УДК 343.98
DOI https://doi.org/10.24144/2307-3322.2025.92.4.57

ВИОКРЕМЛЕННЯ ВИДІВ ЗЛОЧИННОЇ ДІЯЛЬНОСТІ, У ЯКИХ ВІРТУАЛЬНІ АКТИВИ Є ЗАСОБОМ ВЧИНЕННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ЯК ПІДСТАВА ФОРМУВАННЯ ОКРЕМИХ КРИМІНАЛІСТИЧНИХ МЕТОДИК РОЗСЛІДУВАННЯ

Саєнко В.В.,
аспірант Донецького державного університету внутрішніх справ
ORCID: 0009-0003-4806-5436

Саєнко В.В. Виокремлення видів злочинної діяльності, у яких віртуальні активи є засобом вчинення кримінальних правопорушень, як підстава формування окремих криміналістичних методик розслідування.

В останні десятиліття у криміналістиці поняття «злочинна діяльність» набуло дещо ширшого розуміння. Така протиправна діяльність почала розглядатися як спосіб існування, процедура його життєзабезпечення, а не лише як конкретні акти спрямовані на досягнення окремих злочинних цілей. У такому тлумаченні поняття «злочинна діяльність» є ширшим за поняття «злочин», «злочинна поведінка», «механізм злочину», останні включаються до поняття «злочинної діяльності» в якості окремих складових. Модель злочинної діяльності окремого виду, в основі якої лежить механізм злочину, є підставою для формування окремих криміналістичних методик розслідування кримінальних правопорушень.

Кримінально-правові та криміналістичні ознаки кримінальних правопорушень є підставою для класифікації криміналістичних методик розслідування. Тому формування таких методик, може передбачати виокремлення окремих видів злочинної діяльності, враховуючи при цьому найбільш вагомі кримінально-правові та криміналістичні ознаки такої протиправної активності.

Поширення віртуальних активів серед населення, тенденція до збільшення випадків їх використання у злочинній діяльності, відсутність методик розслідування даного виду кримінальних правопорушень у криміналістиці, зумовили актуальність дослідження.

Тому здійснене автором статті виокремлення видів злочинної діяльності, у яких віртуальні активи є засобом вчинення кримінальних правопорушень, слугує підставою для формування відповідних методик розслідування кримінальних правопорушень.

У статті проаналізована слідча практика розслідування кримінальних правопорушень, де віртуальні активи використовуються як засіб вчинення таких протиправних дій. Це дало можливість зробити висновок про доцільність виокремлення таких окремих криміналістичних методик: створення та обігу шкідливих програмних чи технічних засобів; незаконного обігу наркотичних засобів, психотропних речовин або їх аналогів; виготовлення та обігу дитячої порнографії; незаконного позбавлення волі, викрадення людини, торгівлі людьми, проституції; незаконного обігу зброї, бойових припасів, вибухових речовин та вибухових пристроїв; незаконного обігу електричної або теплової енергії; незаконних дій з документами на переказ, платіжними картками, іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення.

Ключові слова: криміналістична методика, методика розслідування, злочинна діяльність, легалізація відмивання злочинних доходів, неправомірна вигода, збут наркотичних засобів та психотропних речовин, дитяча порнографія, торгівля людьми, незаконний обіг зброї, віртуальні активи, цифрові активи, криптовалюта, фінансування тероризму, методика розслідування комп'ютерних правопорушень, злочини у кіберпросторі, комп'ютерне шахрайство, цифрова валюта, фіатні гроші.

Saenko V.V. Identification of types of criminal activity in which virtual assets are a means of committing criminal offenses as a basis for the formation of separate criminalistics investigation methods.

In recent decades, the concept of «criminal activity» has acquired a somewhat broader understanding in criminology. Such illegal activity began to be considered as a way of life, a procedure for its life support, and not only as specific acts aimed at achieving individual criminal goals. In this interpretation, the concept of «criminal activity» is broader than the concepts of «crime», «criminal behavior», «mechanism of crime», the latter being included in the concept of «criminal activity» as separate components. The model of criminal activity of a particular type, based on the mechanism of the crime, is the basis for the formation of individual criminalistics methods of investigating criminal offenses.

Criminal-legal and criminalistics signs of criminal offenses are the basis for the classification of criminalistics methods of investigation. Therefore, the formation of such methods may involve the isolation of individual types of criminal activity, taking into account the most significant criminal-legal and criminalistics signs of such illegal activity.

The spread of virtual assets among the population, the tendency to increase cases of their use in criminal activity, the lack of methods for investigating this type of criminal offenses in criminalistics, determined the relevance of the study.

Therefore, the author of the article's isolation of types of criminal activity in which virtual assets are a means of committing criminal offenses serves as the basis for the formation of appropriate methods for investigating criminal offenses.

The article analyzes the investigative practice of investigating criminal offenses where virtual assets are used as a means of committing such illegal actions. This made it possible to conclude that it is appropriate to isolate the following separate criminalistics methods: creation and circulation of malicious software or hardware; illegal circulation of narcotic drugs, psychotropic substances or their analogues; production and circulation of child pornography; illegal deprivation of liberty, kidnapping, human trafficking, prostitution; illegal circulation of weapons, ammunition, explosives and explosive devices; illegal circulation of electrical or thermal energy; illegal actions with transfer documents, payment cards, other means of access to bank accounts, electronic money, equipment for their production.

Key words: criminalistics methodology, investigation methodology, criminal activity, legalization of money laundering, illicit profit, sale of narcotic drugs and psychotropic substances, child pornography, human trafficking, illegal arms trafficking, virtual assets, digital assets, cryptocurrency, terrorist financing, methodology for investigating computer crimes, cybercrime, computer fraud, digital currency, fiat money.

