УДК 342.951
DOI https://doi.org/10.32782/2524-0374/2021-12/82

КРИМІНОЛОГІЧНІ РИЗИКИ ОБІГУ КРИПТОВАЛЮТ

THE CRIMINOLOGICAL RISKS OF CRYPTOCURRENCY CIRCULATION

Бохенко В.М., старший науковий співробітник
Український науково-дослідний інститут спеціальної техніки та судових експертиз Служби безпеки України

Статтю присвячено висвітленню кримінологічних ризиків обігу криптовалют. У сучасному світі спостерігається динамічне поширення та розвиток у глобальних масштабах криптовалют як сучасних фінансово-економічних інструментів на основі технології блокчейн. Поряд із динамічним розвитком передових інформаційних технологій та прагненням держави до суцільної цифрової трансформації всіх сфер суспільного життя цифровий прогрес удосконалює також й інструменти для здійснення кримінальних правопорушень, значно збільшуючи їх кількість. Оскільки все ще в багатьох країнах світу правовий статус криптовалют законодавчо не визначений, все частіше з'являються злочинні посягання, пов'язані з обігом криптовалют, які отримали системний характер.

Метою статті є розгляд кримінологічних ризиків обігу криптовалют та формування на підставі їх аналізу методологічних засад удосконалення правоохоронної діяльності щодо розслідування кримінальних правопорушень, пов'язаних із криптовалютами. Акцентовано, що світова статистика кримінального обігу наркотиків, вогнепальної зброї, порнографії, заборонених послуг з використанням криптовалюти не ведеться, проте згідно з даними експертів саме віртуальні активи використовується криміналітетом як платіжний засіб.

Проведено аналіз оприлюдненої доповіді ФАТФ, яка тематично присвячена використанню цифрових валют як інструмента для можливого фінансування тероризму. Окреслено засади міжнародної політики захисту глобальної фінансової системи від злочинного відмивання грошових коштів, запобігання будь-яким проявам фінансування тероризму з використанням криптовалют. Розглянуто деякі аспекти практики правоохоронної діяльності щодо розслідування злочинів, які скоєні з використанням криптовалют. Розкрито зміст та особливості проведення технологічного прийому на базі технології блокчейн під назвою «Атака 51%». Підсумовано доцільність розроблення криміналістичної методики протидії кримінальним посяганням з використанням криптовалюти. Така криміналістична методика має базуватися на основних засадах криптовалют, до яких відносяться: децентралізація їх випуску (емісії); відсутність технічних можливостей контролю обігу; анонімність осіб, які здійснюють трансакції з криптовалютою; відсутність адміністративно-територіальних обмежень для створення та використання криптовалюти. Під час розслідування злочинів з використанням криптовалют правоохоронним органам необхідно мати відомості про умови, порядок обігу криптовалют, особливості здійснення трансакцій, про специфіку функціонування криптовалютних бірж.

Акцентовано, що успішне розслідування та розкриття злочинів у сфері обігу криптовалют також потребує наявності спеціальних знань та сучасного програмного забезпечення в арсеналі на озброєнні правоохоронців. Важливим залишається проведення навчальних тренінгів та стажування правоохоронців з метою набуття практичних вмінь та навичок, спеціальних знань під час розслідування злочинів, пов'язаних із криптовалютами. На підставі проведеного дослідження узагальнено, що кримінологічні ризики, пов'язані з обігом криптовалюти, та передумови до поширення використання цих цифрових рішень у злочинному середовищі мають комплексний характер. Пропонується з метою збільшення кількості розкритих злочинів, що вчиняються з використанням криптовалют, прискорити схвалення правових засад, які мають урегулювати криптовалюти та розроблення методологічних основ і рекомендацій щодо особливостей розслідування цієї категорії кримінальних правопорушень. Також аргументовано, що вітчизняним правоохоронним органам необхідно налагодити комплексну взаємодію з криптовалютними компаніями та біржами з метою блокування будь-якої незаконної та протиправної діяльності у блокчейн-платформах. Вирішення цієї проблеми має комплексний характер та вимагає розроблення сучасної тактики і стратегії правоохоронної діяльності, спрямованої на результативне запобігання використанню злочинцями нових сучасних фінансових механізмів. Визначено шляхи подальшого вдосконалення правоохоронної діяльності щодо збільшення кількості розкритих злочинів, які вчиняються з використанням криптовалют.

