використовують паперові гроші, здійснюють на базі обмінного курсу. Причому часу на стандартну транзакцію витрачають в середньому більше, ніж на аналогічну операцію з використанням паперових грошей. Такі заходи мають профілактичний характер і застосовуються переважно до «новачків» (новостворені рахунки).

Коли йдеться про переказ цифрової валюти на рахунок (електронний гаманець), потрібно зважати на те, яку саме валюту використовують. Більшість операцій підтверджується за лічені секунди, а час затримки зазвичай не перевищує декількох хвилин. Транзакції цифрової валюти в децентралізованих системах (біткоїни) після отримання статусу підтвердження є незворотними. Цей аспект є позитивним з позицій пересічного користувача, який може бути впевнений у тому, що кошти не стануть об'єктом реверсної транзакції після втручання шахраїв. Однак для зловмисників це також досить вигідно – відсутність клірингового циклу (отримання, звірка і поточне оновлення інформації за проведеними розрахунками) та інших інструментів для запуску механізму повернення коштів можуть бути використані ними для замітання слідів злочинної діяльності. Правопорушники також використовують принцип анонімності, який забезпечує більшість децентралізованих електронних систем (будь-яке ускладнення процесу ідентифікації завжди є суттєвим фактором ризику).

2.2. Фактори, що впливають на ефективність розслідування

Слабка теоретична підготовка кадрів правоохоронних органів

Рівень поінформованості слідчих та прокурорів про функціональні особливості та специфіку використання цифрової валюти є вкрай низьким. З огляду на це, проведення фінансового розслідування буде гальмуватися та потребуватиме залучення спеціалістів, що призведе до додаткових витрат і

бюрократії. Однак фахівців із досвідом, спроможних надати консультації та технічну підтримку правоохоронним органам, не так багато. Вирішенням цієї проблеми потребує реалізації проектів (міжнародних і національних) інформаційно-роз'яснювального та навчального (спеціальні курси, семінари, тренінги для тренерів, навчальні програми у вищих навчальних закладах) характеру, спрямованих на ознайомлення з означеною тематикою студентів, слухачів, а також досвідчених практиків, які бажають підвищити власну кваліфікацію.

Пріоритезація електронних доказів

Цифрова валюта є нематеріальним об'єктом і функціонує лише у віртуальному світі, який безперервно насичується інформацією. Успішність будь-якої електронної транзакції залежить лише від наявності у користувача комп'ютерної техніки та виходу до Інтернет-мережі. Це забезпечує відсутність жодних «паперових» слідів (за винятком операцій, що передбачають конвертацію цифрової валюти в паперову і навпаки), які можна було б використати як докази. Саме тому під час розслідування махінацій з цифровою валютою правоохоронні органи та фінансова розвідка переважно можуть розраховувати лише на електронний документ як доказ.

Електронний доказ – це інформація, що генерується, зберігається чи передається у віртуальному просторі з одного електронного пристрою на інший і може бути використана як доказ у суді. На відміну від традиційних видів (документи, фотографії, зафіксовані на матеріальних носіях свідчення), електронні докази фіксують у віртуальному просторі. Також вони можуть бути відображені матеріально за допомогою різноманітних приладів – комп'ютерів, засобів мобільного зв'язку, цифрових фото- та відеокамер, зовнішніх накопичувачів, мережевих сервісів зберігання даних тощо. До електронних доказів висувають стандартні вимоги, серед яких автентичність, допустимість та релевантність. Однак електронні докази мають специфічні риси, які варто брати до уваги під час розслідування фінансових злочинів із використанням цифрової валюти:

– труднощі в процесі відслідковування та ускладнений оперативний контроль;

– необхідність залучення спеціалістів;

– нестабільність електронних систем (високий ризик втручання шляхом форматування та знищення інформації);

– системні модифікації;

– необмежене копіювання інформації.

Таким чином, ефективність розслідування таких злочинів буде залежати від наявних у працівників спеціалізованих органів технічних можливостей та практичного досвіду для якісного збору і аналізу електронних доказів.

Законодавчі недоліки

Коли йдеться про законодавче регулювання, то основним питанням є те, наскільки доступним та функціональним постає на практиці сам концепт цифрової валюти в межах національної правової системи. Ідеальний сценарій передбачає гарантію визнання та використання в кримінальному провадженні електронних доказів, закріплену у відповідних положеннях кримінального законодавства. Однак зазвичай юристи і слідчі повинні «переформатовувати» зібрані матеріали у «документи» чи «інформацію» для визнання їх судом допустимими та обґрунтованими. Окрім того, до електронних доказів застосовують аналогічні стандарти та процедури.

Також можливий варіант визнання електронного доказу ненадійним джерелом даних. У міжнародно-правових актах, які визначають статус електронних доказів, зафіксовано вимоги щодо застосування цифрового підпису з метою забезпечення рівної юридичної сили електронних і паперових документів як доказів у кримінальному провадженні, що може призвести до певних труднощів у визнанні судом допустимості електронних доказів.

Концепт електронного доказу є базовим у розслідуваннях фінансових злочинів із використанням цифрової валюти. Деякі матеріали об’єктивно не можуть бути представлені для ознайомлення, якщо, наприклад, їх опрацьовує і використовує фінансова чи кримінальна розвідка. Якщо ці матеріали мають електронний формат, то сторона захисту має можливість оскаржити допустимість таких доказів під час розгляду справи.

Не варто забувати, що електронні докази (як і матеріальні) не повинні бути об’єктом будь-яких зовнішніх втручань (змін, виправлень, скорочень тощо), які можуть суттєво вплинути на їх форму та зміст. Цифровий формат передбачає високу ймовірність втручання зловмисників, тобто можливість

здійснення різних видів маніпуляцій з цими матеріалами. Правоохоронні органи повинні забезпечувати цілісність електронних документів з метою збереження наявної інформації та їхню відповідність офіційним вимогам для подальшого використання як доказів.

Контроль за діяльністю фінансових установ

Вимоги щодо регулювання діяльності фінансових установ з метою ефективної протидії відмиванню коштів чітко визначено в рекомендаціях FATF: «Інші фінансові установи повинні пройти процедуру ліцензування та реєстрації. Їхню діяльність контролюють компетентні органи/служби задля виявлення потенційних ризиків участі в злочинних схемах з відмивання грошей чи фінансування тероризму. Обов'язковій реєстрації та ліцензуванню у визначеному міжнародними стандартами порядку підлягають установи, які надають мінімальний пакет фінансових послуг, охоплюючи здійснення грошових переказів та/або обмін валют».

З огляду на визначення, яке надає FATF, статус фінансових установ автоматично отримують і централізовані системи обігу цифрової валюти. Окреслити статус децентралізованих систем за цим визначенням складніше, адже вони не є фінансовими установами, які здійснюють переказ коштів чи валютний обмін. Проте система здійснює переказ ціннісного еквівалента на основі показників цифрового валютного курсу (на прикладі біткоїнів). Суттєвою перешкодою на шляху до контролю діяльності таких систем також є відсутність центрального адміністративного елемента, який міг би виступати суб'єктом кримінального провадження.

Притягнення до кримінальної відповідальності та винесення вироку судом

Процедура притягнення до кримінальної відповідальності осіб, звинувачених у вчиненні фінансових злочинів із використанням цифрової валюти, не має визначеної специфіки. Так, чинне законодавство держав-членів ГУАМ (Грузія, Україна, Азербайджан та Молдова) наділяє прокурора повноваженнями, які передбачають контроль за проведенням кримінальних розслідувань. Практично на всіх етапах провадження в межах визначених законом процедур з перерахованими викликами будуть стикатися як слідчий, так і прокурор. Водночас особливі

повноваження прокуратури, визначені національним законодавством, сторона обвинувачення може використати на етапі опрацювання доказової бази.

Законодавство закріплює за прокуратурою право діяти на власний розсуд (концепт дискреційної влади) під час розслідування кримінальних справ. Дискреційний підхід у цьому разі передбачає застосування стандартів в інтересах суспільства з метою прийняття відповідного рішення (ініціація/продовження судового розгляду або альтернативне рішення). Механізм прийняття альтернативних рішень активізується після перекваліфікації злочинів у бік «пом'якшення». Так, визнане кіберзлочином протиправне діяння передбачатиме інші види покарання або закриття провадження в справі. Уникнути таких наслідків можна, якщо правоохоронні органи нададуть переконливі докази участі обвинувачених у злочинних схемах із відмивання коштів.

У багатьох країнах поширеною є практика укладання між прокурором та обвинуваченим угоди про визнання вини, яка має як очевидні недоліки, так і позитивні аспекти. З одного боку, прокурор може застосувати вищезгаданий дискреційний підхід та гарантувати обвинуваченому перекваліфікацію вчиненого ним діяння після надання згоди на добровільну співпрацю з правоохоронними органами (можливість здійснення спрощеного кримінального провадження, менший термін ув'язнення, уникнення обов'язкового вилучення доходів у разі доведення причетності до відмивання грошей), а з іншого – таку угоду правоохоронні органи можуть використати як ефективний інструмент для отримання інформації у справі (не витрачається зайвий час та ресурси для поповнення доказової бази).

Підвищити результативність розслідування можна за допомогою використання повноважень прокуратури щодо організації створення слідчих груп, до складу яких зазвичай належать слідчі й експерти різного профілю. Поєднання досвіду правоохоронців та експертів з розслідування фінансової та кіберзлочинності цілком виправдовує затрачений час і ресурси. Компіляція різних методик і технік збору та опрацювання доказів, а також практичний досвід професіоналів забезпечує найкращі результати. Також не варто забувати і про вдосконалення

професійної компетенції суддів, яких залучають до розгляду справ про шахрайство з цифровою валютою та кіберзлочини.

Співпраця на національному рівні

Ефективність розкриття будь-якого інформаційного злочину залежить від того, наскільки узгодженими є дії всіх учасників процесу – від збору даних кримінальною розвідкою до розгляду справи в суді. Співпраця на державному рівні є різновидом нетворкінгу, основним завданням якого постає розширення кола партнерів з різними функціями та компетенцією, залучених до розслідування фінансового злочину, із забезпеченням високого рівня результативності на всіх етапах (фіксація злочину, слідчі дії, експертизи та застосування обмежувальних заходів, компенсація збитків та профілактична діяльність).

Яких саме партнерів передусім варто залучати? Під час виявлення та розслідування злочинів із використанням цифрової валюти суттєву підтримку правоохоронним структурам можуть надати служби фінансової розвідки (СФР) – спеціалізовані державні наглядові органи, які здійснюють збір та аналіз звітної документації від фінансових установ і фізичних (юридичних) осіб з метою подальшого направлення до місцевих правоохоронних структур та закордонні СФР у межах протидії відмиванню коштів. Ці служби є неоціненними джерелами інформації щодо специфіки фінансових злочинів, статистичних даних і наявного практичного досвіду. СФР потребують підтримання постійного зв'язку зі спеціалізованими відділами з боротьби з кіберзлочинністю (ІТ-підрозділи) для надання фахівцями своєчасної експертної оцінки і технічного консультування.

Ще одна партнерська ланка – це ІТ-підрозділи і служби фінансових розслідувань. Розслідування фінансових і кримінальних злочинів у багатьох державах здійснюють спеціалісти структурно відокремлених інституцій. Вони застосовують різні методи та підходи. Оскільки розслідування фінансових злочинів потребує від слідчих специфічних навичок роботи з інформаційними системами і аналітичними інструментами (опрацювання даних, переданих службою розвідки), а також досвіду роботи з електронними доказами (справи про шахрайство, ухиляння від сплати податків, ведення

«чорної бухгалтерії»), то повинна бути налагоджена тісна співпраця з IT-фахівцями.

Активно формуються партнерські зв'язки між IT-підрозділами та національними Групами швидкого реагування на інциденти, пов'язані з комп'ютерною безпекою (CSIRT). CSIRT – це групи, до яких належать експерти, завданням яких є забезпечення захисту ключових об'єктів національної інформаційної інфраструктури шляхом вжиття профілактичних заходів із використанням різних методик та інструментів, ситуативне втручання в разі виникнення інцидентів, що загрожують безпеці національного кіберпростору, а також нейтралізація негативних наслідків. CSIRT здійснюють обробку величезних обсягів інформації, отриманої від державних органів нагляду і контролю та міжнародних баз даних (наприклад, Shadowserver або Arbor Networks): дані про загрозу кібербезпеці та потенційні ризики. У контексті розслідування фінансових злочинів із використанням цифрової валюти експертів CSIRT можна залучати з метою консультування щодо специфіки загроз та їхніх наслідків, які використовують хакери, їхніх «портфоліо» і «слабких місць» інформаційних систем.