Постановка проблеми. В останні десятиліття проблема вивчення злочинної діяльності набула поширення, таку діяльність розглядають у кримінально-правовому, кримінологічному, соціологічному, психологічному та відповідно криміналістичному аспектах. Ще до недавнього у криміналістиці найчастіше зміст поняття «злочинна діяльність» обмежувався поодинокими протиправними актами, як то реальні рухи, дії чи операції. У минулому допускалося змішування понять «злочин» та «злочинна діяльність», ставився знак рівності між поодинокими «злочинним діянням» та «злочинною діяльністю».

Коли «злочинна діяльність» розглядається лише як сукупність певних дій та рухів особи, що спрямовані на реалізацію чи задоволення потреб, то можливе ототожнення поняття «злочину» та «злочинної діяльності». Однак в останні десятиліття у криміналістиці поняття «злочинна діяльність» набуло дещо ширшого розуміння. Така протиправна діяльність почала розглядатися як спосіб існування, процедура його життєзабезпечення, а не лише як конкретні акти спрямовані на досягнення окремих злочинних цілей. У такому тлумаченні поняття «злочинна діяльність» є ширшим за поняття «злочин», «злочинна поведінка», «механізм злочину», останні включаються до поняття «злочинної діяльності» в якості окремих складових [1].

Кримінально-правові та криміналістичні ознаки кримінальних правопорушень є підставою для класифікації криміналістичних методик розслідування. Тому здійснене автором статті виокремлення видів злочинної діяльності, у яких віртуальні активи є засобом вчинення кримінальних правопорушень, слугує підставою для формування відповідних методик розслідування кримінальних правопорушень.

Стрімке поширення віртуальних активів серед населення, тенденція до збільшення випадків їх використання у злочинній діяльності, відсутність дієвих криміналістичних методик розслідування таких криміналістичних правопорушень, зумовлюють актуальність здійсненого автором дослідження.

Метою статті є аналіз видів злочинної діяльності, у яких віртуальні активи використовуються як засіб вчинення кримінальних правопорушень, з метою формування відповідних криміналістичних методик розслідування.

Стан опрацювання проблематики. Здійснений нами аналіз стану наукового дослідження злочинної діяльності, у якій віртуальні активи використовуються як засіб вчинення кримінальних правопорушень показало, що у посібниках, періодичних виданнях та збірках конференцій такі проблеми розв'язували у своїх публікаціях Р.О. Баранов [2; 3], Л.В. Герасименко і О.В. Тихонова [4], М.В. Гуцалюк [5], В.А. Динту і А.А. Мітрофанов [6], Д.Й. Никифорчук і Д.Д. Чемерис [7], Є.В. Панченко [8; 9], В.І. Пісний [10], В.В. Федчишина [11], М.М. Фрідман-Козаченко [12], колектив науковців під керівництвом С.С. Чернявського [13; 14], О.В. Халін [15, с. 154-155], інші науковці.

Однак проблематика злочинної діяльності, у якій віртуальні активи є засобом вчинення кримінальних правопорушень, в останні роки на стільки динамічно розвивається, що поодинокі її дослідження не встигають задовольняти потреб як теорії криміналістики так і практики виявлення та розслідування такої протиправної діяльності.

Виклад основного матеріалу. На думку науковців, в сучасних умовах криптовалюта все частіше є засобом або предметом вчинення кримінальних правопорушень та завдяки своїм особливостям виступає фактором злочинності [7, с. 138.]

Злочинну діяльність пов'язану з використанням віртуальних активів доцільно розподіляти на дві основні групи: 1) злочинна діяльність у якій віртуальні активи є засобом вчинення правопорушень; 2) злочинна діяльність у якій віртуальні активи є об'єктом замаху.

У даній статті ми проаналізуємо види злочинної діяльності у якій віртуальні активи є засобом вчинення правопорушень. Злочинна діяльність цієї групи, в останні роки, характеризується значними темпами поширення. В її основі лежать дії, в ході яких віртуальні активи, зазвичай криптовалюти, обмінюються на предмети з обмеженим або забороненим обігом (наркотичні засоби та психотропні речовини, зброя, порнографічні предмети тощо).

Злочинна діяльність щодо легалізації (відмивання) майна, одержаного злочинним шляхом. Така протиправна діяльність кваліфікується за ст. 209 Кримінального кодексу України (далі – КК України). В загальному значенні, відмивання коштів полягає в тому, щоб узяти гроші, отримані від злочинної діяльності, та провести їх крізь низку операцій, маскуючи їхнє походження та інтегруючи їх до фінансової системи для подальшого використання в інтересах злочинців.

В узагальненнях фахівців Державної служби фінансового моніторингу України зазначається, що фінансова сфера, завдяки розвитку нових продуктів та технологій, надає злочинцям нові практики дистанційного способу вчинення злочину як в реальному світі, так і у віртуальному. Основними факторами трансформації фінансових злочинів є перехід світової економіки до нового технологічного укладу, інформатизація суспільства у всіх сферах, глобалізація, використання різних юрисдикцій до здійснення відмивання коштів [16, с. 24].

Аналіз слідчої практики вказує на те, що традиційною технологією відмивання коштів в цій сфері є придбання за «злочинні» кошти різних видів віртуальних активів (криптовалют) та на наступному етапі за допомогою різних бірж та спеціальних сервісів-міксерів подрібнення початкових монет та конвертація їх в інші криптовалюти. Таким чином кошти можуть пройти сотні адрес, ускладнюючи відстеження початкового власника. Принцип роботи подібних сервісів простий, вони беруть криптовалюту у різних клієнтів, «перемішують» її, у наслідок чого утворюється «мікс», який не дозволяє або утруднює процес відстеження власника грошей [16, с. 89].

