УДК 343.98:341.322.5
DOI: 10.31733/15-03-2024/2/69-71

Вадим БОЛГАРЕНКО
курсант ННІ права та підготовки
фахівців для підрозділів
Національної поліції

Віталій ТЕЛІЙЧУК
професор кафедри
оперативно-розшукової діяльності
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук,
старший науковий співробітник, доцент

БЛОКЧЕЙН-АНАЛІТИКА ЯК СУЧАСНИЙ ІНСТРУМЕНТ В РОЗСЛІДУВАННІ ВОЄННИХ ЗЛОЧИНІВ

В сучасному світі комп'ютер відіграє ключову роль у житті людей. Він використовується для спілкування, зберігання, створення, збору, обробки та використання інформації в усіх сферах діяльності. Бурхливий розвиток Інтернету як постачальника товарів та послуг, а також сфери грошового обігу призвів до зростання кількості шахрайств, скоєних з його допомогою. З огляду на вимоги законодавства України, зокрема Конституції України, Кримінального та Кримінального процесуального кодексів, законів України «Про Національну поліцію» та «Про оперативно-розшукову діяльність», актуальним завданням стає суттєве покращення діяльності правоохоронних органів щодо запобігання, виявлення та ефективного досудового розслідування цих злочинів в умовах воєнного стану [1].

Блокчейн – це технологія, яка в останні роки здобула велику популярність. Вона використовується для збереження даних у вигляді ланцюжка блоків, де кожен блок містить інформацію про певну подію або транзакцію. Одними з найважливіших характеристик блокчейну є безпека та надійність. Ця технологія може бути особливо корисною в умовах воєнного стану, коли збереження та передача інформації є критично важливим завданням. Блокчейн-аналітика дозволяє відстежувати переміщення криптовалюти, пов'язаної з злочинною діяльністю. Це є важливим в умовах воєнного конфлікту, де фінансування терористичних організацій та інших злочинних груп може бути приховано. Крім того, подібна технологія допомагає правоохоронцям ідентифікувати та розслідувати злочинні схеми.

Наразі блокчейн-технології активно використовуються для розслідування кіберзлочинів. Як приклад, з початку 2022 року поліція Канади та підрозділ кіберполіції України спільно з Chainalysis відкрили центр криптовалютних розслідувань, який працюватиме над розкриттям злочинів з використанням криптовалюти та блокчейну, крім того, завдяки співпраці із Crystal Blockchain вдалося зібрати доказову базу протиправної діяльності фігурантів, які фінансово підтримують російську армію чи інші незаконні збройні формування ,та встановити понад 40 причетних осіб [2; 3]. Блокчейн-аналітика – це потужний інструмент, який може допомогти правоохоронним органам розслідувати злочини більш ефективно та точно. Правоохоронні органи в усьому світі інвестують в розвиток своїх можливостей блокчейн-аналітики, оскільки вони розуміють її потенціал для боротьби з різними видами злочинності. Так, подібна аналітика допомогла ООН встановити факт того, що Північна Корея викрала криптовалюту на суму понад 50 мільйонів доларів і використовує її для фінансування своєї ракетної програми, оскільки зазнала обмежень через санкції та не має інших можливостей [4].

Блокчейн-аналітика дозволяє відстежувати переміщення криптовалюти, пов'язаної з злочинною діяльністю, включаючи тероризм, відмивання грошей, торгівлю наркотиками та кіберзлочинність. Завдяки їй правоохоронці можуть ідентифікувати та розслідувати злочинні схеми, а також конфіскувати криптовалюту, здобуту злочинним шляхом. Блокчейн-аналітика може використовуватися для виявлення підозрілих транзакцій, які можуть свідчити про злочинну діяльність. Алгоритми аналітики відстежують аномальні патерни транзакцій, моніторять поведінку користувачів та ідентифікують ризиковані гаманці. Крім того, дані блокчейну можуть використовуватися як докази у кримінальних провадженнях. Така

інформація з блокчейну, як записи транзакцій, адреси гаманців тощо, може бути представлена у суді, щоб підтвердити причетність особи до злочину.