Корисною може бути співпраця з приватними підприємствами та організаціями. Провайдери Інтернет-послуг, які є первинним джерелом даних про мережевих користувачів, потоки інформаційного обміну та іншої важливої інформації, часто відсутні в «партнерських списків» з різних причин правового (законодавча неврегульованість питань про конфіденційність особистих даних, фіксацію та порядок зберігання даних) і суто практичного (відсутність чітко прописаних механізмів співпраці у двосторонніх договорах/меморандумах, затримки з фінансуванням придбання спеціального обладнання тощо) характеру. Аналогічні перешкоди унеможливлюють налагодження інформаційного обміну правоохоронних органів з такими важливими інформаційними джерелами як фінансові установи, що фіксують дані про переміщення грошових потоків і служби захисту прав

споживачів, які можуть надати матеріали для поповнення доказової бази у справах про шахрайство та відмивання грошей.

Співпраця на міжнародному рівні

Будь-який інформаційний злочин (від махінацій з цифровою валютою до різних видів кіберзлочинів) має транснаціональну природу. Тому ефективність розслідувань, які на початковому етапі можуть не виходити за межі національної юрисдикції, рано чи пізно буде визначатися рівнем злагодженості співпраці між відповідними службами і структурами різних держав.

Однак досить непросто досягти оптимального рівня злагодженості. Так, під час розслідування злочинів із використанням цифрової валюти будь-які розбіжності в інтерпретації національним законодавством самого визначення цього концепту, його статусу чи навіть питання визнання державою такої валюти як функціональної розрахункової одиниці може стати серйозною проблемою. Незалежно від того, чи наявний у правоохоронних органів окремої держави правовий інструментарій для відкриття кримінальних проваджень за обвинуваченнями у відмиванні грошей, шахрайстві та інших фінансових злочинах у межах національної юрисдикції, вихід на міжнародний рівень все одно потребуватиме звернення до міжнародно-правових документів (конвенцій, угод), які відрізняються набагато вищим рівнем формалізації процедур і механізмів розподілу повноважень.

Таким чином, залучення інших держав до розслідування учиненого злочину вимагатиме застосування механізму Mutual Legal Assistance (MLA) – взаємної правової допомоги, що реалізується через підписання дво- чи багатосторонніх угод між урядами держав. Такий варіант правової регламентації співробітництва на практиці є тривалою і досить забюрократизованою процедурою, що може ускладнити або унеможливити своєчасне та повне розслідування злочинів, у межах якого опрацьовуються та аналізуються електронні докази. Існує ще один варіант налагодження прямої співпраці між правоохоронними структурами різних держав «в обхід» вищезазначених бюрократичних процедур у межах MLA – контактні пункти Інтерполу, мережа національних

IT-підрозділів G8 (розслідування кіберзлочинів) і взаємодія національних служб фінансової розвідки (розслідування відмивання грошей).

Міжнародну співпрацю також можна здійснювати через державно-приватне партнерство, значення якого в цьому контексті досить часто недооцінюють. Йдеться про суб'єктів міжнародного права – іноземні компанії, які можуть надати матеріали для використання їх як доказів (інформація з соціальних мереж, мейл-серверів, дані про діяльність дочірніх підприємств, які контролюють іноземні материнські компанії). Існує високий ризик виникнення правових колізій, пов'язаних з питаннями національної юрисдикції. Наприклад, материнська компанія, зареєстрована на території іншої держави, має законні підстави відмовити у доступі до запитуваної інформації щодо діяльності дочірнього підприємства згідно з чинним національним законодавством, якщо ця інформація зберігається та опрацьовується на території іншої держави.

2.3. Останні тенденції ринку цифрової валюти

Ринок криптовалют перебуває в постійному та динамічному розвитку. З моменту представлення широкому загалу в 2009 р. біткоїнів кількість цифрових розрахункових засобів лише зростає (табл.).

Таблиця

Рік	Загальна кількість криптовалют на ринку	Криптовалюта
2009	1	Bitcoin
2010	1	Bitcoin
2011	3	Bitcoin, Litecoin, Namecoin
2012	4	Bitcoin, Litecoin, Namecoin, Peercoin
2013	8	Bitcoin, Litecoin, Namecoin, Peercoin, Ripple, Dogecoin, Mastercoin, Primecoin
2014	12	Bitcoin, Litecoin, Namecoin, Peercoin, Ripple, Dogecoin, Mastercoin, Primecoin,

		Auroracoin, Vertcoin, MazaCoin, Coinye

Динаміка криптовалютного ринку має специфічні риси:

– спостерігається глобальна тенденція тяжіння до децентралізованої моделі;

– попри фактичну відсутність конкуренції на ринку централізованих цифрових платіжно-обмінних систем, ключових гравців (Second Life Linden Dollars, World of Warcraft Gold, Project Entropia Dollars), можуть у недалекому майбутньому витіснити більш успішні проекти;

– компанія Amazon.com нещодавно презентувала власну криптовалюту під назвою Amazon Coins. Користувачі можуть оплачувати нею додатки для ПК та мобільних телефонів, електронні книжки та інші товари, придбані на веб-сайті amazon.com. Amazon Coins також можна переказувати на рахунки інших користувачів Amazon.com. Поки що це єдиний глобальний торговельний Інтернет-майданчик, який запустив цей проект.

Чим можна пояснити зростання популярності криптовалют серед мережевих користувачів у всьому світі? По-перше, ці розрахункові засоби стають все більш доступними для широкого загалу для придбання цифрової валюти. Усе, що необхідно – це наявність надійного джерела фінансування для забезпечення безперешкодної конвертації (інші види криптовалют, грошові перекази, платіжні картки, готівка та електронні платіжні системи на зразок PayPal). Збільшення кількості таких джерел розширює базу користувачів цифрової валюти. Для прикладу, в 2014 р. біткоїни були доступними для придбання у 246 країнах світу. Зважаючи на те, що криптовалюта є елементом електронного обігу, будь-яких географічних обмежень для її використання немає. Єдиною вимогою постає забезпечення дотримання вимог убезпечення від шахрайства з її використанням.

Зростання популярності криптовалют має й негативні наслідки. Так, реальні користувачі активніше відмежовуються від електронних операцій, маючи при цьому можливість створення необмеженої кількості індивідуальних рахунків. До того ж, розширення клієнтської бази є стимулом до запуску нових видів цифрової валюти, яку можуть використати в шахрайських схемах для приховування джерел фінансування та її виведення з потенційно небезпечних секторів задля унеможливлення подальшої ідентифікації.

Вище згадувалося, що статус фінансових установ автоматично отримують централізовані системи обігу цифрової валюти, які здійснюють конвертацію та переказ ціннісних еквівалентів (криптовалюти). Зауважимо, що спеціалісти прогнозують посилення адміністративного контролю за діяльністю таких систем. Необхідність якісного моніторингу діяльності децентралізованих систем визначає три ключові підходи:

– заборона чи обмеження діяльності на національному рівні;

– регулювання обігу криптовалюти з наданням їй відповідного законодавчо закріпленого статусу «товару»;

– контроль за наданням окремих послуг.

3. ВІДСЛІДКОВУВАННЯ ТА ВІДМИВАННЯ ЗЛОЧИННИХ ДОХОДІВ ІЗ ВИКОРИСТАННЯМ ЦИФРОВОЇ ВАЛЮТИ

3.1. Правові інструменти

Матеріальне право

Одним з основних завдань будь-якого кримінального розслідування є забезпечення правильної кваліфікації вчиненого злочинного діяння відповідно до положень чинного кримінального законодавства, тобто визначення елементів складу злочину. Принципи кваліфікації злочинів традиційно формувалися за нормами прецедентного права. Однак виникнення нових видів, способів і сфер злочинної діяльності (наприклад, шахрайство з цифровою валютою) потребує перегляду та оновлення наявних законодавчих інструментів. Перед розглядом можливостей кримінального законодавства щодо профілактики та протидії відмиванню коштів із використанням криптовалют, необхідно зазначити, що на цьому етапі в чинному законодавстві держав-членів ГУАМ не закріплено правовий статус цифрової валюти і, відповідно, її використання *per se* не буде визнано порушенням за принципом технологічного нейтралітету.

Відмивання грошей: елементи складу злочину

Відмивання грошей – це схема, яка передбачає здійснення низки транзакцій з метою унеможливлення ідентифікації джерела злочинних доходів та особу кінцевого реципієнта. Зазвичай порушниками є наркодилери, корумповані чиновники або розкрадачі державного майна. Вони використовують такі схеми для власного збагачення чи надають протизаконні послуги тим, хто хоче уникнути можливих правових наслідків. Об’єктом приховування є походження, джерело, розміщення, право власності та будь-які операції з майном, отриманим у результаті учинення злочинних дій. Усі зусилля зловмисників спрямовані на знищення будь-яких доказів зв’язку наявних доходів чи майна зі злочинною діяльністю з метою уникнення арешту і вилучення цих ресурсів. Криміналітет використовує динамічну глобалізацію світових економічних процесів для безперешкодного переміщення коштів з країни в країну за

короткий термін паралельно з інформаційним потенціалом віртуального простору.

Незалежно від того, хто використовує ці схеми, вони функціонують за одним принципом. Виділяють три основні етапи:

– етап *розміщення* передбачає первинну реєстрацію доходів у фінансовій системі. Цей процес може ускладнюватися, якщо, наприклад, розміщенню підлягають великі суми готівки;

– етап *розшарування* полягає в послідовності транзакцій, здійснених з метою приховування походження коштів. Цей процес є найбільш ресурсноємним. Також він цілком незалежний від географічних кордонів, адже порушник переказує через електронну систему певну суму за кордон, після чого вона фрагментується та у вигляді інвестицій реєструється на закордонному ринку опціонів. До того ж, кошти постійно переміщуються в самій системі для уникнення їх відслідковування, а також здійснюється безперервний аналіз та оцінка законодавства щодо виявлення недоліків та «сірих зон» для використання їх під час замітання слідів своєї злочинної діяльності;

– етап *інтеграції* є завершальним. Він передбачає, що кошти в повному обсязі та легально асимілюються в економіку. Після початкового розміщення у вигляді готівки і «очищення» їх за допомогою низки фінансових операцій такі ресурси успішно інтегруються в фінансову систему і можуть бути використані для будь-яких потреб.

Предикатні кіберзлочини

Аспекти кіберзлочинності в контексті незаконного використання цифрових валют можуть виявлятися різним чином. Кіберзлочини як автономна категорія в будь-якому разі пов’язані з використанням таких платіжних засобів і часто не отримують належної уваги з боку правоохоронних органів під час розслідування відмивання коштів. Таким чином, з поля зору випускають важливе джерело оперативних даних, які можуть допомогти у виявленні злочинних схем.

Предикатний злочин – це злочин, доходи від якого можуть стати об’єктом відмивання. Відмивання коштів із використанням цифрових валют може бути безпосередньо пов’язано зі злочинними доходами, отриманими внаслідок учинення кіберзлочинів (наприклад, маніпуляції з комп’ютерними обліковими даними або фальшування/шахрайство з використанням

інформаційних технологій). Статус предикатного злочину варіюється залежно від юрисдикції (згідно з чинним національним законодавством). У такому разі для встановлення складу злочину правоохоронці будуть спиратися на елементи кіберзлочинів. Однак кіберзлочини матимуть статус вторинних щодо відмивання коштів із використанням цифрових валют.

«Основний» кіберзлочин проти комп'ютерних систем чи даних може також бути вторинним в межах розслідування низки злочинів, пов'язаних із використанням цифрової валюти. Наприклад, коли електронний гаманець стає об'єктом «зламування» для крадіжки біткоїнів або коли рахунки третіх осіб використовують для проведення операцій без їх попереднього інформування і згоди. Таким чином, важливо добре розуміти природу окремих кіберзлочинів, охоплюючи неправомірний доступ, втручання в роботу системи і дані, незаконне використання пристроїв. Практика підтверджує, що більшість потенційних випадків кіберзлочинів не розслідують належним чином. Для прикладу наведемо декілька визначень, важливих з точки зору їх застосування з метою розслідування злочинів, пов'язаних з цифровими валютами.

Неправомірний доступ є базовим злочином, що становить загрозу безпеці (конфіденційності, цілісності та доступності) комп'ютерних систем і даних. Цей злочин є хакерською атакою, яка не завжди передбачає наявність негативних наслідків для систем чи даних (втручання, втрата тощо), але є демонстрацією вразливості системного захисту і може бути сигналом про можливі більш деструктивні атаки та злочини. Елементами складу злочину (централізованих і децентралізованих систем) є:

а) акт «доступу» передбачає проникнення в систему чи її структурну частину (обладнання, компоненти, збережені дані, каталоги, дані трафіку та контенту) незалежно від типу з'єднання та зв'язку. Метою може бути база даних акаунтів у комп'ютерних іграх, гаманці/чарунки з біткоїнами, серверна інфраструктура обмінних ресурсів тощо;

б) вхід до комп'ютерної системи здійснено незаконно (законним визначається доступ в межах адміністративного чи судового провадження чи домовленості); демонстрація поведінки, яка не має легальних пояснень, виправдань чи підстав відповідно до чинного національного законодавства;

в) намір щодо неправомірного доступу повинен бути доведений першочергово;

г) немає потреби в завданні конкретних збитків та іншого негативного впливу – сам по собі факт учинення такого діяння є кримінальним правопорушенням (цей момент може бути важливим для кваліфікації спроби відмивання коштів).