Ускладнюють розслідування легалізації злочинних доходів також поширені Blockchain-інструменти, такі як: а) однорангові операції P2P (зазвичай, здійснюються на спеціалізованих веб-сайтах із певним відсотком комісії); б) Bitcoin-банкомати (операції обміну на готівку, здійснюються при бажання Bitcoin-нерів залишитися анонімними, особливо якщо ці банкомати обмінюють Bitcoin без отримання інформації KYC («знай свого клієнта», вимога FATF); в) Bitcoin-тумблери або змішувачі, є сервісом з відмивання коштів через заплутування ланцюжка транзакцій (за відносно невисокий відсоток, з високим ступенем анонімності клієнта); г) використання анонімних

криптовалют (засіб «транспортер»), правопорушники за його допомогою здійснюють анонімний обмін, між наприклад, фіатною та криптовалютою.

Так, у поточному році правоохоронці викрили масштабну міжнародну схему з відмивання коштів. Група зловмисників організувала переведення коштів у готівку за допомогою конвертаційного центру, переміщення готівки між містами України та країнами Європейського союзу, а також нелегальний обмін валют та продаж криптовалют. Детективи Бюро економічної безпеки провели обшуки приміщень, де здійснювалася незаконна діяльність з обміну валют, та вилучили готівку на 152 млн грн. Основною метою діяльності центру було відмивання доходів отриманих злочинним шляхом, конвертація коштів в Україні та у країнах Євросоюзу, приховуючи згадані операції від фінансових регуляторів. Зазначеною злочинною «схемою» користувалися сотні фізичних осіб та великі компанії. Що підтверджують документи, вилучені під час обшуків та чорнові записи щодо фізичних та юридичних осіб України та країн Євросоюзу, які користувалися зазначеною «схемою». Злочинне угруповання було виявлене завдяки взаємодії й співпраці детективів Бюро економічної безпеки з експертами Євросоюзу. Розпочато досудове розслідування у кримінальному проваджені за ознаками кримінального правопорушення, передбаченого ч. 2 ст. 212 КК України [17].

31.10.2024 Національне антикорупційне бюро України та Спеціалізована антикорупційна прокуратура повідомили про підозру голові Державної служби спеціального зв'язку та захисту інформації України (далі – Держспецзв'язок) Щиголю Ю., його заступнику та іншим у заволодінні державними коштами у сумі понад 62 млн грн. За версією слідства, 2020 року власник групи компаній у змові з керівництвом Держспецзв'язку розробили схему заволодіння бюджетними коштами, виділеними на закупівлю обладнання та програмного забезпечення. Для цього залучили дві підконтрольні компанії, а закупівлю засекретили, щоб уникнути відкритих торгів та забезпечити їхню перемогу. З цими компаніями підпорядковане Держспецзв'язку держпідприємство уклало договори на постачання відповідного програмного забезпечення та послуг та перерахувало у 2021-2022 роках кошти на суму понад 285 млн грн.

Проте реальна вартість програмного забезпечення, яке компанії придбали у іноземного виробника, становила 223 млн грн, а різницею більш ніж 62 млн грн і заволоділи учасники злочину. Ці кошти було виведено на рахунки підконтрольних компаній за кордоном з метою легалізації та розподілу між членами організованої групи.

В телефоні колишнього голови Держспецзв'язку Щиголя Ю. виявили криптогаманець, на якому зберігається 1 201 285 одиниць Tether USDT (еквівалент 1 201 928 дол США) і 6,9 Bitcoin (275 тис дол США). Загалом 1,476 млн дол США у криптовалюті. Крім зазначеного, під час обшуків у Щиголя Ю. знайшли ще 82 тис євро і 72 тис дол США готівкових коштів [18; 19].

Злочинна діяльність щодо ухилення від сплати податків, зборів (обов'язкових платежів). Такі протиправні дії кваліфікуються за ст. 212 КК України. Використання віртуальних активів характерне для умисного ухилення від сплати податків, зборів (обов'язкових платежів), що входять в систему оподаткування, введених у встановленому законом порядку, якщо ці діяння призвели до фактичного ненадходження до бюджетів чи державних цільових фондів коштів у значних розмірах.

Так, 2022 року було повідомлено про підозру 7 особам в ухиленні від сплати податків на суму понад 71 млн грн через махінації на ринку криптовалют. Учасникам злочинної «схеми» повідомлено про підозру в ухиленні від сплати податків в особливо великих розмірах та легалізації доходів, одержаних злочинним шляхом (ч. 3 ст. 28, ч. 3 ст. 212, ч. 3 ст. 209 КК України).

За даними органів досудового розслідування, підозрювані для реалізації схеми ухилення від сплати податків використовували ресурси з обміну електронних коштів, які дозволяють користувачам, у тому числі і з російської федерації, а також так званих «ЛНР/ДНР», конвертувати готівкові та безготівкові кошти у криптовалюту та навпаки. Фінансові операції здійснювалися в обхід вимог українського законодавства у сфері регулювання таких послуг, без відображення відповідних операцій у податковій звітності, ідентифікації клієнтів та сплати обов'язкових платежів до державного бюджету України.

Згідно висновку судово-економічної експертизи за період 2017-2020 років такі дії учасників «схеми» сприяли фактичному ненадходження до бюджету понад 71 млн грн у вигляді податку на доходи фізичних осіб та військового збору.

Органи досудового розслідування Національної поліції України встановили, що незаконно отримані прибутки були легалізовані шляхом придбання квартир, земельних ділянок та іншого

майна. Під час обшуків в учасників «схеми» вилучили понад 830 кг банківського срібла у злитках та грошові кошти у сумі близько 50 млн грн у різній валюті – 830 тис євро, 470 тис дол США та 460 тис грн. На вилучені грошові кошти, а також придбане підозрюваними майно – 6 земельних ділянок та 3 квартири, судом накладено арешт. Загальна вартість арештованого майна становить понад 100 млн грн [20].