Ключові слова: технологія блокчейн, цифрова економіка, криптовалюта, віртуальні активи, трансакція, злочинність, правоохоронна діяльність.

The article is devoted to the coverage of criminological risks of cryptocurrency circulation. In today's world there is a dynamic spread and development on a global scale of cryptocurrencies as modern financial and economic instruments based on blockchain technology. Along with the dynamic development of advanced information technologies and the state's desire for continuous digital transformation of all spheres of public life, digital progress also improves the tools for committing criminal offenses, significantly increasing their number. As the legal status of cryptocurrencies is still not legally defined in many countries around the world, there are more and more criminal encroachments related to the circulation of cryptocurrencies that have become systemic.

The purpose of the article is to consider the criminological risks of cryptocurrency circulation and the formation on the basis of their analysis of methodological principles for improving law enforcement activities to investigate criminal offenses related to cryptocurrencies. It is emphasized that the world statistics on criminal trafficking in drugs, firearms, pornography, illicit services using cryptocurrency are not kept, but according to experts, only virtual assets are used by crime as a means of payment.

An analysis of the published FATF report, which is thematically devoted to the use of digital currencies as a tool for possible terrorist financing. The principles of the international policy of protection of the global financial system from criminal money laundering, prevention of any manifestations of terrorist financing with the use of cryptocurrencies are outlined. Some aspects of law enforcement practice in the investigation of crimes committed with the use of cryptocurrencies are considered. The content and features of the technological reception based on blockchain technology called "Attack 51%" are revealed.

The expediency of developing a forensic method of combating criminal encroachment with the use of cryptocurrency is summarized. Such forensic methodology should be based on the basic principles of cryptocurrencies, which include: decentralization of their issuance (issue); lack of technical capabilities to control circulation; anonymity of persons who make transactions with cryptocurrency; lack of administrative and territorial restrictions on the creation and use of cryptocurrency. When investigating crimes using cryptocurrencies, law enforcement agencies need to have information about the conditions, the order of circulation of cryptocurrencies, the peculiarities of transactions, the specifics of the cryptocurrency exchanges. It is emphasized that the successful investigation and detection of crimes in the field of cryptocurrency circulation also requires special knowledge and modern software in the arsenal of law enforcement. It is important to conduct training and internships for law enforcement officers in order to acquire practical skills, special knowledge in the investigation of crimes related to cryptocurrencies. Based on the study, it is concluded that the criminological risks associated with cryptocurrency circulation and the preconditions for the spread of the use of these digital solutions in a criminal environment are complex. It is proposed to accelerate the adoption of legal bases for cryptocurrencies and to develop methodological bases and recommendations on the specifics of the investigation of this category of criminal offenses in order to increase the number of detected crimes committed using cryptocurrencies. It is also argued that domestic law enforcement agencies need to establish comprehensive cooperation with cryptocurrency companies and exchanges in order to block any illegal and illegal activities in blockchain platforms. The solution to this problem is complex and requires the development of modern tactics and strategies for law enforcement activities aimed at effectively preventing the use of new modern financial mechanisms by criminals**.** The directions of further improvement law enforcement activities to increase the number of detected crimes committed using cryptocurrencies have been identified.

Key words: blockchain technology, digital economy, cryptocurrency, virtual assets, transaction, crime, law enforcement.

Постановка проблеми. В умовах поширення пандемії у світових масштабах відбувся вимушений перехід на дистанційний режим роботи, що призвело до збільшення кількості кримінальних правопорушень, які скоєні з використанням передових інформаційних технологій та у сфері цифрової економіки. Пандемія загострила та прискорила негативні тенденції – зростання глобального суперництва, протекціонізму та популізму, призвела до зменшення мобільності населення і міжлюдських контактів, проте сприяла появі нових форм та методів поширення злочинності, в тому числі й у віртуальному просторі. На цьому фоні спостерігається динамічне поширення та розвиток у глобальних масштабах криптовалют у світі як сучасних фінансово-економічних інструментів на основі технології блокчейн, що у свою чергу провокує злочинців незалежно від їхнього територіального розміщення та юрисдикцій держав учиняти кримінальні правопорушення, реалізовувати злочинні схеми, пов'язані з обігом криптовалют. Шахрайства з платіжними картками, крадіжки грошей із криптогаманців, розповсюдження комп'ютерних вірусів, викрадення хакерами персональних даних громадян, онлайн-торгівля наркотиками, поширення протиправного контенту – це лише невелика частина злочинів, які має розслідувати та припиняти правоохоронна система в сучасних умовах.