Криміналізація втручання в комп'ютерні дані має на меті захист цілісності та конфіденційності комп'ютерних даних від дій, які становлять загрозу їх цілісності та/або доступності. Цей злочин можна інтерпретувати як діяння, вчинене для перешкоджання належному функціонуванню даних чи програм шляхом пошкодження, видалення, зміни комп'ютерних даних. Елементами складу злочину є:

а) акт маніпуляції даними (пошкодження, видалення, зміна) здійснено через використання різних вірусних, троянських та інших шкідливих програм, що становлять загрозу як для цифрової валюти, так і для особистих даних користувачів;

б) наявне незаконне втручання в дані (будь-які несанкціоновані угодою чи законом дії), тобто в контексті цифрових валют повинні бути заборонені «конкретні дії, пов'язані з анонімною комунікацією (наприклад, коли інформація заголовка пакету змінюється з метою приховування особи зловмисника». Йдеться про те, що використання додаткових онлайн-інструментів для підвищення рівня анонімності користувачів систем децентралізованих цифрових валют може розглядатися як елемент складу злочину;

в) намір щодо неправомірного доступу потребує першочергово доведення.

Втручання в систему є перешкоджанням належному функціонуванню комп'ютерної системи. Елементами складу злочину є:

а) акт перешкоджання вчинений шляхом введення, передачі, пошкодження, видалення, зміни чи блокування комп'ютерних даних (дії, що провокують коротко- чи довготривалий вихід з ладу системи обробки операцій з віртуальними валютами чи серверної інфраструктури комп'ютерних ігор, які використовують такі валюти);

б) перешкоджання повинно суттєво негативно впливати на здатність власника чи оператора використовувати систему чи

забезпечувати взаємодію з іншими системами (наприклад, за допомогою програм, які генерують атаки «відмови в обслуговуванні» та вірусних програмних кодів для сповільнення роботи програми);

в) перешкоджання повинно бути здійснено незаконно;

г) намір щодо перешкоджання із завданням збитків повинен бути доведений першочергово.

Незаконне використання пристроїв передбачає використання потенціалу програмного забезпечення (ПЗ) і апаратних засобів з метою учинення злочину проти конфіденційності, цілісності та доступності комп'ютерних систем чи даних. Більшість таких інструментів представлені пристроями чи технологіями подвійного призначення (можуть бути використанні як законно, так і незаконно). Для уникнення надмірної криміналізації основну увагу варто зосередити на пристроях, які можуть бути першочергово використані чи адаптовані для злочинної діяльності. Елементами складу злочину є:

а) володіння, використання, виробництво, продаж, придбання з метою використання, імпорт, розповсюдження та інші дії, спрямовані на підвищення рівня доступності пристроїв (включаючи комп'ютерні програми), призначених або пристосованих для вчинення злочинів проти комп'ютерних систем і даних (хакерські утиліти, віруси та інші шкідливі програми для здійснення цільових атак на комп'ютерні системи і дані систем цифрових валют та їх користувачів, «зламані» системи і рахунки клієнтів як засоби для відмивання злочинних доходів);

б) виробництво, продаж, придбання задля використання, імпорт, розповсюдження та інші дії з метою отримання доступу до паролів, кодів доступу та аналогічних даних;

в) використання повинно бути визнане незаконним;

г) намір щодо здійснення такої діяльності повинен бути доведений першочергово.

Комп'ютерне шахрайство є асимілюючим злочином, що об'єднує елементи традиційного шахрайства з інформаційно-комунікаційними технологіями. Тому таку діяльність не криміналізують як окремий злочин, а визначають як юридичну конструкцію, що інтегрує елементи інформаційних та комунікаційних технологій в одне обвинувачення. В контексті цифрових валют такі елементи представлені конкретними

маніпуляціями з даними, а саме – введення, зміна, псування та видалення інформації. Для доказування наміру (на відміну від інших кіберзлочинів) необхідно підтвердити наявність наміру щодо введення, зміни, псування та видалення інформації та специфічного наміру щодо вчинення неправомірних дій з метою отримання вигоди для себе чи третьої особи.

Об'єктивні та суб'єктивні аспекти використання цифрових валют

Кримінальне право держав-учасниць ГУАМ поділяє елементи складу злочину на об'єктивні (діяння, об'єкти та засоби вчинення злочину) і суб'єктивні (намір, мета, співучасть тощо). Розглянемо ці категорії на прикладі відмивання коштів з використанням цифрових валют. Об'єктивні елементи такого злочину з технічної точки зору не будуть відрізнятися від аналогічних елементів інших злочинів. Залучення експертів для отримання відповідних висновків може бути необхідним на етапі опрацювання технічних питань і порівняльного аналізу з урахуванням особливостей традиційних фінансових операцій. Використання цифрової валюти можна розглядати як об'єктивний елемент кримінального правопорушення (відмивання коштів):

– на етапі розміщення, введення отриманих злочинним шляхом грошей в обіг передбачено, що факт придбання цифрової валюти через обмінні пункти (децентралізовані валюти) чи адміністратора (централізовані валюти) може бути представлено як елемент злочину;

– на етапі розшарування (процес легалізації злочинних доходів шляхом маскування джерела походження та приналежності) передбачено, що такі характерні для цифрових валют риси, як анонімність і проблематичне відслідковування операцій можуть бути представлені як елемент складу злочину (доказування наміру);

– на етапі інтеграції (процес реінтеграції «легалізованого» майна в економіку) використання цифрової валюти може бути одним з елементів складу злочину залежно від ситуації; реінвестування «відмитих» доходів на ринку цифрових валют також може бути використане в цьому аспекті.

Аргументи сторони обвинувачення в процесі доказування наявності наміру можуть бути підкріплені характерними особливостями цифрових валют, серед яких:

– анонімність і відсутність особистої взаємодії;

– проблематичне відслідковування, зокрема відсутність паперового/документального сліду (наприклад, чіткий намір уникнення традиційних фінансових механізмів і ставка на криптографію для ускладнення процедури криміналістичної експертизи);

– обіг цифрових валют за межами визначених фінансових установ в умовах повної відсутності регулювання.

Процесуальне право

Процесуальні аспекти розслідувань випадків відмивання коштів з використанням цифрових валют спрямовані на забезпечення правової основи для конкретних заходів, вжитих правоохоронцями чи органами контролю з метою виявлення, розслідування та кримінального переслідування. З огляду на визначення нами кіберзлочинів як предикатних чи вторинних щодо відмивання грошей із використанням цифрової валюти, варто детальніше зупинитися на процесуальних правилах та інструментах, що використовуються для збору та збереження електронних доказів. Процесуальні повноваження з точки зору їх призначення розподіляють на:

– процедури, націлені на збір оперативних даних (виявлення злочинних діянь та/або доходів);

– процедури, спрямовані на забезпечення і використання доказів у кримінальному провадженні.

Збір оперативних даних про використання цифрових валют для відмивання злочинних доходів забезпечується за допомогою вжиття відповідних заходів (інформаційна безпека) декількома способами, передусім через повідомлення центрів з реагування на інциденти в галузі комп'ютерної безпеки (англ. Computer security incident response team, CSIRT). Інформація про різноманітні інциденти проти комп'ютерних систем і даних може стати предметом розслідувань, які провадять IT-підрозділи. На практиці реагування на подібні інциденти CSIRT здійснює згідно з визначеними процедурами, у результаті чого не завжди будуть отримані докази, допустимі в кримінальному провадженні. Таким чином, зважаючи на тісний

зв’язок між кіберзлочинами, цифровими валютами і відмиванням коштів у Інтернет-мережі, правоохоронні мають можливість використовувати такі джерела інформації (компетенція національного CSIRT):

– повідомлення про інциденти у сфері комп’ютерної безпеки, безпосередньо пов’язані з фінансовим сектором, отримані з місцевих, секторальних або національних сенсорних мереж (апаратне чи програмне забезпечення, призначене для моніторингу національного Інтернет-сегмента з питання підозрілих коливань трафіку) та міжнародних баз даних CSIRT (ShadowServer чи Arbor Networks). Для отримання відомостей про інциденти необхідними є спеціальні (найчастіше письмові) угоди з CSIRT про надання інформації (які можуть також містити конфіденційну інформацію). Сам запит повинен містити чітке визначення мети отримання необхідної інформації;

– інформація про використання шкідливих програм з метою крадіжки особистих даних чи порушення недоторканості приватної фінансової інформації, зокрема випадки фіксації даних ПЗ (для управління централізованими чи децентралізованими цифровими валютами) в слідах трафіку таких програм;

– загальні відомості про хакерські спільноти і загрози національному кіберпростору, серед іншого інформацію з різноманітних форумів і платформ.

З огляду на те, що дані CSIRT часто є приватними та/або конфіденційними, відомості про інциденти у сфері комп’ютерної безпеки повинні запитуватися в кожному конкретному випадку і в межах поточного фінансового розслідування. Попри наявність можливості запровадження механізму регулярного надання такої інформації в межах міжвідомчого співробітництва, така звітність навряд чи буде мати важливе практичне значення для розслідування з огляду на її сукупний об’єм і суто технічний характер.

Збір інформації в режимі реального часу – це процедура збору генерованих комп’ютерами даних про потоки інформації, які надають можливість забезпечити її трансфер від джерела походження до місця призначення. Дані трафіку, які можна зібрати за допомогою наявних процедур, містять джерело інформації, пункт призначення, маршрут, час (GMT), дату, об’єм, тривалість і тип сервісу.

Збір даних трафіку є можливим завдяки судовому санкціонуванню і використанню спеціалізованого обладнання представниками правоохоронних органів (ІТ-підрозділи) та/або Інтернет-провайдерами. Таким чином, діяти варто в межах визначених процедур. Залежно від юрисдикції, слідчий чи прокурор звертається з клопотанням до суду, уповноваженого розглядати і санкціонувати вжиття визначених заходів. У зазначеному клопотанні повинні бути вказані засоби для збору таких даних і компетентний підрозділ.

Зазвичай національні ІТ-підрозділи мають досвід збору даних трафіку в режимі реального часу. Проте вимога щодо дотримання балансу між інтересами слідства і втручанням в особисте життя Інтернет-користувачів розкриває причини застосування таких процедур лише у важливих ситуаціях. Зауважимо, що навіть в разі готовності державних (центри криміналістичної ІТ-експертизи) чи приватних (Інтернет-провайдери) партнерів забезпечувати збір даних трафіку в режимі реального часу спільно з відомствами, відповідальними за фінансові розслідування, варто обов'язково звертатися до експертів ІТ-підрозділів із запитом на отримання відповідних технічних інструкцій.

На відміну від збору даних трафіку в режимі реального часу, перехоплення даних контенту (будь-які інші дані комунікації за межами трафіку) передбачає застосування традиційних методів збору даних контенту з телекомунікаційних пристроїв (наприклад, телефонні розмови). Цей метод є ефективним слідчим інструментом для встановлення незаконного характеру комунікації, тобто чи містить вона загрозу, елементи харасменту (сексуального домагання), злочинної змови чи шахрайства тощо. У контексті розслідування кіберзлочинів таке перехоплення охоплює отримання, перегляд, збір та копіювання всього змісту чи будь-якої складової комунікативного блоку, охоплюючи комп'ютерні дані, дані контенту, трафіку та/або їх електронних емісій, що передаються за допомогою дротових, радіо-, електронних, оптичних, магнітних та інших форм і засобів комунікації.

У державах-учасницях ГУАМ процедура перехоплення даних повинна бути зафіксована в положеннях закону про оперативно-розшукову діяльність (перехоплення даних з будь-яких

інформаційних та комунікаційних мереж в межах традиційних процедур перехоплення/прослуховування) або інкорпорована в кримінально-процесуальне законодавство. Незалежно від джерел права, перехоплення даних контенту можуть здійснювати різні відомства (ІТ-департаменти та оперативні підрозділи поліції). З огляду на необхідність дотримання принципу недоторканості приватного життя перехоплення даних контенту може проводитися лише за наявності судової санкції, тому до розгляду суду повинні бути надані всі клопотання із зазначенням мети, методів та засобів перехоплення даних контенту, а також відповідальних підрозділів.

Забезпечення доказової бази

Правоохоронні органи можуть подати запит або аналогічним способом ініціювати передачу комп'ютерних даних як доказів для розслідування конкретного кримінального провадження чи судового розгляду. Метою такої процедури є профілактика знищення комп'ютерних даних, важливих для розслідування кіберзлочину шляхом збереження їхньої цілісності і забезпечення захисту від негативного впливу на якість чи доступність. Процедуру збереження даних застосовують за наявності потенційного ризику її знищення чи псування (наприклад, згідно з внутрішньою політикою установи, дані підлягають видаленню після завершення визначеного терміну або, якщо вони збережені на носії, то їх видаляють для звільнення простору, а також у разі регулярного видалення даних трафіку, доступних в обмежений період часу). Ордер на збереження комп'ютерних даних є ефективним інструментом, оскільки дає змогу забезпечити цілісність електронних доказів на визначений термін (до 90 днів), впродовж якого компетентні органи можуть подати запит на їх розкриття. Ордер може бути використано як додаткову гарантію забезпечення автентичності даних, які будуть подані як докази у кримінальному провадженні. Фізичні та юридичні особи, які володіють чи розпоряджаються зазначеними даними, зобов'язані не розголошувати іншим особам інформацію про застосування вищезгаданої процедури. Ордер на забезпечення збереження цілісності даних може використовувати будь-який орган досудового слідства (спеціальні знання з опрацювання

електронних доказів для цього не потрібні, лише чітко визначений об'єм і характеристика даних).