Злочинна діяльність щодо одержання неправомірної вигоди службовою особою. Така протиправна діяльність кваліфікується за ст. 368 КК України. Поширення віртуальних активів сформувало новий інструмент корупції, який є ускладненим для протидії, у порівнянні з готівкою або безготівковою неправомірною вигодою. У даному випадку «схема» є такою: хабародавець реєструє криптогаманець, зараховує до нього віртуальний актив (зазвичай, криптовалюту) та повідомляє відкритий та закритий ключі особі, якій надається неправомірна вигода, цей хабароотримувач може обміняти віртуальний актив на реальні гроші. З метою посилання своєї безпеки, дані правопорушники можуть відкрити крипто-гаманець і банківську карту, шляхом якої буде здійснено виведення коштів, на третіх осіб, що ускладнить ідентифікацію особи зловмисників.

Здійсненню таких злочинних дій сприяють анонімність (неможливість відстежити або перехопити транзакцію, а також проблематичність встановлення особи, яка здійснила переказ криптовалюти на певну адресу) і децентралізація (відсутність єдиного емітента і регулятора, що зумовлює як дефляційну природу криптовалюти, так і неможливість її довільної зміни або блокування). Певну проблему також становить оцінка віртуального активу у випадку притягнення правопорушника до кримінальної відповідальності. Хоча, той же Bitcoin має очевидну мінову вартість і може бути досить легко конвертований у валюту, яка виконує функцію платіжного засобу. Додамо, що в останній час як предмет неправомірної вигоди використовується не лише Bitcoin як взаємозамінний токен, але й невзаємозамінні токени (NFT). Якими є криптографічно унікальні токени, що пов'язані з цифровим контентом, які й забезпечують підтвердження права власності на віртуальні, а при потребі й фізичні активи. Вони є віртуальними активами, що містять ідентифікуючу інформацію, записану в смарт-контрактах. Невзаємозамінні токени (NFT) мають унікальні атрибути, зазвичай пов'язані з конкретним активом, вони можуть бути використані для підтвердження права власності на цифрові предмети аж до володіння фізичними активами. Ними можуть бути представлені будь-які віртуальні об'єкти для доказу їхньої цінності чи рідкості: предмети колекціонування, витвори мистецтва, земельні ділянки та ін.

Віртуальний актив, зокрема криптовалюта, зазвичай, зберігається у спеціальному криптогаманці, який є програмою з управління такими віртуальними активами. У такій програмі найціннішим є логін та пароль, використання яких підтверджують активність в мережі. Важлива специфіка віртуального активу, зокрема криптовалюти, полягає у тому, що втрата криптогаманця (логіна або пароля) означає безумовну втрату віртуальних активів, оскільки за відсутності адміністратора системи вони є непоправними. Така ситуація є зворотною стороною децентралізації, тобто більше свободи, передбачає й більше відповідальності. Втрата паролів є основною причиною, через яку обсяг віртуальних активів, зокрема криптовалюти, в обігу постійно (незначно, але й незворотно) знижується, оскільки, як відомо, емісія криптовалют є обмеженою.

Все це зумовлює ситуацію при якій ключову роль при викритті злочинної діяльності, де фігурує криптовалюта, відводиться роботі з власниками криптогаманців. Останній є певним еквівалентом банківського рахунку, на якому користувач зберігають свої віртуальні активи, зокрема криптовалюту, та через який здійснює транзакції. Варто зазначити, що криптогаманець не зберігає у собі віртуальний актив, зокрема криптовалюту, у вигляді певних даних, а містить лише ключі, що використовуються в управлінні адресами і реалізує технічну взаємодію з Blockchain. Для прикладу, криптогаманець формує транзакції або здійснює пошук інформації в реєстрі. Окремі типи криптогаманців допомагають обмінювати валюту, надають додаткові засоби безпеки тощо. Один криптогаманець може використовуватися для різних віртуальних активів, зокрема криптовалют. Відомості щодо статусу криптогаманця та його власника можуть отримуватися лише за допомогою спеціальних аналітичних програмних інструментів, а також використовуючи криміналістично значущу інформацію отриману внаслідок проведення пізнавальних процесуальних дій (огляд, обшук, проведення експертизи тощо).

Зазвичай, встановлення власників криптогаманців ускладнене відсутністю їх реєстрація на біржі (спеціальному сервісі), де не вимагається надання будь-яких персональних даних про особу власника. Все це зумовлює вирішення слідчим тактичного завдання, спрямованого на доказу-

вання під час розслідування кримінального правопорушення належності певного криптогаманця конкретній особі. Відповідно джерелами для з'ясування такої криміналістично значущої інформаціє є комп'ютерна техніка і відомості, отримані унаслідок проведених з нею пізнавальних процесуальних дій (огляд, експертиза і т. ін.).

Так, нещодавно правоохоронці оприлюднили в медіа інформацію про те, що Національне антикорупційне бюро і Спеціалізована антикорупційна прокуратура передали до суду обвинувальний акт проти депутата Верховної Ради Андрія Одарченка. Якого обвинувачують у спробі підкупити голову Державного агентства відновлення та розвитку інфраструктури Мустафу Найєма Bitcoin в обмін на сприяння в отриманні грошей із фонду ліквідації наслідків збройної агресії на ремонт будівель Державного біотехнологічного університету, де депутат продовжує обіймати посаду ректора (дію контракту призупинено).