На нашу думку, до основних переваг використання блокчейн-аналітики належить точність, прозорість, швидкість та ефективність. Блокчейн забезпечує прозорість та незмінність даних, що ускладнює фальсифікацію інформації. Подібна технологія допомагає зробити розслідування злочинів більш економним та ефективним. Завдяки аналітиці блокчейну дані про транзакції можна отримати значно швидше, ніж за допомогою традиційних методів. Алгоритми аналітики постійно вдосконалюються, що робить їх все більш точними та надійними.

На жаль, існує безліч правових та регуляторних питань, пов'язаних з використанням блокчейн-технологій в розслідуванні злочинів. Сам Закон України «Про віртуальні активи» [5] досі не набрав чинності, через що виникає колізія – ми не можемо конфіскувати віртуальні активи через те, що вони досі не визнані благом. Тобто наразі дозволено лише здійснювати аналітику та встановлювати сам факт того, що діяння відбулося, але притягнути особу до кримінальної відповідальності набагато складніше. Незважаючи на ці виклики, блокчейн-аналітика стає все більш важливим інструментом у боротьбі зі злочинністю.

Зараз вводяться системи AML («Протидія відмиванню грошей») та CFT («Боротьба з фінансуванням тероризму»). AML – це процедура ідентифікації осіб, які використовують криптовалюту. Після отримання інформації вона перевіряється та зберігається. Інформація про користувача містить дані про доходи та витрати. Цю процедуру проводять постійно, щоб запобігти відмиванню грошей, фінансуванню терористичних організацій, створенню зброї масового знищення, спонсорству злочинних організацій та іншим негативним явищам. AML збирає інформацію не лише про користувача, але й про його статок, доходи та витрати. CFT – це дотримання комплексу заходів та дій, які заважають тероризму та навіть його існуванню як явища у цілому [6].

Міжнародна група з протидії відмиванню брудних грошей (далі – FATF) – це міжурядова організація, заснована у 1989 році Великою вісімкою. Основна мета FATF – боротьба з відмиванням грошей та фінансуванням тероризму (з 2001 року) та забезпечення виконання стандартів AML/CFT. Незважаючи на те, що FATF може тільки надавати рекомендації, її вплив дуже великий. Організація може проводити взаємні перевірки країн-членів, щоб перевірити прогрес у виконанні ними рекомендацій. Одним із інструментів FATF є «заклик до дії», або чорний список. Цей список містить країни з високими фінансовими ризиками та країни, які спонсорують тероризм. Країни, які потрапляють до цього цей списку, можуть зазнати економічного тиску. Для того щоб уникнути потрапляння до списку або вийти з нього, уряди країн здійснюють певні заходи для виконання вимог FATF та відповідних регуляцій AML і CFT.

Отже, країни, які потрапляють до чорного списку FATF, мають складну економічно-правову ситуацію, високий ризик відмивання грошей або спонсорують тероризм, такі як Куба, Іран, Північна Корея та Сирія. Щодо деяких країн, зокрема Ірану, Північної Кореї та М'янми, FATF закликає застосовувати жорсткі санкції, щоб змусити їх дотримуватись вимог. Ці країни мають значні проблеми у своїй антивідмивальній системі та фінансовій системі щодо відповідності міжнародним стандартам AML і CFT.

росія була включена до цього списку через ряд причин, зокрема величезні фінансові ризики, початок конфлікту, систематичні порушення законів війни та прав людини, численні випадки військових злочинів, акти тероризму та їх фінансування. Включення до чорного списку сприятиме позбавленню російською військовою машиною фінансування. Проте російська влада не лише відмиває гроші, але і легалізує це, і стандарти AML та CFT у цій країні практично відсутні [7; 8].

Блокчейн-аналітика виявляється надзвичайно потужним інструментом у сучасних розслідуваннях злочинів. Вона дозволяє правоохоронним органам ефективно виявляти та розслідувати порушення, пов'язані з криптовалютами та блокчейн-технологіями. Завдяки блокчейн-аналітиці правоохоронці можуть точно відстежувати рух криптовалютних коштів, що допомагає виявити та припинити фінансові злочини, включаючи відмивання грошей та тероризм. Переваги цього інструменту полягають у його точності, прозорості, швидкості та ефективності, що робить його незамінним у боротьбі зі злочинністю.

1. Телійчук В., Горілик Д. Оперативно-розшукова протидія шахрайству, що здійснюється через мережу Інтернет. *Міжнародний науково-практичний правовий журнал «Legea si Viata»*. 2019. № 12 (336). С. 105–110.