Забезпечення збереження даних трафіку здійснюється за вказаною вище процедурою на підставі запиту правоохоронних органів. Отримання даних трафіку є необхідним для ідентифікації джерела чи адресата відповідної комунікації, що має вирішальне значення для встановлення осіб, які безпосередньо вчинили злочин. Варто зауважити, що такі дані часто зберігають протягом нетривалого періоду (політика захисту даних, що передбачає визначення строку зберігання даних виключно за необхідністю їх опрацювання). До того ж, дані трафіку, пов'язані з комп'ютерними злочинами, можуть бути об'єктом розпорядження декількох провайдерів. У такому разі провайдер, який отримав ордер на збереження даних, повинен терміново проінформувати відповідний правоохоронний орган про кількість даних трафіку з метою виявлення інших провайдерів послуг і маршрут передачі даних.

Значна частина інфраструктури та комп'ютерні системи, які використовують для Інтернет-зв'язку, підпорядковані приватному сектору. Інтернет-провайдери, а також провайдери електронного зв'язку та веб-сервісу виконують функції управління, зберігання та контролю інформації про підключення до Інтернету, транзакції та контент. Використання правоохоронними органами заходів примусу (арешт та обшук) з метою отримання цих даних є неможливим через значну кількість паралельних розслідувань та неминучу загрозу втручання в законну підприємницьку діяльність. Ордер на надання інформації використовують для отримання комп'ютерних даних, які перебувають в розпорядженні фізичної особи чи провайдера послуг. Поняття «володіння» і «контроль» застосовують до даних, які юридично та технічно перебувають у фізичному володінні провайдера послуг чи в локалізованому архіві (дистанційно). Термін «інформація про абонента» застосовують до будь-якої інформації про абонента і надані йому послуги, які контролює провайдер. Таку інформацію можна використати для ідентифікації конкретних послуг і технічних процедур або тоді, коли за допомогою наявної технічної адреси та інформації про абонента встановлюють особу.

Процедури обшуку і вилучення комп'ютерних даних (електронних доказів) є асимілюючими механізмами, спрямованими на гармонізацію наявних кримінально-процесуальних повноважень щодо обшуку і вилучення матеріальних об'єктів з позиції їх використання під час роботи з комп'ютерними системами і даними. Обшук і вилучення таких даних суттєво відрізняється від аналогічної процедури з матеріальними об'єктами (огляд локації та вилучення матеріального об'єкта з приміщення/середовища). У віртуальному середовищі збір даних здійснюють під час обшуку та щодо інформації, зафіксованої на момент його проведення. Є два основних способи проведення розслідування: вхід до системи і пошук даних, які локалізовані в ній чи її структурній частині (наприклад, через підключений пристрій зберігання даних); аналогічний пошук даних на автономному носії. Специфіка електронних доказів зумовлює необхідність застосування нетрадиційного підходу. Головним є забезпечення читабельності даних. Зазначене передбачає такі дії: якщо дані можна прочитати лише за допомогою комп'ютерної системи, в якій вони зберігаються, то необхідно повністю її вилучати. В інших випадках достатньо скопіювати дані на автономний носій. Аналогічно відбувається вилучення інформації з підключених пристроїв (накопичувачів, мереж тощо).

Одним із найважливіших повноважень під час проведення обшуку і вилучення комп'ютерних даних, відповідно до Конвенції Ради Європи про боротьбу з кіберзлочинами, є заборона доступу до визначених даних. Їхня цінність розкривається саме в контексті розслідування відмивання коштів з використанням ІТ-технологій, оскільки деактивація обладнання, ПЗ і онлайн-платформ, що використовуються для відмивання злочинних доходів, може бути необхідною для мінімізації завданих потерпілим збитків.

У контексті практичного застосування питання проведення обшуку та вилучення може бути більш проблемним порівняно зі специфічними процесуальними повноваженнями. З іншого боку, правоохоронні органи традиційно вживають ці заходи із залученням експертів з ІТ-підрозділів (за необхідності).

Електронні докази, отримані в межах відповідних правових процедур, потребують належної попередньої обробки

з метою представлення їх у суді допустимими доказами. Переважно дотримання правових вимог щодо збору та вилучення доказів є достатнім для гарантування їх допустимості в кримінальному провадженні (не варто забувати про додаткові характеристики електронних доказів під час забезпечення відповідності цим вимогам).

Системи кримінального правосуддя в країнах ГУАМ акцентують на експертизі та показаннях свідків. Важливо, щоб докази були належним чином опрацьовані та представлені в кримінальному провадженні. Ставка на експертну підтримку є актуальною й щодо опрацювання електронних доказів. Сучасні комп'ютерні системи та пристрої мають специфічні індивідуальні характеристики та конфігурації, які потребують чіткого дотримання визначених процедур для вилучення необхідних даних, а опрацювання електронних доказів «неспеціалістами» суттєво підвищує ризик їх непередбачуваних трансформацій і визнання їх надалі недопустимими в межах кримінального провадження. Під час проведення експертного аналізу враховують:

– цілісність даних (висока волатильність електронних доказів зумовлює необхідність забезпечення надійного захисту від можливих трансформацій та автентичності з використанням різних прийомів і методів: доступ в режимі «Лише читання», аналіз цифрової копії, формування зображень чи фіксація обробки тощо);

– автентичність (відсутність будь-яких сумнівів щодо зв'язку між матеріалами доказової бази та фактом учинення злочинного діяння);

– повноту (докази оцінюють з точки зору збалансованості й об'єктивності щодо здатності розкрити повну картину злочину);

– достовірність;

– контрольний слід (збереження всіх офіційних документів, що підтверджують процес розслідування – скріншоти, фотографії чи відеозапис);

– експертну підтримку (підсилює аргументацію сторони процесу, яка надає докази);

– законність.

Гарантії та механізми захисту

Всі процедури, які застосовуються до електронних доказів, повинні бути здійснені з повагою до фундаментальних прав і свобод учасників кримінального провадження. Оскільки процесуальні дії в межах розслідування відмивання коштів з використанням цифрових валют визначають закони та нормативні положення в сфері боротьби з кіберзлочинами, то аналогічні підходи, передбачені стандартами, будуть також застосовані у визначеному випадку. Всі процесуальні дії, що передбачають втручання в особисте життя, потрібно здійснювати в межах відкритих розслідувань незалежно від того, про який злочин йдеться – кіберзлочини, відмивання коштів чи шахрайство (офіційне рішення про ініціацію кримінального розслідування розглядається як гарантію проти зловживання процесуальними повноваженнями, що може спровокувати негативні наслідки для приватного життя конкретних осіб). У деяких юрисдикціях обов'язковою умовою для можливості застосування спеціальних повноважень під час роботи з електронними доказами (перехоплення даних контенту чи збереження даних трафіку) є певний ступінь тяжкості злочину. Інакше кажучи, учинення злочину повинно передбачати застосування покарання у вигляді позбавлення волі. На це необхідно обов'язково зважати, тому що національне кримінальне законодавство більшість злочинів проти комп'ютерних систем і даних не кваліфікує як тяжкі. Таким чином, юристам-практикам доцільно кваліфікувати кіберзлочини в контексті відмивання грошей, що за будь-яких обставин надасть можливість визначити його як тяжке. Судовий наказ щодо застосування спеціальних процесуальних повноважень, які передбачають втручання в особисте життя (наприклад, перехоплення даних контенту), розглядається як першочергова гарантія дотримання балансу між інтересами держави та громадянина. У контексті злочинів, учинених з використанням цифрових валют, це часто передбачає свідому відмову правоохоронців від застосування таких процедур. Проте заміна таких «ліберальних» процедур іншими опціями (обшук

та вилучення без судового наказу) може спровокувати появу певних труднощів, якщо цей вибір буде оскаржено в суді з позиції пропорційності. Особливу увагу також варто приділити національним нормам у сфері захисту персональних даних. Попри те, що існує уніфікований міжнародний стандарт щодо незастосовності гарантій захисту даних (наприклад, згоди суб'єкта на опрацювання даних) під час проведення розслідування, наявна тенденція контролю за дотриманням вимог захисту даних під час збору та опрацювання оперативної інформації. Правоохоронні органи повинні бути проінформовані про такі стандарти і мати можливість консультуватися зі спеціалізованими місцевими установами.

3.2. Методологія розслідування

Маркери («червоні прапорці») та індикатори

Маркери та індикатори є важливим інструментом під час проведення фінансового розслідування, що передбачає вжиття визначених заходів з метою:

– виявлення масштабу злочинних мереж та/або масштабу злочинної діяльності;

– виявлення та відслідковування доходів від учинення злочинів, засобів для забезпечення терористичної діяльності та іншого майна, що підлягає конфіскації;

– опрацювання доказів, які можуть бути використані в кримінальному провадженні.

Більшість маркерів та індикаторів, що застосовуються під час розслідувань типових випадків відмивання коштів у Інтернет-мережі чи із використанням нових платіжних систем, доцільно розглядати також в контексті випадків відмивання коштів із використанням цифрової валюти, а саме:

– неспівпадіння між ідентифікаційними даними користувача та його IP-адресою;

– підозрілі IP-адреси та імена користувачів (клички, прізвиська, ICQ-номери);

– вхід чи спроби входу до систем через ненадійні IP-адреси або з IP-адрес чи адрес, ідентифікованих як сумнівні.

Однак такі маркери мають дещо узагальнений характер. Корисними саме для розслідувань злочинів із цифровою валютою можуть бути маркери/індикатори, запропоновані FATF (в контексті причетного провайдера платіжних послуг), наприклад:

– значна кількість банківських рахунків, зареєстрованих на одного адміністратора цифрової валюти чи компанії, що надає конвертаційні послуги (іноді розташовані на території різних держав), які використовують як транзитні (індикатор одного з етапів процесу відмивання грошей – «розшарування»);

– адміністратор цифрової валюти чи компанія, що надає конвертаційні послуги, перебувають на території однієї держави, але мають рахунки за кордоном за відсутності розширеної клієнтської бази (сумнівні підстави для ведення бізнесу за кордоном);

– циклічний рух грошових коштів між банківськими рахунками, зареєстрованими на різних адміністраторів цифрової валюти чи компаній, що надають конвертаційні послуги в різних державах (індикатор одного з етапів процесу відмивання грошей – «розшарування»);

– об'єм і регулярність операцій з готівкою (іноді розбивається на суми, менші від звітного ліміту), які здійснює власник адміністратора цифрової валюти чи компанії, що надає конвертаційні послуги, не є доцільними (прибутковими).

Технічні індикатори

Операції з деякими видами цифрових валют, особливо децентралізованими, передбачають встановлення відповідного ПЗ, ідентифікація якого на конкретному обладнанні може бути використана як індикатор. Серед найпопулярніших, яке встановлюють безпосередньо на ПК, – Bitcoin. Таке ПЗ функціонує як Bitcoin-гаманець із типовим позначенням wallet.dat. Існує декілька видів таких гаманців – Bitcoin Core, MultiBit, Hive, Bitcoin Armory, Electrum. Деякі модифікації після встановлення потребують завантаження повного ланцюга блоків, об'єм якого може досягати 20 ГБ, що є допоміжним інструментом для встановлення Bitcoin-директорії. Аналогічно функціонують і LiteCoin, DogeCoin та WebMoney, адже встановлення ПЗ супроводжується завантаженням доволі

об’ємних файлів. Переважно цифрові валюти використовують у віртуальних «світах» (локалізованих онлайн-середовищах).

Більшість цифрових валют віртуальних середовищ – Second Life Linden Dollars, Project Entropia Dollars чи World-of-Warcraft Gold – можуть бути придбані за допомогою спеціальних додатків.

Не всі цифрові валюти передбачають встановлення ПЗ (наприклад, Ripple-клієнт працює як додаток JavaScript в браузері користувача). Інші системи пропонують обрати між завантаженням ПЗ і взаємодією через веб-браузер. До того ж, зазвичай торгівлю цифровою валютою на біржах здійснює веб-браузер. Таким чином, закладки, історія веб-сторінок і кеш на комп’ютері підозрюваного можуть бути використані як докази операцій з цифровою валютою.

