Худенко Д. М.,
т.в.о. начальника Департаменту
кримінального аналізу
Національної поліції України

ЗАБЕЗПЕЧЕННЯ ОПЕРАТИВНИХ ПРАЦІВНИКІВ ТА ІНСПЕКТОРІВ, ЯКІ ЗАЙМАЮТЬСЯ КРИМІНАЛЬНИМ АНАЛІЗОМ, ІНФОРМАЦІЄЮ ПРО ВІРТУАЛЬНІ АКТИВИ НА ОСНОВІ ПОЛІЦЕЙСЬКИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Верховною Радою України протягом останнього десятиліття зареєстровано більше 4 законопроєктів, пов'язаних із віртуальними активами або криптовалютами чи її похідними тощо. Було ухвалено закони, для цілей яких визначено поняття віртуальних активів [1], встановлено обов'язок декларування криптовалют [2] та ін. Як бачимо з попереднього твердження, законодавець допустив різні варіанти термінів щодо останніх сутностей або речей. Зауважимо, що з огляду на обсяг тез не будемо вдаватися у полеміку довкола термінології. Надалі будемо оперувати термінологією на основі чинного законодавства (п. 13 ч. 1 ст. 1 [1]) та наведемо факти й оціночні судження. І зосередимось на соціальному феномені цих речей в оперативно-розшуковій діяльності, кримінальному праві та процесі, суспільні відносини щодо яких склались та потребують подальшого правового врегулювання.

Відомо, що 11 червня 2020 року парламентом одержано черговий проєкт Закону України «Про віртуальні активи» № 3637. На думку авторів законопроєкту, його норми мають застосовуватися до правовідносин, що виникають у зв'язку з обігом віртуальних активів в Україні, визначати права та обов'язки учасників ринку віртуальних активів, засади державної політики у сфері обігу віртуальних активів [3].

У м. Києві у торговому центрі «Globus», неподалік входу до станції метро «Майдан Незалежності», розташований один із перших криптоматів. Компанія TripleA повідомила, що за минулий рік Україна посіла 1-ше місце у світі за відсотком населення, яке володіє криптовалютами [4]. Chainalysis Inc. провело дослідження допустимого приросту Bitcoin за 2020 рік, за результатами рейтингу якого виявилось, що Україна посіла 10-те місце серед 25 країн [5].

З огляду на такий невичерпний перелік фактів та оцінок для нас стає очевидним, що суспільні відносини щодо віртуальних активів чи криптовалют та їх похідних виникли, існують та набувають поширеності. Однак використання віртуальних активів у злочинній діяльності, значна їх волатильність, яка приховує спокусу швидкого збагачення та високі ризики майнових втрат вимагає переосмислення не лише законодавчих підходів до правового регулювання, але й наявного арсеналу засобів та джерел

інформації.

Науковий інтерес до різних аспектів проблем, пов'язаних із віртуальними активами в оперативно-розшуковій діяльності, кримінальному праві та процесі виявили у своїх працях В. Білинський, Р. Благута, О. Карапетян, С. Леськів, А. Лисенко, В. Носов, О. Юхно та інші вчені.

На нашу думку, за умови ухвалення згаданого законопроєкту та узгодження нормативно-правових актів із цим Законом для кримінальної поліції особливої актуальності набуде потреба у подальшому вдосконаленні відповідних оперативно-розшукових засобів. Одним із таких засобів є обліки у вигляді інформаційних підсистем. На практиці міжнародні партнери вже допомогли українській поліції з придбанням спеціального програмного забезпечення із відслідковування руху засобів у вигляді віртуальних активів, але нами ще не використано власний потенціал засобів поліції. Зокрема, не вирішено питання щодо забезпечення оперативних працівників та інспекторів, які займаються кримінальним аналізом, інформацією про віртуальні активі на основі наявних інформаційних ресурсів.

Треба констатувати, що на сьогодні жоден із поліцейських інформаційних ресурсів не містить полів, які дозволяють систематизувати інформацію про віртуальні активи, що стали предметом або засобом злочину. Не систематизовану інформацію складно піддавати будь-якому аналізу, у тому числі кримінальному. Така ситуація в інформаційно-аналітичному забезпеченні оперативно-розшукової діяльності та кримінального провадження є не бажаною та змушує її вирішити. Нами з'ясовано, що є поліцейські інформаційні ресурси, які містять інформацію про віртуальні активи та адреси їх гаманців. Ми маємо на увазі інформаційну підсистему інформаційного порталу Національної поліції України (далі – ІП ІПНП) «Єдиний облік». Дана підсистема містить відомості стосовно повідомлень про кримінальні та адміністративні правопорушення, надзвичайні ситуації та інші події, що надійшли технічними каналами зв'язку (п. 3 розд. ІІІ [6]). На жаль, у змісті її словників відсутні різновиди віртуальних активів. Це призводить до того, що надалі вибірка за певним критерієм є ускладненою, на неї доводиться витрачати зусилля декількох фахівців, а саме залучати представників підрозділу інформаційно-аналітичної підтримки. Особливо складно та довго робити вибірки, коли зустрічаються різні варіанти написання різновидів віртуальних актів, як-от: BTC або Bitcoin чи біткоїн, ETH, Ethereum або ефір чи ефірум тощо.