Поряд із динамічним розвитком передових інформаційних технологій та прагненням держави до суцільної цифрової трансформації всіх сфер суспільного життя цифровий прогрес удосконалює також й інструменти для здійснення кримінальних правопорушень, значно збільшуючи їх кількість. Тобто у зв'язку зі сталим розвитком інноваційних технологій актуальними вбачаються питання щодо розроблення алгоритмів протидії використанню криптовалют у протиправних діях і посилення кримінальної відповідальності за такі дії, впровадження у правоохоронну діяльність сучасних методик запобігання кримінальних правопорушенням, пов'язаним з обігом криптовалюти.

У багатьох країнах світу правовий статус криптовалют все ще законодавчо не визначений, у зв'язку з чим в умовах популяризації нових платіжних засобів все частіше з'являються злочинні посягання, пов'язані з обігом криптовалют, які отримали останнім часом масовий та системний характер. Загалом злочинці, використовуючи криптовалюту як платіжний засіб, здійснюють чималі грошові перекази через мережу Інтернет, таким чином ігнорують використання звичайних фінансових систем, спричиняючи колосальні економічні збитки, посягаючи на основи національної безпеки тієї чи іншої держави. Враховуючи викладене, актуальним та своєчасним є розгляд кримінологічних ризиків обігу криптовалюти та її використання у злочинних цілях.

Результати аналізу наукових публікацій. Проблемні питання розвитку криптовалют, змісту та особливостей їх обігу досліджували у своїх наукових працях: С. Волосович [1], В. Іванюк [2], І. Доронін [3], О. Драчов [4], А. Кісіль та В. Пряміцин [5], І. Краснова [6], С. Мерінова [7] та інші. Кримінологічні засади запобігання злочинній діяльності з використанням криптовалют і технології блокчейн певним чином розглядали у своїх наукових працях: Р. Благута та А. Мовчан [8], М. Гребенюк, А. Черняк [9], Д. Казначеєва і А. Дорош [10]. Але кримінологічні ризики обігу криптовалют вказані фахівці не висвітлювали, що посилює актуальність наукової статті.

Метою статті є розгляд кримінологічних ризиків обігу криптовалют та формування на підставі їх аналізу методологічних засад удосконалення правоохоронної діяльності щодо розслідування кримінальних правопорушень, пов'язаних із криптовалютами.

Виклад основного матеріалу. Особливу роль у швидкому зростанні нових видів кіберзлочинності відіграють мережеві технології формування грошових потоків між економічними утвореннями різного роду, включаючи міжнародні організовані злочинні товариства та угрупування. При цьому у відповідних суб'єктів виникають нові сприятливі можливості для маскування своєї злочинної діяльності та покриття джерел її фінансування за допомогою сучасних інформаційних технологій, включаючи алгоритми розподіленого зберігання та доступу до зашифрованої інформації типу блокчейн. Під час переведення криптовалют у готівкові кошти обов'язково встановлюється ринкова вартість криптовалюти або її ринковий курс. Зручність використання криптовалют зумовлюється також високою швидкістю внутрішньомережевих трансакцій та невеликими часовими затратами на весь процес здійснення угоди за схемою «реклама-гроші-товар» у цілому. Комфортні умови операцій із цифровими активами для користувачів також надає той факт, що для криптовалют не мають значення наявність національних, територіальних або державних кордонів, при цьому розрахунки в криптовалюті можливо здійснювати як всередині країни, так і за кордоном. При цьому не має потреби узгоджувати з державними органами проведення трансакцій, отримувати дозволи на їх здійснення, звітувати за результатами їх проведення тощо. У таких умовах формуються нові завдання перед правоохоронними органами, які в межах компетенції та відповідно до своєї функціональності мають виявляти, запобігати та припиняти такі злочини, здійснювати відповідне розслідування таких кримінальних проявів.

Нині світова статистика кримінального обігу наркотиків, вогнепальної зброї, порнографії, заборонених послуг з використанням криптовалюти не ведеться, проте згідно з даними експертів саме криптовалюта є засобом розрахунків у 95% операцій. При цьому спостерігаються принципово нові кримінологічні тенденції розвитку Даркнету: поступова специфікація окремих кримінальних сервісів та покращення їхніх технологічних характеристик, поступова монополізація криптовалютного ринку тощо. На цьому фоні актуальним для світової спільноти залишається питання протидії легалізації (відмиванню) доходів, отриманих злочинним шляхом з використанням криптовалюти, протидії фінансуванню тероризму.