Нагадаємо, що цифрові валюти (особливо децентралізовані) є оцифрованим вартісним еквівалентом, який зберігає свої характеристики незалежно від місця та способу збереження. Саме тому немає причин «прив’язуватися» до локально досліджуваного комп’ютера. Об’єм даних у цифровому форматі зазвичай є невеликим (< 100 байт), тому існує безліч способів зберігати їх на інших носіях. Одним із таких способів є використання послуг дистанційного збереження даних. Також можна використовувати послуги електронної пошти, доступні через веб-браузер. У деяких випадках забезпечення приватності є додатковим бонусом. Такі послуги можна активувати за допомогою відповідного ПЗ, веб-інтерфейсу, стандартних (електронна пошта) чи мобільних додатків.

Існує ПЗ, що дає змогу зберігати інформацію про акаунти та логіни користувача. Так, користувач, маючи один пароль, отримує доступ до інших персональних облікових записів, що зберігаються у закодованому файлі (ідеальний варіант для зберігання невеликих текстових документів). Більшість веб-браузерів також забезпечують зберігання паролів доступу до веб-сайтів. Можливим є варіант, коли, за умови виявлення такого ПЗ, облікові дані щодо використання цифрової валюти чи сама валюта будуть зберігатися в ньому. Більшість таких ПЗ підтримують функції дистанційного архівування (облікових

даних, заміток тощо), плагінів для браузерів та синхронізації інформації з мобільним додатком.

Віртуальна машина – це ПЗ, яке використовують для емуляції роботи цілої операційної системи. Ідеться про те, що користувач може мати щось на зразок другого windows-комп'ютера, позначеного як «гість» (зберігається на комп'ютері, позначеному «користувач»). Більшість віртуальних машин використовується для кодування файлів з жорсткого диска. Відповідно, така машина не може бути активована без пароля. За таких умов можна використовувати захищену паролем віртуальну машину для всіх операцій з цифровими валютами, не залишаючи слідів у основній операційній системі «користувач».

ПЗ для цифрових валют та історія перегляду відповідних веб-сторінок, ідентифікованих на пристроях мобільного зв'язку (мобільні додатки Bitcoin, WebMoney та Ripple), також можуть бути індикаторами використання цифрових валют для відмивання злочинних доходів.

Криміналістична експертиза

Коректний збір доказів – це основа кримінального провадження. Розглянемо декілька окремих джерел електронних доказів та їх специфіку.

Під час розслідування злочинів у зазначеній сфері комп'ютер підозрюваного постає цінним джерелом доказів (не лише сам ПК, а й будь-які носії інформації – CD, DVD, зовнішні жорсткі диски, флеш-накопичувачі):

– докази у вигляді облікових записів, відвідування веб-сайтів, електронної пошти тощо;

– докази, що підтверджують факт володіння цифровою валютою підозрюваним;

– можливість ідентифікації окремих адрес, контрольованих підозрюваним, та історії здійснених транзакцій/контактів (у випадку роботи з біткоїнами);

– IP-адреса комп'ютера, що може бути зафіксована як «слід» у фінансовій діяльності підозрюваного (визначений період);

– доказ використання послуг дистанційного зберігання та архівування даних із можливістю зберігання цифрової валюти;

– паролі та інші облікові дані, що можуть бути використані з метою доступу до рахунків у цифровій валюті.

Хмарні сервіси

Оскільки цифрова валюта є віртуальним ціннісним еквівалентом, то немає підстав стверджувати, що такий еквівалент повинен обов'язково зберігатися локально на комп'ютері підозрюваного. Підозрюваний може використати онлайн-сервіс зберігання даних:

– хмарний сервіс (DropBox);
– послуги електронної пошти в Інтернет-мережі;
– будь-які мережеві сервіси з функцією збереження даних.

Знайти докази використання підозрюваним таких послуг з особистого ПК можливо за умови виявлення ПЗ, необхідного для роботи з хмарними сервісами, або ознак такої діяльності за історією перегляду веб-сторінок. Докази можуть бути підкріплені запитом про надання інформації, направленим провайдеру послуг із використанням відповідних правових інструментів:

– прямий контакт (через офіційний запит) з сервіс-провайдером для розкриття необхідної інформації;
– використання поліцейських каналів (контактні центри 24/7, мережа G8 або національне бюро Інтерполу);
– процедура надання взаємної правової допомоги (через Генеральну прокуратуру чи Міністерство юстиції).

Дослідження мережі

Під час аналізу даних мережевого (вхідного і вихідного) трафіку ПК підозрюваного можна виявити інформацію, яка свідчить про використання цифрових валют:

– зв'язок з розподіленою піринговою мережею віртуальної валюти;
– зв'язок ПК підозрюваного з адміністратором чи обмінним ресурсом;
– хмарні сервіси.

Перед фахівцями, які здійснюють аналіз мережі, можуть постати певні труднощі. По-перше, канал зв'язку між комп'ютером підозрюваного та комп'ютером третьої особи найімовірніше буде закодований. Проблема полягає в тому, що

аналіз мережевого трафіку не дає змоги визначити зміст здійсненої комунікації. Однак, навіть якщо канал зв'язку закодований, можливим є встановлення факту взаємодії через IP-адреси. По-друге, існують спеціальні проксі-програми, що надають можливість встановити анонімне з'єднання і приховати факт здійснення комунікації, найпопулярнішою серед яких є Tor (раніше називалася The Onion Router). Це програма, яка кодує та передає трафік через серію проміжних вузлів. Опрацьований системою трафік інші мережеві сервери ідентифікують як надісланий з конкретного вузла, приховуючи при цьому істинне джерело. Зауважимо, що відслідкувати трафік і визначити джерело в такому разі практично неможливо.

Альтернативою для приховування особи користувача є використання онлайнових проксі-програм. Принцип роботи передбачає, що користувач входить на веб-сайт через проксі, а не через стандартний браузер. У такому разі оригінальне джерело трафіку визначають за допомогою:

– звернення безпосередньо до адміністратора проксі-сервера з офіційним запитом про надання необхідної інформації (якщо такі дії не заборонені умовами надання послуг чи політикою конфіденційності);

– використання поліцейських каналів (контактні центри 24/7, мережа G8 або національне бюро Інтерполу);

– процедури надання взаємної правової допомоги (через Генеральну прокуратуру чи Міністерство юстиції).

Взаємодія з адміністраторами/біржами цифрових валют

Використовуючи процесуальні повноваження та інструменти, розглянуті вище, правоохоронні органи повинні також ініціювати і розвивати співробітництво з адміністраторами централізованих цифрових валют за прикладом аналогічного співробітництва з представниками приватного сектору під час розслідування кіберзлочинів.

Передусім варто спробувати встановити безпосередній контакт з адміністратором на основі договору щодо умов надання послуг чи правил конфіденційності, де часто передбачені положення про співробітництво з правоохоронними органами і гарантії конфіденційності та/або збереження

конкретних даних (про рахунки, операції тощо) за визначений період. Юридичні відділи адміністраторів можуть встановлювати таке співробітництво за відсутності спеціальних положень із забороною подібної практики. Центральні адміністратори мають статус юридичних осіб у межах національної юрисдикції, що забезпечує високі шанси започаткувати успішне співробітництво.

Саме тому, коли прямі неформальні контакти є малоймовірними або потребують забагато часу, взаємодія органів поліції є найбільш прийнятним варіантом. Такі можливості забезпечують контактні центри 24/7 (для держав-учасниць Конвенції Ради Європи про кіберзлочинність) мережею підрозділів у сфері ІТ-злочинів G8 та національними бюро Інтерполу, уповноваженими вживати від імені правоохоронних органів заходи, визначені двосторонніми угодами.

Взаємна правова допомога (ВПД) – це виключно формалізована процедура, що передбачає застосування традиційних підходів до взаємодії в межах кримінальних розслідувань (дво- чи багатосторонні угоди). Запити про надання ВПД щодо центральних адміністраторів направляють через центральні органи (найчастіше через Генеральну прокуратуру і Міністерство юстиції).

4. ІНСТРУМЕНТАРІЙ ТА ПРОЦЕДУРА ВИЛУЧЕННЯ ЗЛОЧИННИХ ДОХОДІВ

4.1. Поняття вилучення злочинних доходів

Вилучення злочинних доходів і засобів визначають як позбавлення компетентним органом чи судовою інстанцією підозрюваного (обвинуваченого) можливості відчужувати певне майно шляхом ініціації процедури арешту. На відміну від арешту, який є тимчасовим заходом, вилучення забезпечує безпосередній контроль компетентних органів чи суду над зазначеним майном. Вилучене майно залишається у власності підозрюваного (обвинуваченого) – фізичної чи юридичної особи (осіб) – на момент вжиття вказаного заходу. Проте компетентний орган чи суд може прийняти рішення про управління вилученим майном.

У процесі розгляду особливостей процедури вилучення злочинних доходів ми будемо використовувати такі дефініції:

– «доходи» визначаються як будь-яке майно, безпосередньо чи опосередковано отримане шляхом вчинення протиправних дій (матеріальне/ нематеріальне, рухоме/нерухоме, а також будь-які документи, які підтверджують право власності на це майно та причетність особи до будь-яких операцій із ним);

– «засоби» визначаються як будь-яке майно, яке було використано чи було заплановано його використання (повністю чи частково) з метою вчинення протиправних дій.

Наведені визначення застосовують також у контексті використання зловмисниками цифрової валюти (централізованої та децентралізованої) та електронних платіжних систем. Для операцій з децентралізованою цифровою валютою характерний надзвичайно високий ступінь анонімності користувачів. Тому вони можуть бути використані для відмивання злочинних доходів через придбання чи конвертації реальної валюти в електронну. Причому однією з найпоширеніших схем є «інвестування» в біткоїни, яке забезпечує накопичення доходів у вигляді біткоїнів, що використовуються для оплати різноманітних послуг, а також заробіток на коливаннях курсу цифрової валюти. Таким чином, процес розслідування

злочинів, пов'язаних з відмиванням електронних грошей, а також винесення судом відповідних вироків ускладнюється тим, що часто не вдається провести чітку межу між злочинними засобами та доходами. На практиці точки зору відсутність чіткого розмежування цих понять суттєво не впливає на виконання рішення щодо вилучення, оскільки засоби і доходи в багатьох випадках представлені одними й тими самими ресурсами.

Міжнародні правові процедури і стандарти

Ідентифікація, арешт, вилучення та конфіскація злочинних доходів є правовими процедурами, які застосовують як дієві заходи в боротьбі з організованою злочинністю. До того ж, кожна з окреслених процедур вимагає вагомих підстав для застосування. Якими саме міжнародними та національними нормативно-правовими актами потрібно послуговуватися в контексті застосування процедури вилучення злочинних доходів і засобів?

Одним із перших міжнародно-правових актів, у тексті якого було визначено застосування конфіскації злочинних доходів як профілактичного заходу і одного з принципів здійснення правосуддя, була Конвенція ООН про боротьбу із незаконним обігом наркотичних засобів і психотропних речовин 1988 року. Положення цього документа визначають підстави і процедуру арешту, вилучення та конфіскації доходів або майна еквівалентної вартості, отриманих у результаті вчинення злочинів, пов'язаних із незаконним вживанням чи обігом наркотичних засобів і психотропних речовин. Так, порушено питання про перенесення тягаря доказування в разі наявності сумнівів щодо законності походження майна.

Ці принципи відображено в положеннях Конвенції ООН проти транснаціональної організованої злочинності та протоколів, де визначено процедуру вилучення та конфіскації доходів організованих злочинних груп і висвітлено рекомендації для держав-членів ЄС щодо посилення міжнародної співпраці у сфері застосування процедур вилучення, конфіскації та управління злочинними активами. Конвенція ООН проти корупції, прийнята у 2003 р., визначає порядок застосування аналогічних заходів у рамках розслідування злочинів,

пов'язаних із незаконним збагаченням та зловживанням владою. У документі вперше фігурує термін «повернення активів», а також розкрито особливості функціонування цього правового механізму в країнах Європи. Необхідність стандартизації й оптимізації процедур вилучення, арешту та конфіскації злочинних доходів і засобів визнають необхідними й експерти FATF. Ідеться про обов'язкову конфіскацію майна і доходів, отриманих у результаті відмивання коштів та інших видів фінансових злочинів; засобів, які було використано або планувалося використати з метою учинення цих злочинів або майно еквівалентної вартості без порушення прав третіх сторін *bona fide*. Усі вищезазначені заходи застосовують компетентні органи, які були наділені відповідними повноваженнями:

– ідентифікація, відслідковування та оцінка майна, яке підлягає конфіскації;

– арешт та конфіскація майна з метою запобігання здійсненню будь-яких операцій (використання, передача, продаж тощо);

– вжиття заходів, спрямованих на попередження чи припинення дій, що унеможливлюють застосування державою механізмів для повернення активів, які є об'єктом конфіскації;

– вжиття будь-яких інших необхідних заходів у межах розслідування.

Національні правові процедури і стандарти

З метою належного вжиття компетентними органами таких заходів, як вилучення і конфіскація злочинних доходів, держава повинна не лише законодавчо закріпити ці повноваження у відповідних правових актах, а й створити умови, необхідні для їх реалізації та отримання ефективних результатів.