За це депутат пообіцяв неправомірну вигоду у криптовалюті Bitcoin в еквіваленті 50 тис дол. США, а згодом надав її частину у розмірі 0,39 Bitcoin, що на той момент дорівнювало 10 тис дол. США.

Це перша в історії антикорупційних органів України неправомірна вигода, яку вдалося задокументувати у криптовалюті. Дії депутата кваліфікували як спробу дати хабар – ч. 4 ст. 369 КК України. Депутат, однак, заперечує, що перераховував гроші. За його словами, він лише допомагав розібратися Найєму в криптовалютах. Одарченко також припускав, що справу проти нього ініціювали вороги, яких він міг нажити як член антикорупційного комітету Верховної Ради [21].

За повідомленням Національного антикорупційного бюро, правоохоронці викрили також співробітника Державної прикордонної служби на наданні хабаря у криптовалюті представнику правоохоронного органу.

За даними слідства, прикордонник через посередника надав правоохоронцю криптовалюту USDT в еквіваленті 355 тис. дол. США За це він хотів, щоб правоохоронець «закрив очі» на його протиправну діяльність. На момент викриття злочинця хабар надійшов у повному обсязі на криптогаманець посередника, був переведений у готівку та переданий правоохоронцю.

Прикордоннику повідомлено про підозру за ч. 1 ст. 369 КК України. правоохоронцю та його посереднику про підозру за ч. 4 ст. 368 КК України [22].

Злочинна діяльність щодо вчинення шахрайства та шахрайства з фінансовими ресурсами. Протиправна діяльність щодо шахрайства кваліфікується за ст. 190 КК України, а шахрайства з фінансовими ресурсами за ст. 222 КК України. Нещодавно Національний банк України викрив онлайн-сервіс «BitCapital» у спробах обійти фінансове законодавство держави. Згадана компанія створила незаконну схему надання коштів у кредит, маскуючи свою діяльність під операції з криптоактивами. Від зазначеної діяльності компанії вже постраждало більше 700 людей. Серед яких соціально незахищені групи населення, а також військовослужбовці, яким компанія відмовляла у пільгах, передбачених законодавством України та агресивно стягувала заборгованість.

Фахівці Національного банку України вказали на те, що «онлайн-сервіс «BitCapital» вибудував складний механізм обходу законодавства: формально надаючи позики в USDT, фактично видають кредити в гривні, оминаючи усі встановлені законом регуляторні механізми. У діях зазначеної компанії виявлені системні порушення законодавства: перевищення гранично допустимих процентних ставок; маніпуляції з розкриттям інформації про реальну вартість кредиту; введення споживачів в оману щодо умов договору. І все це здійснюється на фоні повної непрозорості щодо умов надання послуги та свідомого ухилення від дотримання нормативних вимог.

В діях «BitCapital» вбачається: шахрайство (ст. 190 КК України), адже компанія вводить клієнтів в оману щодо умов кредитування, приховує реальні ставки, або маскує кредити під криптоопераціїї; шахрайство з фінансовими ресурсами (ст. 222 КК України), адже маскування гривневих кредитів під позики в USDT може розглядатися як маніпуляція з фінансовими ресурсами; порушення порядку здійснення господарської діяльності (ст. 202 КК України), «BitCapital» фактично надає кредити без реєстрації як фінансова установа, що є прямим порушенням законодавства про фінансові послуги; примушування до виконання цивільно-правових зобов'язань (ст. 355 КК України) – компанія використовує агресивні методи стягнення боргів.

Висновки фахівців щодо протиправної діяльності онлайн-сервісу «BitCapital» передані до Національної поліції України та Бюро економічної безпеки [23].

Злочинна діяльність щодо фінансування тероризму. Відповідальність за таку протиправну діяльність передбачена ст. 258-5 КК України. Високий ступінь анонімності, створює преваги

і полегшує етап підготовки до терористичного акту, який може включати виплату винагороди учасникам терористичного угруповання, а також закупівлю необхідних засобів для такого виду злочинної діяльності (одягу, обладнання, зброї тощо). Проте, є протилежні думки експертів, вони вказують, що побоювання використання криптовалюти у фінансуванні тероризму є дещо перебільшеним.

Працівники Державної служби фінансового моніторингу України навели такий приклад: 28.08.2015 Алі Шукрі Амін був засуджений до 11 років тюремного ув'язнення з подальшим довічним перебуванням під наглядом поліції. Цей вирок був винесений йому за діяльність в Інтернеті, спрямовану на надання матеріальної підтримки та надання ресурсів терористичній організації ІДІЛ. В ході своєї злочинної діяльності Алі Шукрі Амін розмістив у соціальній Інтернет-мережі «Твіттер» посилання на написану ним статтю під назвою «Bitcoin та благодійна діяльність для джихаду». У цій статті ним розглядалися способи використання Bitcoin, і те, як джихадисти могли б скористатися цією валютою для фінансування своєї протиправної діяльності. У статті також надавались пояснення, що таке Bitcoin, як функціонує ця система віртуальної валюти, а також пропонувалося використовувати новий Bitcoin-гаманець Dark Wallet, що забезпечує анонімність користувача Bitcoin.

Крім зазначеного, у наведеній статті містилися вказівки на алгоритм створення анонімної системи збору пожертв з використанням Bitcoin для надсилання коштів моджахедам [24, с. 65-66].

У іншому прикладі, Служба безпеки України заблокувала діяльність злочинного угруповання, яке займалося відмиванням та незаконним переведенням коштів, зокрема й з використанням криптовалют. Так, організатори створили низку онлайн-ресурсів (сайти, телеграм-канали), які дозволяли користувачам конвертувати криптовалюту у готівку в особливо великих розмірах (на понад 240 млн грн). Біло з'ясовано, що даним сервісом користувались також особи, які підтримують тероризм та сепаратизм. Транзакції здійснювалися через заборонені іноземні електронні платіжні системи. Для відмивання коштів злочинці інвестували в нерухомість, земельні ділянки та дорогоцінні метали [16, с. 92].