Financial Action Task Force (ФАТФ) – незалежний міжурядовий орган, який здійснює розроблення світової політики захисту глобальної фінансової системи від злочинного відмивання грошових коштів, запобігання будь-яким проявам фінансування тероризму тощо. В оприлюдненій доповіді цієї структури під назвою «Нові терористичні ризики» [11] присутній розділ, присвячений цифровим валютам як інструменту для можливого фінансування тероризму та структурований аналіз кіберзлочинності. Проте в доповіді зазначається, що міжнародні терористичні угрупування передусім використовують традиційні методи: приватні пожертви, самофінансування, злочинну діяльність щодо збору коштів. Статистика переконливо засвідчує, що нові технології оплати являють собою певну уразливість для терористів. Проте цифрові валюти є об'єктом зацікавленості терористів, оскільки вони пропонують анонімність трансакцій та користувачів, гарантують швидкість оформлення угод, низьку волатильність та надійність. Правоохоронні органи країн – членів ФАТФ акцентували увагу на тому, що деякі терористичні вебсайти використовують біткойн для прийому пожертв на свої злочинні потреби. Також були зафіксовані непоодинокі випадки придбання зброї терористами за віртуальну валюту. Навіть один із підрозділів терористичного угрупування «Ісламської Держави» використовує біткойн як форму розрахунків. У доповіді достеменно висвітлено випадок, коли підліток із Вірджинії (США) Алі Шукрі Аміна, якого була зарештовано за використання Twitter з метою проведення навчальних інструктажів терористів, як використовувати біткойн, мав аудиторію прихильників понад 4 тис. осіб.

Як уже зазначалося, правова неурегульованість і невизначеність статусу криптовалют у більшості країн світу значно ускладнює не тільки нагальну оцінку її використання під час кваліфікації таких дій, але й також гальмує розкриття та розслідування злочинів, під час скоєння яких використовується криптовалюта або як предмет злочину, або як засіб скоєння кримінального правопорушення. Таким чином, з метою ефективної протидії злочинності у сфері обігу криптовалют правоохоронцям необхідно більш детально і всебічно опанувати процеси та явища, які можуть мати опосередкований або виражений негативний вплив на обіг криптовалют. Правоохоронці в переважній більшості держав світу намагаються ідентифікувати власників рахунків віртуальної валюти й у межах оперативно-технічних та аналітичних можливостей створюють бази даних уже з відомими власниками криптогаманців. Одночасно у світовій практиці не є злочином операції, спрямовані на переведення криптовалюти в готівкові кошти. Тобто саме слідство має довести, що за допомогою таких операцій відбувається легалізація доходів, грошей або майна, які здобуті злочинним шляхом. З метою отримання необхідних доказів слід ураховувати, що для переведення криптовалюти в готівку зазвичай використовуються криптовалютні біржі та посередники, які мають аккаунти в криптовалютних системах, а також і звичайні банківські рахунки з безготівковими грошовими коштами. Саме через таких посередників слідство може вийти на тих осіб, які зверталися до них за допомогою в переведенні своєї криптовалюти в готівку, та з'ясувати, наскільки легальними є джерела їх отримання.

Особи, які використовують криптовалюту, в переважній більшості встановлюють відповідне програмне забезпечення на свої персональні комп'ютери або смартфони. Це дозволяє досить легко керувати біткойнами без наявних спеціалізованих технічних знань про протокол обігу віртуальних активів. З використанням криптогаманців користувачі можуть відправляти та отримувати біткойни в електронному вигляді на своєму персональному комп'ютері, мобільному пристрої або у вебзастосунку. Кожен криптогаманець зберігає посилання на криптографічні ключі, які забезпечують доступ до балансів і трансферів біткойнів, можуть містити декілька облікових записів. Також кожен криптогаманець отримує власний індивідуальний код, що являє собою послідовність цифр та букв (зазвичай 33 символи). Відслідковування трансакцій стає реальним тільки тоді, коли користувач пов'язує своє ім'я та реквізити з публічною адресою в Інтернеті. До цих пір особа користувача, який використовує біткойн або криптогаманець, залишається невідомою для мережі.