Держави-учасниці ГУАМ офіційно криміналізували легалізацію злочинних доходів шляхом внесення відповідних змін до чинних національних законодавств. У трьох із них (за винятком України) було застосовано принцип *all-crime*, за яким засоби і доходи, отримані в результаті учинення будь-якого злочину, можуть стати об'єктом арешту, вилучення та

конфіскації. Порядок здійснення зазначених процедур визначається чинними КПК. Позаяк жодне з положень кримінального законодавства цих держав не містить вказівок щодо заборони чи обмеження повноважень стосовно вжиття вищевказаних заходів. У процесі ідентифікації цифрової валюти як злочинного доходу чи засобу, варто звернути увагу на таке:

– беручи до уваги варіативність умов, в яких здійснюється арешт майна, а також наявність різних тлумачень самого визначення, потрібно враховувати природу цифрових валют (в межах законодавства, яке чітко визначає підстави для арешту засобів учинення злочину, арешт злочинних доходів передбачено у випадках учинення визначених видів злочинів або з урахуванням ступеня тяжкості);

– існують різні ступені залучення судових інстанцій до процедури арешту майна, охоплюючи утвердження проведеного арешту (надзвичайні обставини), які впливають на оперативність цієї процедури і мають першочергове значення для забезпечення недоторканості електронних доказів;

– законодавство окремих держав передбачає застосування процедури накладення арешту на майно в межах цивільного законодавства, що потребує відповідної підготовки працівників правоохоронних органів, уповноважених проводити арешт;

– законодавство всіх держав-учасниць ГУАМ передбачає можливість проведення арешту до винесення обвинувального вироку. Це означає, що стандарт доказування, необхідний для вжиття цього заходу, є нижчим за стандарт, необхідний для винесення судового рішення.

Не менш важливим є питання визначення відомств, уповноважених проводити арешт у межах розслідування кримінальних злочинів із використанням цифрової валюти. На сьогодні держави-учасниці ГУАМ передали відповідні функції правоохоронним органам, уповноваженим використовувати будь-які передбачені чинними КПК процедури, якщо вони мають статус підслідних у межах поточного кримінального розслідування (у контексті нашої

тематики – підрозділи, уповноважені розслідувати легалізацію злочинних доходів).

Визначення юрисдикції

Цифрова валюта функціонує у віртуальному середовищі, яке не має національних кордонів. Аспект визначення юрисдикції в межах міжнародного співробітництва є одним із найбільш проблематичних під час вирішення питань з повернення активів, які мають статус злочинних доходів і були отримані з використанням цифрової валюти. На сьогодні не зафіксовано випадків активізації міжнародного співробітництва з метою проведення арешту чи конфіскації цифрової валюти. Таким чином, наведені нижче рекомендації базуються на загальних принципах встановлення юрисдикції для накладення арешту на цифрову валюту, визначену як засіб або дохід від злочинної діяльності.

Юрисдикційні аспекти арешту злочинних доходів і засобів учинення злочинів виявляють відмінності між централізованими і децентралізованими цифровими валютами. Наприклад, обмін централізованих валют, які використовують в онлайн-іграх, розглядають як дозвіл для отримання доступу до конкретних функцій чи послуг, запропонованих адміністратором. Унаслідок цього валюта залишається під контролем компанії-емітента з технічної та юридичної точок зору. Децентралізовані валюти (криптовалюти) демонструють дещо іншу картину. Біткоїни не мають чітко визначеного формату, навіть у вигляді цифрового файлу. Фактично існує лише реєстр операцій між електронними гаманцями з динамічним балансом. Біткоїни не можна розглядати як доходи чи засоби вчинення злочину незалежно від фіксації розміщення в конкретному середовищі. Однак біткоїн-транзакції є власне угодами між біткоїн-адресами окремих користувачів, які можна використати як ідентифікатор. Таким чином, територіальна юрисдикція над доходами і засобами вчинення злочинів із використанням криптовалют визначатиметься місцем фактичного розташування обладнання,

на якому зберігається електронний гаманець. Суттєвою перешкодою для встановлення юрисдикції в таких випадках є використання cloud-сервісів («хмарних сервісів»). Дані гаманців можуть регулярно мігрувати з одного сервера на інший, легко перетинаючи національні кордони. Експерти називають цей процес «делокалізацією». Тому принцип територіальності буде залишатись основним під час встановлення юрисдикції до перегляду відповідних положень міжнародного публічного права.

4.2. Покрокова стратегія

Крок 1. Ініціація фінансового розслідування

Фінансове розслідування передбачає забезпечення збору, опрацювання й аналізу всієї наявної інформації з метою здійснення кримінального переслідування та вилучення злочинних доходів і засобів. Його головним завданням є ідентифікація та документальна фіксація переміщення коштів під час учинення злочинних діянь. Зв'язок між джерелом походження цих коштів та бенефіціарами, які отримували, зберігали чи переказували гроші, є ключовим доказом причетності до злочину. Тобто фінансове розслідування можна визначити як процес, що здійснюється паралельно з основним кримінальним розслідуванням (незалежно від виду злочину – кіберзлочини, шахрайство чи відмивання грошей) і надає можливість спеціалістам сконцентруватися на роботі зі злочинними доходами та засобами.

Фінансові розслідування, які вимагають застосування спеціальних знань та досвіду, часто потребують залучення експертів з інших установ. У межах національної юрисдикції це питання можна вирішити декількома способами:

– створення об'єднаної слідчої групи за рішенням прокурора, уповноваженого координувати та розподіляти завдання;

– залучення експертів з відслідковування та аналізу фінансових транзакцій (цю роботу координує відповідний правоохоронний орган);

– виділення двох паралельних ліній розслідування – пошуку злочинних активів та кримінальної складової із забезпеченням належної міжвідомчої співпраці.

Незалежно від того, який варіант буде обрано, варто завжди пам'ятати про специфіку фінансових розслідувань. Зокрема вона передбачає застосування вищих стандартів доказування порівняно з кримінальним правопорушенням (відмивання коштів). Доказування злочинного походження майна та доходів не потребує застосування принципу «за межами розумного доказування», на відміну від традиційних кримінальних розслідувань.

Крок 2. Відслідковування та ідентифікація активів

Відслідковування активів, що власне є пошуком слідів, залишених у системі, постає важливим етапом будь-якого фінансового розслідування в межах визначення злочинного походження цих коштів або засобів учинення злочину. Під час розслідування злочинів із використанням цифрової валюти цей процес є підготовчим і дає змогу зафіксувати сам об'єкт потенційного арешту чи вилучення.

Відслідковування активів як аналітичний механізм працює за принципом індикації. Маркерами є так звані червоні прапорці, виявлення яких допомагає встановити злочинне походження ідентифікованого майна чи доходів. Для злочинів з використанням цифрової валюти як «червоних прапорців» характерним є:

– використання значної кількості банківських рахунків, зареєстрованих одним адміністратором цифрової платіжної системи чи обмінного ресурсу (іноді в декількох державах), що використовуються як «фільтраційні»;

– наявність адміністратора цифрової платіжної системи чи обмінного ресурсу, офіційно зареєстрованого на території однієї держави, який обслуговує рахунки на території інших держав, де не має розширеної клієнтської бази;

– двостороннє переміщення доходів між рахунками, зареєстрованими різними адміністраторами цифрової платіжної системи чи обмінного ресурсу на території різних держав (може бути індикатором злочинного посередництва);

– об'єми та частота здійснення готівкових транзакцій (із надмірною структурованістю та суттєвими перевищеннями порогу обов'язкової реєстрації), здійснені адміністраторами цифрової платіжної системи чи обмінного ресурсу без видимої економічної доцільності;

– системи обігу цифрової валюти з проблемною реєстрацією та/або зафіксованими непрозорими операціями.

Так, усі вказані індикатори мають спільну рису – визначення «точок контакту» цифрової валюти з фінансовими установами, які в такому разі представлені адміністраторами цифрових платіжних систем чи обмінних ресурсів, хостинг-провайдерами та компаніями з обслуговування торговельних майданчиків тощо. Варто пам'ятати, що транзакції з використанням цифрової валюти здійснюють в кіберпросторі «в обхід» фінансових установ. Вони характеризуються високим ступенем анонімності, використанням криптографічного підпису та зведенням до мінімальної системної фіксації, що максимально ускладнює процедуру відслідковування обігу криптовалюти під час проведення фінансового розслідування. Специфічні умови функціонування такої валюти визначають декілька опцій для забезпечення її відслідковування в системі.

Опція 2.1: служба фінансової розвідки

Служба фінансової розвідки (СФР) є одним з ключових партнерів, який доцільно залучати на етапі ідентифікації та відслідковування злочинних доходів і засобів, оскільки вона має право першочергового доступу до відповідної інформації та здійснює безперервний аналіз даних з метою профілактики використання злочинних схем для відмивання коштів і фінансування тероризму (наприклад, так звані ЗСТ – звіти про сумнівні транзакції). У централізованих системах контроль за випуском та розподілом обмінних одиниць або ігрових ресурсів

здійснюють через внутрішні канали (системні елементи, що функціонують за межами державних фінансових структур). Таким чином, доступність і цінність ЗСТ, наданих адміністраторами таких систем, буде залежати від політики державного регулювання обігу цифрової валюти, зокрема від того, чи закріплені законодавчо зобов'язання адміністраторів щодо подання зазначеної звітності до СФР.

Проте ефективність міжвідомчої співпраці залежить не лише від оперативності обміну даними, а й від рівня поінформованості правоохоронних структур про специфіку (структурну організацію, роль та повноваження) функціонування СФР.

Опція 2.2: контроль за транзакціями

Інформація та оперативні дані можуть бути отримані за допомогою видачі моніторингового ордера чи ордера на надання інформації.

Моніторинговий ордер – це виданий компетентним органом наказ із вимогою щодо розкриття фінансовою установою уповноваженій особі інформації про операції, здійснені за конкретним рахунком, відкритим цією установою, або за рахунком, який належить вказаній в ордері особі. Такий наказ може визначати зобов'язання фінансової установи щодо інформування компетентних органів про транзакцію (під час спроби або одразу ж після її здійснення). Також моніторинговий ордер може зобов'язати фінансову установу утриматися від проведення чи завершення операції впродовж визначеного періоду часу.

Згідно з чинним кримінально-процесуальним законодавством держав-учасниць ГУАМ, моніторингові ордери видаються правоохоронними органами і СФР (за винятком Азербайджану), уповноваженими здійснювати моніторинг будь-якого «сумнівного» рахунку. Правові підстави таких повноважень закріплені спеціальним законодавством з боротьби з відмиванням грошей або законом про оперативно-розшукову діяльність. Підставою для видачі такого ордера може бути запит

іноземного компетентного органу, зокрема СФР, результати внутрішнього аналізу, ЗСТ (отримані від суб'єкта моніторингу), запит прокуратури.

Ордер на надання інформації – це санкціонований судом наказ, що зобов'язує конкретну особу надати для перевірки уповноваженим представником документи, що мають пряму вказівку чи інформацію, яку можна використати для встановлення місцеперебування майна (об'єкта арешту чи конфіскації), або яка допоможе визначити вартість майна чи матеріальну вигоду, отриману обвинуваченим після вчинення ним злочинного діяння.

Основним завданням таких ордерів є примусове надання зазначеною в них фізичною чи юридичною особою інформації/документів (копій) упродовж визначеного часу. Такі ордери матимуть суттєві відмінності з огляду на застосування їх до централізованих чи децентралізованих цифрових валют:

– адміністратори централізованих цифрових валют безпосередньо отримують і забезпечують виконання відповідних вимог;

– зважаючи на відсутність центральних адміністративних органів у систем децентралізованих цифрових валют, моніторингові ордери щодо надання інформації із зазначенням імен конкретних клієнтів та/або їхніх рахунків, що підлягають перевірці та моніторингу, можуть бути направлені особам, які здійснюють конвертацію цифрових валют.

Опція 2.3: розкриття фінансової інформації

Розкриття фінансових даних – це ще одна можливість для використання ордерів на надання інформації в межах виявлення злочинних доходів та засобів. Обов'язковою вимогою для банківських та небанківських установ у питанні протидії відмиванню грошей є зберігання інформації про рахунки та діяльність власних клієнтів, яка може бути надана за запитом компетентних органів і використана під час пошуку відповідних активів.

З позицій цифрових валют такі запити потрібно направляти компаніям, які контролюють їх конвертацію та можуть надати згадану вище інформацію. Грошові перекази часто застосовують для обміну фіатних грошей на децентралізовані цифрові валюти (біткоїни) і навпаки. Такі види розрахункових операцій, які використовують обмінні ресурси, є додатковим цінним задокументованим джерелом інформації, що обов'язково потрібно взяти до уваги.