Злочинна діяльність щодо створення та обігу шкідливих програмних чи технічних засобів. Така протиправна діяльність кваліфікується за ст. 361-1 КК України. Певною криміногенною загрозою поширення криптовалюти є збільшену кількість кібератак з використанням програм-вимагачів.

Так, працівники Державної служби фінансового моніторингу України виявили невідповідність операцій з криптовалютами фінансовому профілю певної фізичної особи – громадянина України.

Ця фізична особа володіла рахунком на крипто-біржі та здійснювала значні операцій з криптоактивами. Водночас, зазначена фізична особа не мала офіційно задекларованих доходів. Використовуючи програмне рішення Chainalysis Reactor було встановлено: фізична особа отримувала Bitcoin від різних Bitcoin-гаманців, що належать низці осіб, а також з гаманців клієнтів біржі з високим рівнем ризику; адреси походження Bitcoin пов'язані з діяльністю програм-вимагачів, Даркнет-ринком, шахрайством та діяльністю сервісів-міксерів.

Зазначеної фізичною особою використано крипто-біржі для обміну коштів у гривню та надалі використано для придбання різних високовартісних активів.

Правоохоронним органом було встановлено, що зазначена фізична особа здійснює злочинну діяльність з використанням програм-вимагачів [25, с. 57].

Злочинна діяльність щодо незаконного обігу наркотичних засобів, психотропних речовин або їх аналогів. Зазвичай така протиправна діяльність кваліфікується за ст. 307 КК України. Поширеною сферою злочинного використання віртуальних активів, зокрема криптовалюти є незаконний наркообіг (зокрема, наркоторгівля).

Найпоширенішою злочинною «схемою» незаконного наркообігу є розміщення оголошень на сайтах мережі Інтернет, де пропонується робота на вкрай вигідних умовах, пов'язана із збутом наркотичних речовин. Зацікавленим особам пропонують зв'язатися з роботодавцем захищеними каналами зв'язку месенджерами, де збувачі великих партій наркотичних засобів знаходять помічників, так званих «закладчиків», які безпосередньо й займаються збутом у роздріб наркозасобів.

З метою розширення кола покупців, створюються спеціальні сайти фіктивних Інтернет-магазинів, де зазвичай, наркотичні засоби маскуються під найменуваннями харчових чи інших продуктів. Оформлюючи замовлення покупець не надає особисті відомості продавцю, а залишається знеособленим. Домовившись, тобто уклавши угоду, покупець переказує кошти на електронний

гаманець продавця, який згодом зв'язується через соціальні мережі із застосуванням лінгвістичних стегоконтейнерів або захищених каналів зв'язку у месенджері із «закладчиком» повідомляючи адресу постачальника та місце «закладки». Покупця, у свою чергу, інформують про місце «закладки», і таким чином угода вважається завершеною.

При цьому кошти електронного гаманця, отримані унаслідок незаконної угоди, легалізуються через купівлю віртуальних активів, зокрема криптовалюти, з подальшою конвертацією в інші кошти на відповідній електронній біржі.

Здійснюючи купівлю віртуального активу, зокрема криптовалюти, покупці наркотичних речовин переводять кошти на рахунки електронних гаманців збувачів наркозасобів. Після цього зловмисники з анонімних чи підставних електронних гаманців купують віртуальні активи, зокрема криптовалюту на електронних біржах чи спеціальних приватних сайтах обміну валют. Зазвичай, такий віртуальний актив (куплена криптовалюта) обмінюється кілька разів на іншу криптовалюту, щоб було важче відстежити початкове надходження коштів з електронного гаманця.

Далі електронні активи, зокрема криптовалюту, продавці за допомогою електронних бірж назад конвертують у гроші, які надходять на інші анонімні електронні гаманці зловмисників. Далі кошти можуть переводитися на банківські картки зловмисників, що оформлені на підставних осіб, або на ці кошти можуть придбаватися матеріальні блага в Інтернет-магазинах.

Як ми вже зазначали, придбавання віртуальних активів, зокрема криптовалюти, не передбачає надання відомостей про покупця, значно ускладнює роботу правоохоронців щодо ідентифікації осіб, які уклали такі протиправні угоди.

Так, Службою безпеки України в Одеській області виявлено функціонування нарколабораторії, яка займалась виготовленням амфетаміну. Злочинці також здійснювали контрабандне постачання МДМА (напівсинтетична психоактивна сполука амфетамінового ряду) з Нідерландів. Для проведення розрахунків зловмисники активно використовували криптовалюту Bitcoin. Необхідна сума в Bitcoin розміщувалась в електронний гаманець продавця, якому за допомогою системи знеособлених чатів «Джаббер» повідомлявся електронний код для отримання доступу до коштів. Для купівлі Bitcoin клієнти, які мали намір придбати наркотичні засоби або психотропні речовини, з використанням банківських карт українського банку за допомогою різноманітних іноземних сайтів придбавали криптовалюту [16, с. 92].

Злочинна діяльність щодо виготовлення та обігу дитячої порнографії. Такі протиправні дії кваліфікуються за ст. 301-1 КК України. Віртуальні активи, зокрема криптовалюта можуть використовуватися з метою сексуальної експлуатації дітей в Інтернеті. Насамперед це стосується обігу предметів дитячої порнографії, а інколи й оплати прямих трансляцій дій сексуального характеру з неповнолітніми і т. ін. Як і зайняття іншою злочинною діяльністю, оплата «послуг» віртуальними активами, зокрема криптовалютою значно підвищує приватність злочинців та технічно ускладнює виявлення кримінального правопорушення.