У вітчизняних реаліях цікавою видається пропозиція К. Шаповалової передбачити можливість правоохоронних органів звертатися із клопотанням до слідчого судді щодо доступу до інформації на серверах, де зберігаються криптовалютні активи, що, на переконання автора, значно спросило би діяльність слідчого під час проведення досудового розслідування відповідних кримінальних проваджень, пов'язаних із криптовалютами [12, с. 387].

Практика правоохоронної діяльності засвідчує, що активно використовується методика «прослуховування» з'єднань пристрою, на якому встановлено програмне забезпечення біткойну в мережі Інтернет з метою відстеження IP-адреси, за якою ініціюється трансакція. Також допомагає ретельний аналіз інформації з декількох екс-чейнджерів, з якими злочинець мав угоди щодо придбання або продажу криптовалют. Під час отримання речових доказів також правоохоронцям доцільно розуміти, що існують пристрої, подібні до флеш-накопичувачів, які зберігають криптовалюту та мають назву «хардуєр» (холодний криптогаманець), який призначений для захисту криптовалюти, яка перебуває в гаманці.

Ще одним важливим моментом обігу криптовалют є систематичне використання принципу технології блокчейну, який полягає в незмінності проведених трансакцій. Скасувати трансакцію фізично неможливо, навіть коли вона помилкова. Тому єдиний вихід, який може запропонувати ця технологія, – галузевий проект. Зловмисники можуть зробити відкат трансакцій, тобто надрукувати альтернативні блоки, що отримало назву «Атака 51%». Ця комбінація означає, що певна кількість майнерів (добувачів) криптовалюти можуть підтвердити блок і тотально контролювати мережу та всі трансакції, які там відбуваються. «Атака 51%» відбувається тоді, коли в певної кількості майнерів перебуває «контрольний пакет» хешрейта, тобто обчислювальних потужностей. Наприклад, 4 квітня 2018 року мережа анонімної криптовалюти Verge була повністю контрольована злочинцями з використанням принципу «Атака 51%».

Аналіз викладеного переконливо засвідчує, що за таких умов існує суттєва загроза, що комп'ютери, які побудовані на квантових засадах, можуть бути уразливими для криптовалют, в основі яких знаходиться технологія блокчейн. З іншого боку, криптографічні протоколи, які забезпечують безпеку трансакцій та фінансових операцій, потенційно уразливі для досить потужного квантового комп'ютера. Навіть у квітні 2019 року анонімна група хакерів «Великий біткойн-колайдер» нахабно заявила, що може цілеспрямовано взламувати криптогаманці, використовуючи так звану тактику «грубої сили», спрямовуючи велику кількість обчислюваних потужностей на підбір приватних ключів до індивідуальних криптогаманців. Технологія блокчейн має певні недоліки, проте, якщо порівняти її з централізованими системами обробки інформації, блокчейн виглядає як революційна модель з великими перспективами.

Дійсно, на внутрішньодержавному рівні поступово складається слідчо-судова практика розслідування кримінальних проваджень щодо злочинів, які скоєні з використанням криптовалют. Аналіз скоєних злочинів з використанням криптовалют вимагає прискорення розроблення продуманої криміналістичної методики протидії таким кримінальним посяганням та виявленню осіб, які їх здійснили. Така криміналістична методика має базуватися на основних засадах криптовалют, до яких відносяться: децентралізація їх випуску (емісії); відсутність технічних можливостей контролю обігу; анонімність осіб, які здійснюють трансакції з криптовалютою; відсутність адміністративно-територіальних обмежень для створення та використання криптовалюти тощо.

Таким чином, ураховуючи певний рівень анонімності використання криптовалют, необхідним є визначення кордонів, де вказана анонімність завершується та починається так звана «смуга доступу» до персональних даних певної особи, яка здійснює криптовалютні операції, порушуючи вимоги національного або міжнародного законодавства. Враховуючи, що криптогаманці, як правило, є анонімними, однією з таких «смуг доступу» є операції щодо обміну тієї чи іншої криптовалюти на фіатні грошові кошти. Саме під час здійснення операції, яка передбачає зарахування фіатних грошових коштів на банківський рахунок (списання з рахунку) особи, яка продала (придбала) криптовалюту, з'являється можливість установити учасника такої операції або особи, яка діяла в його інтересах. Другою «смугою доступу» з метою персоналізації особи, яка здійснює протизаконні угоди з криптовалютами, є комплексний аналіз інформації про зв'язки такої анонімної особи з іншими пов'язаними з нею реальними особами, в тому числі й у мережі Інтернет. Саме таким способом, за інформацією ФБР США, був установлений та надалі притягнутий до кримінальної відповідальності в жовтні 2013 року власник торговельного інтернет-майданчика «Silk Road» Рос Уільям Ульбрихт [13]. Із цією метою можуть успішно використовуватися комп'ютерні програми щодо побудови алгоритмів виявлення зв'язків