Крок 3. Контроль активів

Одразу після виявлення злочинні доходи та засоби визначають як об'єкт арешту – взяття визначеного майна під контроль і здійснення повноважень володіння, розпорядження чи управління. Попри наявний досвід здійснення арешту та конфіскації електронних грошей чи рахунків (нематеріальні активи), які можна використати за аналогією, обіг цифрових валют за відсутності державного регулювання відбувається за межами встановлених фінансових установ і каналів. Процедура арешту цифрової валюти як злочинного доходу чи засобу буде залежати від типу системи (централізована чи децентралізована).

Опція 3.1: вилучення валютних резервів з централізованих систем

Централізована цифрова валюта як актив залишається під цілковитим контролем адміністратора. Тому арешт такого ресурсу може застосовуватися лише до юридичних осіб, які виконують функцію адміністрування, забезпечуючи виконання законних вимог правоохоронних органів. Однак є й певні особливості такої процедури. Наприклад, якщо системи WebMoney чи E-gold (нині не функціонує) самостійно здійснюють адміністрування цифрової валюти, яку можливо арештувати і конвертувати у фіатні гроші, то накладення арешту на амуніцію чи бойові кораблі

комп'ютерної гри не буде мати практичної цінності для держави. У такому разі застосовують вартісну конфіскацію – накладення грошового стягнення (штраф, сума якого значно перевищує прибуток чи отриману в результаті вчинення злочину вигоду). Така конфіскація може бути застосована до будь-якого типу активів і дає змогу уникнути потенційних труднощів, пов'язаних з управлінням специфічними категоріями активів.

Опція 3.2: вилучення криптовалюти з децентралізованих систем

На відміну від централізованих цифрових валют, криптовалюту не контролює централізований адміністративний орган. Процедура арешту таких ресурсів повинна застосовуватися до визначених користувачів, а об'єктом арешту буде ресурс, зафіксований в індивідуальних гаманцях чи за IP-адресою. Теоретично взяття під контроль електронного гаманця з цифровою валютою можна здійснити двома способами. Перший передбачає примус користувача до надання компетентному органу пароля доступу. Перевагою такого підходу є можливість продовження слідства, оскільки з огляду на анонімність криптовалют неможливо встановити, хто саме є фактичним власником гаманця. Однак недоліків у цього підходу значно більше:

– наявність правових повноважень щодо примусу до надання конфіденційних даних визначається правовою системою держави. Згідно з законодавством держав-учасниць ГУАМ, відмову від розкриття даних доступу до гаманця можна інтерпретувати як маніпулювання доказами, що провокуватиме висунення додаткових звинувачень. Проте низький рівень оперативності, характерний для такого підходу, разом з волатильністю електронних доказів, може стати суттєвою перешкодою для правоохоронних органів;

– відсутність гарантій щодо можливості копіювання інформації зловмисником чи його спільниками з метою відновлення контролю за арештованими активами після розкриття конфіденційних даних.

Тому на сьогодні найбільш оптимальним способом є взяття цифрової валюти під контроль шляхом її передачі на рахунок (гаманець) правоохоронних органів. Цей процес передбачає декілька етапів:

– визначення кількості цифрової валюти та/або гаманців, що підлягають арешту;

– забезпечення співробітництва обвинуваченого з правоохоронними органами чи встановлення контролю за гаманцем із використанням інших законних засобів. Необхідну суму переказують на контрольований державою гаманець з метою подальшої конфіскації та ліквідації;

– належне документування передачі активів;

– у разі неможливості співробітництва чи встановлення контролю за гаманцем необхідним є визначення на основі обмінного курсу вартості цифрової валюти, що підлягає арешту (у національній валюті) та застосування процедури вартісної конфіскації.

Звісно, вартісну конфіскацію можуть застосовувати і на початковому етапі, особливо у випадках, коли традиційний арешт і взяття під контроль неможливо здійснити з огляду на безпеку чи доцільність управління такими активами.

Крок 4. Управління активами

Однією з основних проблем для правоохоронних органів є управління вилученими активами, переданими під контроль держави. Оскільки право власності на майно, яке підлягає конфіскації, належить початковому власнику, то будь-які операції з такими активами повинні бути проведені з дотриманням законності. У цьому контексті будь-яка цифрова валюта сама по собі є найменш проблематичним аспектом, оскільки її віртуальна природа забезпечує відносну «фізичну» недоторканість. Однак така валюта (особливо криптовалюта)

залежить від коливань обмінного курсу, що може викликати труднощі в контексті потенційної конфіскації на користь держави. Відмінності у вартості на момент виявлення та фактичного арешту вимагатимуть перегляду кількісних і вартісних показників. Варто зауважити, що з урахуванням високого рівня доступності даних про обмінний курс цей процес не потребуватиме залучення експертів задля проведення відповідного аналізу.

У контексті забезпечення арешту активів як засобів учинення злочину одним із ключових питань є профілактичний характер цього заходу. Це передбачає, що такі засоби повинні бути вилучені з обігу. Хоча досі не зареєстровано жодного випадку арешту централізованих чи децентралізованих цифрових валют як злочинних засобів, може виникнути необхідність розміщення вилученої валюти (контенту гаманця) на портативному носії з метою ізоляції від віртуального середовища.

Аналогічний підхід застосовується до біткоїнів, вилучених як злочинних доходів і розміщених в контрольованому державою гаманці. У таких випадках доцільно ізолювати від віртуального середовища і гаманець, і його контент шляхом створення локальних файлів, збережених на портативному носії. Така необхідність зумовлена тим, що окрім бажання убезпечити конфісковані активи від маніпуляцій з транзакціями і майнінгом. Також є усвідомлення можливості непередбачуваних змін і втрат унаслідок недотримання вимог щодо використання, системних збоїв та кібератак.

Особливості проведення міжнародних розслідувань

Фінансові розслідування часто виходять за межі національних кордонів, тому важливо забезпечити своєчасне використання компетентними органами можливостей формального і неофіційного міжнародного співробітництва під час слідчих дій. Встановлення контактів на початковому етапі дасть слідчим змогу ознайомитись та засвоїти особливості іноземної правової системи та проблематику процесу отримання

додаткової інформації та формування загальної стратегії розслідування.

З урахуванням транскордонної природи Інтернет-мережі, яка є унікальним середовищем функціонування цифрових валют, міжнародне співробітництво постає важливим елементом розслідувань злочинів, пов'язаних із використанням цифрової валюти. Тому застосування наявних механізмів встановлення такого співробітництва повинно бути максимально ефективним і оперативним з огляду на волатильність, властиву електронним доказам і слідам злочинної діяльності у віртуальному просторі:

– співробітництво через міжнародні мережі, створені для виявлення злочинних доходів: Камденська міжвідомча мережа з повернення активів (CARIN), Ініціатива з повернення викрадених активів (StAR), яка є результатом партнерства між Світовим банком та Управлінням ООН з наркотиків та злочинності, а також спеціалізовані мережі з повернення активів (Глобальна мережа координаторів повернення активів – спільний StAR та Інтерпол);

– використання механізмів співробітництва між органами поліції (контактні центри 24/7, G8 – мережа підрозділів з розслідування інформаційних злочинів та національні бюро Інтерпол) з метою отримання оперативних даних, виконання запитів щодо забезпечення збереження інформації тощо для мінімізації бюрократичного перевантаження в межах стандартної процедури надання взаємної правової допомоги;

– встановлення через національну СФР контактів з аналогічними іноземними відомствами з поданням запитів через захищений канал Egmont Secure Web;

– використання формальних процедур обміну інформацією з Центральним органом (прокуратурою) – механізм обміну запитами в межах взаємної правової допомоги.

ДОДАТКИ

Додаток 1

Справа «Liberty Reserve»*

Резонансним розслідуванням серед злочинів із використанням цифрової валюти була справа «Liberty Reserve» (відмивання грошей у віртуальному середовищі). У травні 2013 р. Департамент юстиції США висунув обвинувачення Liberty Reserve (провайдеру грошових переказів з Коста-Ріки, охоплюючи сімох керівників та співробітників) у здійсненні незареєстрованої діяльності у вигляді грошових переказів і відмивання незаконних доходів на суму 6 млрд доларів США. Департамент казначейства США надав Liberty Reserve статус фінансової установи, яку, відповідно до розділу 311 Патріотичного акта США, було визначено як «об'єкт підвищеного ризику в контексті відмивання грошей» і ефективно відрізано від фінансової системи США.

Liberty Reserve було створено у 2006 р. для відвернення уваги та уникнення контролю регулюючих і правоохоронних органів. Діяльність системи була спрямована на сприяння зловмисникам у поширенні, зберігання та відмивання доходів, отриманих у результаті шахрайства з використанням кредитних карток, крадіжки особистих даних, інвестиційного шахрайства, хакерських атак, незаконного обігу наркотиків та дитячої порнографії. Вона надавала можливість проводити анонімні та складні для відслідковування фінансові операції. Масштаби діяльності Liberty Reserve вражають – більше мільйона клієнтів у всьому світі, охоплюючи 200 000 осіб у США і близько 55 млн зареєстрованих операцій.

---

* Manhattan U. S. Attorney Announces Charges Against Liberty Reserve, One of World's Largest Digital Currency Companies, and Seven of Its Principals and Employees for Allegedly Running A $ 6 Billion Money Laundering Scheme [Electronic resource] // US Department of Justice. – May 2013. – Mode of access: http://www.justice.gov/usao/nys/pressreleases/May13/LibertyReservePR.php?print=1. – Title from the screen.

У розпорядженні Liberty Reserve була власна цифрова валюта – Liberty Dollars, однак на практиці, перекази були прив'язані до фіатної валюти або золота.

Для того, щоб скористатися цифровою валютою Liberty Dollars, користувач мав відкрити рахунок на сайті Liberty Reserve. Вимагаючи (для прикриття) лише базові ідентифікаційні дані, Liberty Reserve не перевіряв їхню автентичність. Користувачі створювали рахунки на вигадані імена, зокрема й імена, які мали певне відношення до кримінального середовища («Хакерський рахунок», «Шахрай Джо»), і вказували неіснуючі адреси («вул. Підставна, 123», «Чудове місто Нью-Йорк»). Також Liberty Reserve зобов'язувала своїх користувачів проводити операції з депонування та зняття готівки через визначені обмінні пункти, які були або неліцензовані, або перебували в юрисдикціях зі слабкими режимами регулювання і контролю у сфері протидії відмиванню коштів. Не проводячи безпосередньо операцій з депонування та зняття готівки Liberty Reserve вдалося позбутися потреби збирати інформацію про користувачів, яка зазвичай необхідна під час здійснення банківських операцій чи інших видів фінансової діяльності. Після створення рахунку користувач міг проводити операції з іншими клієнтами шляхом переказу Liberty Dollars на чужі рахунки, підставні «комерційні» установи, які приймали Liberty Dollars як оплату. За додаткову «оплату конфіденційності» (75 центів США за кожну транзакцію) користувачі могли приховати номери власних рахунків у Liberty Reserve, унеможливлюючи процес відслідковування переказів. Дізнавшись про зацікавленість правоохоронних органів США цією діяльністю, Liberty Reserve «офіційно» перестав діяти на території Коста-Ріки, але продовжив роботу через низку підставних компаній, переказуючи мільйони до Австралії, Кіпру, Китаю, Гонконгу, Марокко, Росії, Іспанії.

Додаток 2

Справа «Mt.Gox»*

Mt.Gox була найпопулярнішою Bitcoin-біржею, яка розпочала свою діяльність в Токіо в липні 2010 році. Упродовж трьох років за її участі було укладено приблизно 70 % всіх угод з біткоїнами. Біржа оголосила про банкрутство в лютому 2014 р. після заяви про втрату майже 850 000 біткоїнів, які були власністю її клієнтів.

За словами представників Mt.Gox, усі проблеми були пов'язані з так званою гнучкістю транзакцій з використанням біткоїнів. Під час проведення такої транзакції в системі генерується важлива інформація, що містить суму надісланих біткоїнів, номери рахунків відправника й отримувача. Ідентифікаційний номер транзакції та її «унікальне» ім'я формується на основі цієї інформації. Однак деякі дані, які використовують для генерування ідентифікаційного номера транзакції, містяться в її незахищених частинах. У результаті існує можливість змінити ідентифікаційний код транзакції без необхідності авторизації відправником.

У такому разі не втрачаються важливі елементи, оскільки вся ключова інформація про операцію є надійно захищеною. Проте проблеми можуть виникнути, якщо відправник очікує побачити конкретний ідентифікаційний номер транзакції. Керівництво Mt.Gox повідомило, що транзакції в публічному реєстрі, згідно зі стандартною процедурою, повинні були фіксуватися під ідентифікаційними номерами. Якщо номери були відсутні (зловмисник самостійно їх змінював), то шахраї подавали скаргу про те, що операція не відбулася і система автоматично повторювала «незавершену» операцію, знову переказуючи визначену суму біткоїнів.

---

* The Guardian: «How a Bug in Bitcoin Led to Mt.Gox's Collapse» [Electronic resource]. – Mode of access: http://www.theguardian.com/technology/2014/feb/27/how-does-a-bug-in-bitcoin-lead-to-mtgoxs-collapse. – Title from the screen.