2. Блокчейн на службі закону: поліція та Chainalysis в одній команді. *GNcrypto.* URL :

https://gncrypto.news/ua/news/blockchain-serving-the-law-police-and-chainalysis-join-forces/.

3. Кіберполіція у співпраці з компанією Crystal Blockchain ефективно протидіє шахрайству з використанням віртуальних активів. *Кіберполіція.* URL : https://cyberpolice.gov.ua/news/kiberpolicziya-u-spivpraczi-z-kompaniyeyu-crystal-blockchain-efektyvno-protydiye-shaxrajstvu-z-vykorystannyam-virtualnyx-aktyviv-205/.

4. North Korea stealing cryptocurrency to develop missile programme. *THE TIMES*. URL : https://www.thetimes.co.uk/article/north-korea-stealing-cryptocurrency-to-develop-missile-programme-un-says-sm0rh3pbl.

5. Про віртуальні активи : Закон України від 17.02.2022. URL : https://zakon.rada.gov.ua/laws/show/2074-20#Text.

6. Як криптовалюта допомагає фінансувати тероризм та як цього уникнути. *SPEKA.* URL : https://speka.media/yak-kriptovalyuta-dopomagaje-finansuvati-terorizm-ta-yak-cyogo-uniknuti-p1dg5p.

7. FATF Statement on the Russian Federation. *FATF.* URL : https://www.fatf-gafi.org/en/publications/Fatfgeneral/fatf-statement-russian-federation.html.

8. Ukraine calls on FATF to blacklist russia as ties with North Korea and Iran strengthen. *Government portal.* URL : https://www.kmu.gov.ua/en/news/ukraina-zaklykaie-fatf-vnesty-rosiiu-do-chornoho-spysku-na-foni-posylennia-zviazkiv-z-pivnichnoiu-koreieiu-ta-iranom.

УДК 343.98:343.344
DOI: 10.31733/15-03-2024/2/71-72

Олександр БОНДАРЕНКО
курсант ННІ права та підготовки
фахівців для підрозділів
Національної поліції

Володимир ВАРАВА
доцент кафедри
оперативно-розшукової діяльності
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук, доцент

ПРОТИДІЯ КРИМІНАЛЬНИМ ПРАВОПОРУШЕННЯМ В УМОВАХ ВОЄННОГО СТАНУ З ВИКОРИСТАННЯМ МЕТОДІВ ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ. ПРОТИДІЯ НЕЗАКОННОМУ ОБІГУ ЗБРОЇ

Збройна агресія російської федерації проти України 24 лютого 2022 р. зумовила введення воєнного стану на всій території країни. Це, в свою чергу, призвело до значного зростання ризиків та масштабів незаконного обігу зброї, боєприпасів та вибухових речовин. Незаконне володіння зброєю становить серйозну загрозу для життя та безпеки громадян, а також дестабілізує суспільство в цілому.

В умовах воєнного стану проблема незаконного обігу зброї набуває особливої гостроти. Збільшення доступності зброї, а також психологічна напруга та дестабілізація суспільства створюють сприятливі умови для скоєння тяжких кримінальних правопорушень.

Встановлено, що основними каналами незаконного обігу зброї в умовах воєнного стану є: збройні формування та правоохоронні органи: крадіжки, розкрадання, хабарництво; зони бойових дій: втрата зброї під час бойових дій, несанкціоноване вивезення з окупованих територій; чорний ринок: контрабанда, перепродаж зброї, викрадення з приватних володінь.

Розроблено комплекс заходів ОРД та НСРД, спрямованих на протидію незаконному обігу зброї в умовах воєнного стану, які включають: розвідувальну діяльність: виявлення каналів постачання зброї, осіб, причетних до її незаконного обігу, місць зберігання та збуту; контрольну закупівлю зброї: документування злочинної діяльності; огляд місця події: вилучення зброї, боєприпасів та вибухових речовин, фіксація слідів злочину; спостереження за особами, підозрюваними в незаконному обігу зброї; проведення негласних слідчих (розшукових) дій: контроль телефонних переговорів, зняття інформації з технічних каналів зв'язку [1, с. 12].

В умовах воєнного стану проблема незаконного обігу зброї становить серйозну загрозу для життя та безпеки громадян. Розроблений комплекс заходів ОРД та НСРД може