Так, у Кривому Розі поліція затримала сімейну пару, яка використовувала свою чотирирічну доньку для створення порнографічних відео. Вихідці однієї з країн Кавказького регіону 29-річний чоловік та його 30-річна дружина вступали з донькою у статеві зносини, фіксуючи це на відео. Продаж відеофайлів здійснювався в анонімному сегменті Інтернету, а для оплати використовувалася криптовалюта.

Поліцейські встановили нік-нейм, який використовували зловмисники для завантаження файлів порнографічного змісту. У квартирі, яку орендували зловмисники, силовики провели санкціонований обшук, вилучивши комп'ютерну та відеотехніку, мобільні телефони [26; 27].

Кіберполіція Дніпропетровщини викрила злочинну групу, яка знімала та продавала незаконне відео з підлітками. Первинну інформацію щодо поширення в мережі відео порнографічного характеру за участі малолітніх дітей Кіберполіція отримала від колег з Австралії. Під час проведення досудового розслідування українські поліцейські встановили усіх учасників злочинної групи, причетних до створення та продажу дитячої порнографії. Жертвами злочину стали діти віком від 9 до 13 років. Їх до порностудії приводили власні ж батьки заради грошей.

Для конспірації, студії розташовувалися у сільській місцевості, а відзнятий порнографічний матеріал збувався в мережі за допомогою засобів анонімізації. Розрахунок за продаж дитячої порнографії відбувався виключно за допомогою криптовалюти. Оператором був організатор групи (43-річний мешканець області), який особисто виконував ролі у таких зйомках. Він також приймав замовлення на створення порнографічного відео за участі дітей різної статі із відповідною тематикою, інтер'єром, кількістю учасників, та інших особистих бажань замовника [28; 29].

Нещодавно Інтернет-видання «Gizmodo» повідомило, що дослідники з Рейнсько-Вестфальського технічного університету Ахена виявили у деяких фрагментах Blockchain, який використовується для функціонування криптовалюти Bitcoin сотні посилань на дитячу порнографію.

Blockchain є ланцюжком блоків, в яких можуть зберігатися замітки або файли. Окремі блоки в загальному ланцюжку зберігають записи транзакцій і можуть потенційно зберігати невеликі замітки або файли, зазвичай це інформація про те, для чого була потрібна транзакція.

Вивчивши приблизно 1600 файлів, дослідники виявили, що 99 відсотків файлів складаються або з тексту, або з зображення, а відносно невелика кількість файлів містить сексуальний контент – всього вісім. Один з цих файлів був ідентифікований як порнографічний образ неповнолітнього суб'єкта. Два інших файли містили в цілому 274 посилання на жорстоке поводження з дітьми, 142 з яких були пов'язані з Даркнетом.

Дослідники вважають, що певний зміст, наприклад, дитяча порнографія, може зробити просте володіння Bitcoin незаконним. На їх думку, оскільки усі дані блокового ланцюга завантажуються і постійно зберігаються користувачами, вони несуть відповідальність за будь-який небажаний контент, доданий в блок-ланцюжок іншими. Отже було б незаконно брати участь у системі на основі Blockchain, як тільки вона буде містити незаконний контент.

Зазначається, що Blockchain є ланцюжком транзакцій, куди включаються усі підтверджені операції. Blockchain постійно синхронізується і додає нові транзакції. Теоретично Blockchain Bitcoin має зберігати транзакції і файли необмежений час. Це означає, що посилання на порнографічні матеріали неможливо видалити [30].

Це дослідження дає змогу зробити висновки, що криптовалюту, зокрема Bitcoin використовують у незаконному обігу дитячої порнографії. У даному випадку відповідальність за законодавством України може наступати за продаж та зберігання дитячої порнографії. Крім того, протиправним є обмін посиланнями в ланцюжках Blockchain на ресурси в мережі Інтернет чи Даркнет, на яких розміщений (рекламується) такий контент.

Злочинна діяльність щодо незаконного позбавлення волі, викрадення людини, торгівлі людьми, проституції. Протиправні дії щодо незаконного позбавлення волі або викрадення людини кваліфікуються за ст. 146 КК України, торгівля людьми за ст. 149 КК України, а кримінально карані дії пов'язані з проституцією, зокрема за участю неповнолітніх за ст. 303 КК України.

В процесі такої злочинної діяльності створюються Інтернет-сайти, де розміщуються оголошення про надання інтимних послуг. Оголошення і розрахунки за надані інтимні послуги здійснюються віртуальними активами, зокрема криптовалютою.

На початку 2018 року начальник Департаменту карного розшуку Національної поліції України повідомив, що у 2017 році поліція зареєструвала 507 кримінальних проваджень за фактом викрадень людей, згодом 386 зловмисникам повідомлено про підозру. У чотирьох випадках зловмисники вимагали викуп у вигляді криптовалюти. Такі кримінальні правопорушення мали місце у Києві, Вінниці та Одесі. Прикладом стало затримання зловмисників за викрадення двох осіб у Києві. Вони вимагали викуп з потерпілих у криптовалюті – Bitcoin. Сума викупу складала еквівалент п'яти мільйонам доларів США. У наслідок проведеної роботи поліцейські звільнили заручників, які кілька місяців провели у полоні [31].

Злочинна діяльність щодо незаконного обігу зброї, бойових припасів, вибухових речовин та вибухових пристроїв. Протиправні дії щодо незаконного обігу зброї, тобто придбання, збуту вогнепальної зброї (крім гладкоствольної мисливської), бойових припасів, вибухових речовин або вибухових пристроїв без передбаченого законом дозволу кваліфікуються за ст. 263 КК України.