Зважаючи на вищевикладене, ми пропонуємо розглянути декілька варіантів часткового вирішення питання щодо забезпечення оперативних працівників та інспекторів, які займаються кримінальним аналізом, інформацією про віртуальні активі на основі власних інформаційних ресурсів. Вважаємо, що можливо проводити забезпечення на основі нової бази даних (інформаційної підсистеми) або ж через розбудову частини вже наявної підсистеми.

У першому випадку доведеться провести значно більший обсяг заходів впровадження. Наприклад, таким додатковим заходом є повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних.

У другому ж випадку таких заходів може бути менше, адже вбачається за можливе розбудувати частину вже наявної ІП ІПНП, що не потребує процедур повідомлення. Зокрема, такою базою даних (інформаційною підсистемою) поліції є «Єдиний облік» або «Річ».

Під час розробки проєкту технічного завдання або робочого проєкту треба передбачити створення таких полів з такими типами даних для засобу злочину: «дата та час транзакції» – дата та час; «адреса гаманця відправника» – текстовий; «вид віртуального активу (криптовалюти)» – словник; «сума транзакції віртуального активу» – число з комою із точністю до 10 знаків після коми; «тип гаманця» – словник; «виробник гаманця» – словник; «адреса гаманця отримувача» – текстовий та інші службові поля, які необхідні для ідентифікації введення, корегування та зв'язків даних.

Доцільно розглядати можливість формувати та підтримувати в актуальному стані словники на підставі відкритих джерел або за відомостями відповідного державного регулятора обігу віртуальних активів в Україні.

До того ж там, де це можна, буде раціональним виробити та застосувати відповідні правила перевірки правильності введення даних, що зменшить ризик помилок. Ще більш складними є питання оперативного внесення багатосимвольної і через це складної буквено-числової комбінації адреси та зазначення хешу транзакції. Вирішення цього аспекту розбудови може відбутись, наприклад, за допомогою сканування відповідного QR-коду адреси.

Звісно, виникнуть й інші додаткові питання, які потрібно буде вирішувати, але вищенаведене ілюструє одну з ідей забезпечення оперативних працівників та інспекторів, які займаються кримінальним аналізом, інформацією про віртуальні активі на основі власних інформаційних ресурсів.

Вважаємо, що у такий спосіб можливо не лише систематизувати та оптимізувати використання інформацією про віртуальні активі на основі власних інформаційних ресурсів, але й користати її у ролі відкритих даних для створення публічного інформаційного ресурсу або для розширення функціоналу програмного забезпечення, яке допомагає відслідковувати рух віртуальних активів.

Також разом з розглянутим напрямом забезпечення оперативних працівників та інспекторів, які займаються кримінальним аналізом, інформацією про віртуальні активи на основі власних інформаційних ресурсів, перспективною вважаємо роботу поліції над законодавчими ініціативами щодо інформаційно-аналітичного забезпечення оперативно-

розшукової діяльності та кримінального провадження внаслідок змін законопроєкту № 3637 у частині зберігання інформації, яка супроводжує переказ віртуальних активів, розширення її змісту та доступу до неї.

Бібліографічні посилання

1. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення : Закон України від 06.12.2019 р. № 361-IX. URL: https://zakon.rada.gov.ua/laws/show/361-20#n833
2. Про внесення змін до деяких законодавчих актів України щодо забезпечення ефективності інституційного механізму запобігання корупції : Закон України від 02.10.2019 р. № 140-IX. URL: https://zakon.rada.gov.ua/laws/show/140-20#n389
3. Про віртуальні активи : Проєкт Закону України № 3637. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=69110&pf35401=529256. Назва з екрану.
4. How many crypto owners in Ukraine? URL: https://triple-a.io/crypto-ownership-ukraine
5. Bitcoin Gains by Country: Who Benefited the Most from the 2020 Boom? URL: https://blog.chainalysis.com/reports/bitcoin-gains-by-country-2020.
6. Про затвердження Положення про інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України» : наказ МВС від 03.08.2017 р. № 676. URL: https://zakon.rada.gov.ua/laws/show/z1059-17#Text

Чобану Г.,
доктор экономических наук,
научный сотрудник Национального
научно-исследовательского института
труда и социальной защиты
Бухарестского университета
«ARTIFEX»

НЕОБХОДИМОСТЬ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ И РАСШИРЕНИЯ СПЕЦИАЛИЗАЦИИ В СОВРЕМЕННЫХ УСЛОВИЯХ КРИЗИСА ЭКОНОМИЧЕСКОГО И СОЦИАЛЬНОГО РАЗВИТИЯ

В нынешних условиях экономического развития, быстрой цифровизации всех отраслей общества и экономики, а также в условиях пандемического кризиса Covid-19 необходимость обеспечения информационной безопасности, кибербезопасности становится гораздо более необходимой и значительно более острой. Необходимо адаптироваться к требованиям кибербезопасности как государственных, так и частных организаций, которые в значительной степени выравнивают ее с экранами в связи с развитием информационных систем в последние десятилетия.