тієї чи іншої особи, а також інші схеми комплексного підходу з використанням аналітичних знань та вмінь у поєднанні з наявними можливостями обчислюваних машин.

Загалом, під час розслідування злочинів з використанням криптовалют правоохоронним органам необхідно мати відомості про умови, порядок обігу криптовалют, особливості здійснення трансакцій, про специфіку функціонування криптовалютних бірж тощо. Успішне розслідування вказаної категорії злочинів також є можливим лише за наявності кваліфікованих спеціалістів ІТ-сфери (інформаційно-комунікаційних технологій). Розслідуючи злочини, які вчиняються з використанням криптовалют, доцільно враховувати той факт, що ці злочини мають свої специфічні особливості. Проте існують труднощі визначення належності певної біткойн-адреси. Тому співробітники правоохоронних органів мають шукати засоби прив'язати певну IP-адресу або адресу електронної пошти до конкретної особи. Також, ураховуючи технічну специфіку та особливості проведення криптовалютних операцій, існування процедур можливого маскування походження криптовалютних активів, доцільним вбачається розвиток засобів дослідження слідоутворення, розроблення алгоритму встановлення та закріплення криміналістично вагомих відомостей для цього типу злочинів. Трансакції в мережах технології блокчейн анонімні по відношенню до користувачів, проте не є анонімними щодо самих трансакцій. Технології блокчейн з різноманітними трансакціями мають бути піддані ґрунтовному аналізу, що надає змогу ефективно запобігти злочинам, пов'язаним із криптовалютами. На цьому фоні важливе значення має розроблення та впровадження профілактичних заходів попередження злочинності, пов'язаної з обігом криптовалют.

Слушно вказують В. Носов та І. Манжай, що головними завданнями для правоохоронних органів на сучасному етапі розвитку криптовалют є ідентифікація осіб, причетних до певних операцій із криптовалютами, яка має ефективно відбуватися в процесі попередження і розслідування злочинів; проведення своєчасної оцінки ризиків, пов'язаних із функціонуванням криптовалютних систем та їх обігом, з метою виявлення відповідних загроз [14, с. 99]. Проте вважаємо, що успішне розслідування та розкриття злочинів у сфері обігу криптовалют також потребує наявності спеціальних знань та сучасного програмного забезпечення в арсеналі на озброєнні правоохоронців. Таким чином, обов'язковим є наявність практичних вмінь та навичок, спеціальних знань під час розслідування злочинів, пов'язаних із криптовалютами. У зв'язку з викладеним доцільно започаткувати проведення на перманентній основі обміну досвідом та стажування правоохоронців у вказаному контексті. Так, наприклад, позитивним моментом є проведення в жовтні 2019 року практичних занять для детективів НАБУ, які здобули навички з розслідування злочинців, пов'язаних із використанням криптовалют, напрацювали вміння щодо особливостей збирання та аналізу інформації за результатами здійснених трансакцій криптовалют [15]. Вважається, що така слушна практика має бути успадкована й у діяльності інших вітчизняних правоохоронних органів.