Гнучкість транзакцій є недоліком мережі Bitcoin і Mt.Gox, однак вона не може бути визнана відповідальною за втручання в операційні дані. Про існування такого недоліку відомо з 2011 р. і можливостей для виправлення цієї ситуації було достатньо, зокрема шляхом компенсації за допомогою програмного забезпечення, яке показує точний баланс та кількість операцій. У сучасній практиці втручання в дані та системи визначають як нетяжкі злочини в контексті цифрових валют. Водночас випадок з Mt.Gox демонструє, що наслідки таких злочинів можуть мати безпосередній вплив на віртуальний валютний ринок.

Додаток 3

Використання обмінного ресурсу з метою відмивання грошей*

У січні 2014 р. в міжнародному аеропорту Джона Ф. Кеннеді (м. Нью-Йорк) американські прокурори арештували Чарлі Шрема, відомого 24-річного шахрая, якого звинувачували в участі в злочинній змові з метою відмивання доходів на суму, що перевищувала 1 млн доларів США. Це були гроші користувачів онлайнового чорного ринку Silk Road (Шовковий шлях). Іншого підозрюваного – Роберта Файєлла – також було заарештовано за висунутим Офісом прокуратури Манхеттена аналогічним обвинуваченням: участь у злочинній змові з метою надання допомоги клієнтам сайту Silk Road для анонімного придбання незаконних товарів та об'єктів (від наркотиків до фальшивих паспортів).

Чарлі Шрем керував Bitinstant – Нью-Йоркським біткоїн-обмінником, який був одним із перших зареєстрований у Департаменті казначейства США. У 2013 р. компанія отримала 1,5 млн доларів США у вигляді інвестицій від Winklevoss Capital.

За даними прокуратури Ч. Шрем і Р. Файєлла продали користувачам сайту Silk Road більше 1 млн доларів США у вигляді електронних грошей. Так, 52-річний Р. Файєлла через сайт Silk Road керував «підпільним» біткоїн-обмінником, який здійснював продаж валюти для користувачів сайту з грудня 2011 до жовтня 2013 року. Після підтвердженого замовлення Р. Файєлла отримував валюту від компанії, локалізованої в м. Нью-Йорк, де Ч. Шрем був головним виконавчим директором, а потім продавав її користувачам з націнкою.

---

* Two Charged in Alleged Bitcoin-Laundering Scheme [Electronic resource] // The Wall Street Journal. – Mode of access: http://online.wsj.com/article/BT-CO-20140127-709257.html. – Title from the screen.

Інша компанія, не зафіксована у позові, надавала користувачам можливість для анонімного обміну готівки на біткоїни. Чарлі Шрем також виконував обов'язки compliance-менеджера цієї компанії, який відповідав за дотримання законодавства у сфері протидії відмиванню коштів.

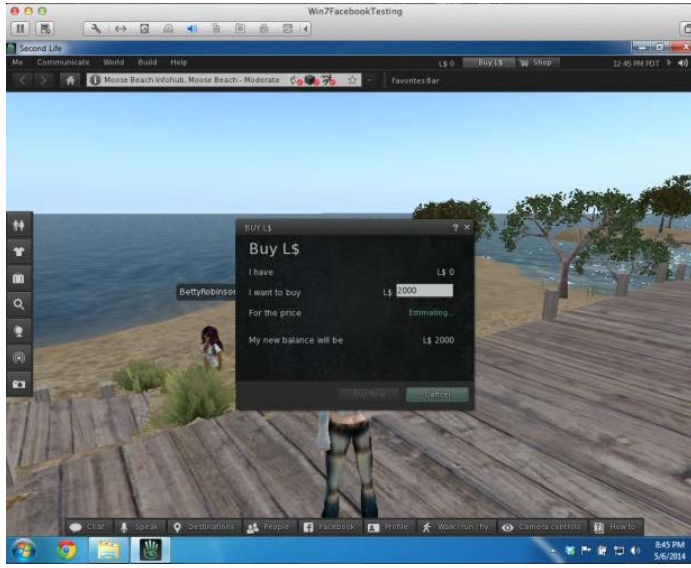
За даними позову, в обмін на винагороду Ч. Шрем виконував замовлення Р. Файєлли, знаючи, що валюта призначалася для користувачів Silk Road, які могли використати її для придбання наркотиків та оплати контрабанди. До того ж, Ч. Шрем надавав Р. Файєллі оптові знижки, маскуючи так замовлення іншого співзасновника його компанії, і не подавав відповідних звітів до правоохоронних органів у встановленому порядку.

Додаток 4

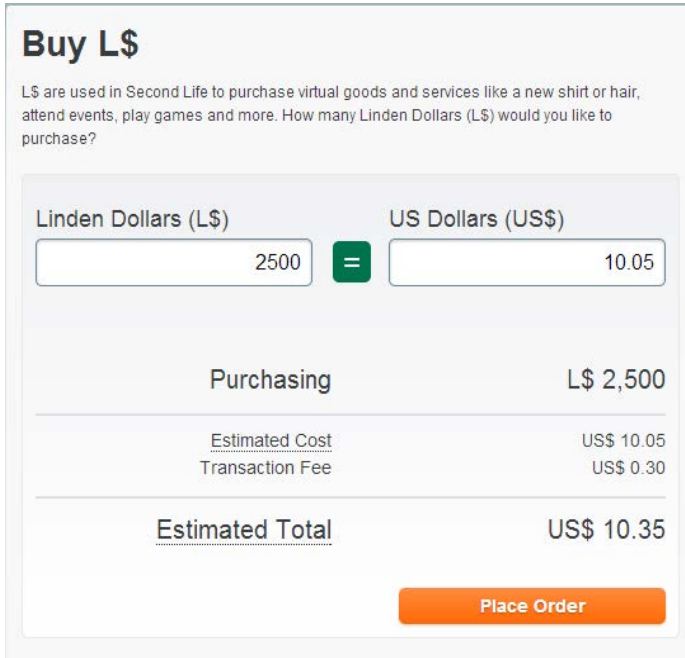
Придбання цифрової валюти (на прикладі Second Life Linden Dollars)

Цифрову валюту Second Life Linden Dollars можна придбати в пункті обміну LindeX або у віртуальному середовищі, використовуючи Second Life Viewer.

Для придбання Linden Dollars через Second Life Viewer достатньо натиснути кнопку «Buy L$» і визначити бажану суму Linden Dollars. Такий механізм налаштовується через веб-сайт Second Life.



Придбання та продаж цифрової валюти може також проходити через пункт обміну Linden безпосередньо на веб-сайті Second Life чи інший аналогічний сервіс. Необхідно вказати або бажану кількість Linden Dollars, або суму в доларах США, які будуть витрачені на придбання.



Паролі від акаунтів у Second Life неможливо відновити безпосередньо з Second Life Viewer. Однак їх можна отримати з програми щодо управління паролями. До того ж, завжди існує можливість, що ці паролі могли бути збережені веб-браузером. Інформація про кількість Linden Dollars, способи оплати та проведені операції зберігається разом із Second Life-акаунтом. Тому Linden Labs може розкрити таку інформацію за умови дотримання необхідних юридичних формальностей у найбільш прийнятний і зручний спосіб:

– прямий запит до Linden Labs щодо надання інформації про дані акаунта, які не є конфіденційними відповідно до умов надання послуг;

– використання поліцейських каналів (контактних центрів 24/7 для держав-учасниць Конвенції Ради Європи про боротьбу з кіберзлочинністю, мережі G8 чи національних бюро Інтерпол);

– процедура взаємної правової допомоги (через Генеральну прокуратуру чи Міністерство юстиції).

Додаток 5

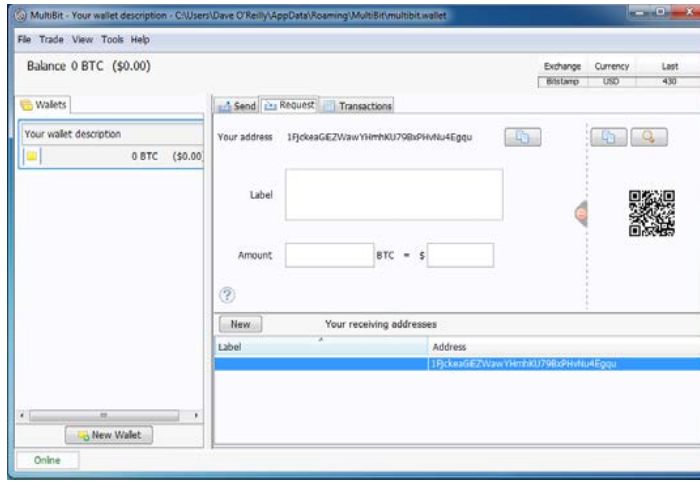
Функціонування біткоїн-гаманця

Розглянемо структуру функціонування програмного забезпечення Bitcoin – Multibit. Multibit – це спрощена версія біткоїн-гаманця для Windows, MacOS та Linux.

Встановлюємо додаток у директорію C:\Program Files (x86)\Multibit-0.5.18. Під час першого запуску Multibit створюється новий, пустий гаманець під назвою «multibit.wallet». Спочатку він не захищений паролем і розташований за адресою C:\Users\<user>\AppData\Roaming\ MultiBit\multibit.wallet, де «<user>» – це ім'я користувача, який увійшов до системи. Користувач може створити стільки гаманців, скільки забажає. Всі вони будуть зберігатись у папці «multibit.wallet».

Multibit буде створювати різні резервні копії створених і налаштованих гаманців у папку «<wallet name>-data», де <wallet name> – це назва конкретного гаманця. Папка резервного копіювання також зберігається в описаному каталогу даних.

Основний екран Multibit має такий вигляд.



Зліва подається список гаманців, які створив і налаштував користувач, з інформацією про наявну кількість біткоїнів. У правій частині наявні вкладки для переказу біткоїнів на інший гаманець, отримання валюти (охоплюючи обрану біткоїн-адресу реципієнта) і вкладка, що дає змогу переглянути всі проведені транзакції.

Користувач може створити необмежену кількість біткоїн-адрес для отримання переказів, використовуючи кнопку «New» у вкладці для отримання біткоїнів. Така адреса має вигляд буквено-цифрового рядка (наприклад: 1FjckeaGiEZWawYHmhKU79BxPHvNu4Egqu).

Файл «.wallet» містить приватні ключі, пов'язані з усіма ідентифікаторами біткоїн-гаманця, а також дані про транзакції, що стосуються всіх адрес. Файл зберігається у двійковому форматі та може бути відкритий за допомогою Multibit. Найпростіший спосіб перевірити зміст файлу «.wallet», знайденого на комп'ютері підозрюваного, – скопіювати директорію даних Multibit на комп'ютер, що використовується для криміналістичної експертизи, та відкрити за допомогою Multibit.

Усі транзакції мають певний зв'язок з біткоїн-адресами і зберігаються в ланцюгу блоків Bitcoin, які можна знайти в Інтернеті. Таким чином, інформація про біткоїн-адреси, знайдена в комп'ютері підозрюваного, може бути додатково опрацьована задля встановлення того, які саме транзакції передували і були здійснені після переказів з/на біткоїн-адреси, пов'язані з підозрюваним.

Варто зауважити, що неможливо за допомогою інформації, яка зберігається в Multibit, пов'язати біткоїн-адреси з IP-адресами чи іншими ідентифікаційними даними за винятком, біткоїн-адрес, які зберігаються у файлах налаштування Multibit та можуть мати відношення до інших файлів, що зберігаються в комп'ютері підозрюваного.

Паралельно з файлом «.wallet» можна знайти відповідний файл «.info», який буде містити всі адреси отримання і відправки біткойнів. Кожний рядок починатиметься з «receive» (отримання) чи «send» (відправлення). У кінці «.info»-файла можна також побачити розташування резервної копії гаманця.

ДЛЯ НОТАТОК / NOTES

Навчальне видання

ЧЕРНЯВСЬКИЙ Сергій Сергійович,
КРЖЕЧКОВСЬКИС Ігоріс,
ТАЦІЄНКО Валерій Вікторович та ін.

ДОСВІД КРАЇН ЄВРОПЕЙСЬКОГО СОЮЗУ ЩОДО ВИЯВЛЕННЯ ТА РОЗСЛІДУВАННЯ ВІДМИВАННЯ ЗЛОЧИННИХ ДОХОДІВ ІЗ ВИКОРИСТАННЯМ ЦИФРОВОЇ ВАЛЮТИ (КРИПТОВАЛЮТИ)

Методичні рекомендації

Редагування *А. О. Ласкова*
Комп'ютерна верстка *Я. В. Шумко*

Підписано до друку 25.01.2017. Формат 60х84/16. Папір офсетний.
Обл.-вид. арк. 5,25. Ум. друк. арк. 4,88.
Тираж 100 прим.

Друк:
ФО-П Поліщук О.В.
Свідоцтво суб'єкта видавничої справи ДК №2142 від 31.03.2005
07400, м. Бровари, вул. Незалежності, 2, кв. 148
тел. (044) 592-13-49