Висновки. Кримінологічні ризики, пов'язані з обігом криптовалюти та передумови до поширення використання цих цифрових рішень у злочинному середовищі мають комплексний характер. Саме технічна складність породжує проблеми правового регулювання феномену криптовалют. Загальновідомо, що різноманітні види криптовалют досить часто використовуються злочинцями не тільки для скоєння фінансових або економічних злочинів. Усе більше поширюється інформація щодо використання криптовалют з метою незаконного обігу наркотичних засобів та психотропних речовин, придання зброї та боєприпасів, фінансування терористичних або екстремістських організацій. Проникнення кібернетичних методів у механізми вчинення злочинної діяльності призводить до необхідності переосмислення кримінального законодавства, а саме щодо: необхідності визначення оптимальної кількості всіх можливих складів злочинів, направлених проти інформаційної безпеки; доцільності «оцифрування» класичних складів кримінальних правопорушень, які зачіпають інформаційні відносини; визначення особливостей кримінальних загроз у віртуальному середовищі. Враховуючи викладене, обґрунтовано підкреслюємо необхідність розроблення методологічних засад щодо кваліфікації кримінальних правопорушень, предметом яких є криптовалюта, або у випадку, коли вона виступає платіжним засобом за наслідками протиправного діяння. З метою збільшення кількості розкритих злочинів, що вчиняються з використанням криптовалют, доцільним вбачається прискорити схвалення правових засад, які мають урегулювати криптовалюти в Україні. Також правоохоронним органам необхідно налагодити комплексну взаємодію з криптовалютними компаніями та біржами з метою блокування будь-якої незаконної та протиправної діяльності в блокчейн-платформах. Вирішення цієї проблеми має комплексний характер та вимагає розроблення сучасної тактики і стратегії правоохоронної діяльності, спрямованої на результативне запобігання використанню злочинцями нових сучасних фінансових механізмів та впровадження методологічних засад розслідування цієї категорії кримінальних правопорушень.

ЛІТЕРАТУРА

1. Волосович С. Державне регулювання ринку криптовалют: зарубіжний досвід. *Зовнішня торгівля: економіка, фінанси, право*. 2018. № 1. С. 97–110.
2. Іванюк В.Д. Фінансово-правове регулювання ринку криптовалют в Україні : автореф. дис. … на здобуття наук. ступеня д-ра філософії : 081. «Право». Тернопіль, 2021. 21 с.
3. Доронін І.М. Криптовалюти: соціально-економічні фактори, право та функції держави. *Інформація і право.* 2017. № 3. С. 85–93.
4. Драчов О.В. Правова сутність криптовалют: генезис, функції та перспективи. *Юридична Україна*. 2018. № 11–12. С. 44–52.
5. Кісіль А.В., Пряміцин В.Ю. Правовий статус криптовалют в Україні. *Прикарпатський юридичний вісник.* 2021. № 1 (36). С. 8–11.
6. Краснова І.В. Світовий досвід регулювання криптовалют. *Наукові праці НДФІ.* 2017. Вип. № 4. С. 48–51.
7. Мерінова С.В., Половенко Л.П. Роль криптовалюти у цифровій економіці. *Науковий вісник Херсонського державного університету. Серія : «Економічні науки»*. 2021. Випуск 42. С. 80–87.
8. Благута Р.І., Мовчан А.В. Новітні технології у розслідуванні злочинів: сучасний стан і проблеми використання : монографія. Львів : ЛьвДУВС, 2020. 256 с.
9. Гребенюк М.В., Черняк А.М. Проблеми протидії організованій злочинності у сфері цифрової економіки. *Підприємництво, господарство і право.* 2019. № 3. С. 297–303.
10. Казначеєва Д.В., Дорош А.О. Кримінальні правопорушення у сфері обігу критовалюти. *Вісник кримінологічної асоціації України*. 2021. № 2 (25). С. 149–157.
11. Риски отмывания денег и финансирования терроризма, связанные с COVID-19, и ответные меры в области политики, ФАТФ. Париж, Франция. 2020. URL: http://www.fatf-gafi.org/publications/methodandtrends/documents/covid-19-ML-TF.html (дата звернення: 07.12.2021).
12. Шаповалова К.Р. Проблемні питання розслідування злочинів, вчинених із використанням криптовалюти. *Юридичний науковий електронний журнал.* 2018. № 6. С. 385–387.
13. Ross Ulbricht, the Creator and Owner of the Silk Road Website, Found Guilty in Manhattan Federal Court on All Counts. URL: https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/ross-ulbricht-the-creator-and-owner-of-the-silk-road-website-found-guilty-in-manhattan-fe (дата звернення: 07.12.2021).
14. Носов В.В., Манжай І.А. Окремі аспекти аналізу криптовалютних трансакцій під час попередження та розслідування злочинів. *Право і безпека*. 2021. № 1 (80). С. 93–100.
15. Детективи НАБУ здобули нові навички з розслідування злочинів, пов'язаних з використанням криптовалют. URL: https://nabu.gov.ua/novyny/detektyvy-nabu-zdobuly-novi-navychky-z-rozsliduvannya-zlochyniv-povyazanyh-z-vykorystannyam (дата звернення: 07.12.2021).