В цілому злочинна діяльність, пов'язана з використанням віртуальних активів вчинювана з метою незаконного обігу зброї схожа до протиправних дій під час незаконного обігу наркотичних засобів, психотропних речовин або їх аналогів. У даному випадку віртуальні активи можуть використовуватися як засіб оплати протиправних дій під час обігу зброї, набоїв до неї та вибухових речовин.

Міжнародній слідчій практиці відомі випадки торгівлі зброєю у Даркнеті за криптовалюту. Таке розслідування, зокрема стосувалося громадянина Словаччини, який торгував вогнепальною зброєю, боєприпасами та наркотиками. Після затримання зловмисника було проведено низку обшуків в ході яких виявлено п'ять одиниць вогнепальної зброї, боєприпаси різного калібру, велику криту плантацію канабісу та Bitcoin-гаманець, який містив Bitcoin на суму 203 000 євро, які, як підозрюється, були отримані через незаконні послуги, що пропонувалися через Даркнет [32, с. 44].

Злочинна діяльність щодо обігу електричної або теплової енергії. Протиправні дії, такі як викрадення, привласнення, вимагання електричної або теплової енергії кваліфікуються за ст. 188-1 КК України.

Співробітники Департаменту кібербезпеки Служби безпеки України спільно з Національною поліцією ліквідували підпільний центр з майнінгу криптовалют на Харківщині, який щомісяця викрадав промислові об'єми державної електроенергії на сотні тисяч гривень.

Правоохоронці вважають, що систематичне перевантаження комунальних мереж могло призвести до масштабних перебоїв з енергопостачанням до об'єктів житлового фонду та критичної інфраструктури у прифронтових районах.

До створення нелегального майнінг-центру були причетні декілька місцевих жителів, які встановили технологічне обладнання в орендованому складському приміщенні поблизу Харкова. З метою генерації електронних грошей використовували понаднормові обсяги необлікованої електроенергії, яку отримували через несанкціоноване підключення до мережі.

Під час обшуків у зловмисників виявлено комп'ютерну техніку та спеціалізоване обладнання з доказами злочинної діяльності [33].

Злочинна діяльність щодо незаконних дій з документами на переказ, платіжними картками, іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення. Такі протиправні дії кваліфікуються за ст. 200 КК України.

Працівники Департаменту кіберполіції спільно з Головним слідчим управлінням Нацполіції та у співпраці з ФБР США провели багаторівневу міжнародну операцію з ліквідації дев'яти сервісів обміну віртуальних активів.

Вебресурси пропонували користувачам анонімний обмін криптовалют. Такі послуги надавалися для сприяння легалізації та відмивання грошей, здобутих протиправним шляхом. Через біржі зловмисники проводили активи, отримані в результаті атак шкідливим програмним забезпеченням (вірусами-шифрувальниками) та онлайн-шахрайства. Рекламування послуг з обміну здійснювалося на закритих хакерських форумах.

Наслідком проведеної операції було блокування інфраструктури мережі, що розміщувалася на серверах у США, країнах Європи та в Україні. Доменні імена були вилучені. А досудове розслідування в Україні здійснювалося за фактами несанкціонованого втручання в роботу електронних комунікаційних мереж та незаконних дій з платіжними картками, електронними грошима (ч. 3 ст. 361, ч. 2 ст. 200 КК України) [34].

Висновки. Проаналізована нами слідча практика розслідування кримінальних правопорушень, де віртуальні активи використовуються як засіб вчинення таких правопорушень, дала можливість зробити висновок про доцільність виокремлення таких окремих криміналістичних методик: – створення та обігу шкідливих програмних чи технічних засобів; – незаконного обігу наркотичних засобів, психотропних речовин або їх аналогів; – виготовлення та обігу дитячої порнографії; – незаконного позбавлення волі, викрадення людини, торгівлі людьми, проституції; – незаконного обігу зброї, бойових припасів, вибухових речовин та вибухових пристроїв; – незаконного обігу електричної або теплової енергії; – незаконних дій з документами на переказ, платіжними картками, іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Starushkevych A., Hrebenyuk A., Fedchyshyna V., Stasiuk L., Bandura I., Holovko O. Criminal activity: concept and content. *AD ALTA: journal of interdisciplinary research.* 2024. № 14/02-XLIII. P. 148-152. URL: https://www.magnanimitas.cz/ADALTA/140243/PDF/140243.pdf (дата звернення: 01.12.2025).
2. Баранов Р.О. Протидія легалізації злочинних доходів та фінансуванню тероризму з використанням віртуальних валют. *Державне управління: удосконалення та розвиток.* 2016. № 6. URL: http://www.dy.nayka.com.ua/?op=1&z=978 (дата звернення: 15.05.2025).
3. Баранов Р.О. Сучасні схеми відмивання злочинних коштів у світі та в Україні. *Аспекти публічного управління.* 2015. № 7-8. С. 62-69. URL: http://nbuv.gov.ua/UJRN/aplup_2015_7-8_10 (дата звернення: 15.05.2025).
4. Герасименко Л.В., Тихонова О.В. Криптовалюта: проблеми визнання неправомірною вигодою. *Реалізація державної антикорупційної політики в міжнародному вимірі:* матеріали

V Міжнар. наук.-практ. конференції (м. Київ, 9-10 грудн. 2020 р.). Київ: НАВСУ. 2020. Ч. 1 С. 66-67. URL: https://www.navs.edu.ua/files/naukova-diyalnist/naukovi-zaxodi/zbirnuki/2020/anty-korupc1_1.pdf (дата звернення: 15.05.2025).

5. Гуцалюк М.В. Протидія протиправній діяльності в кіберпросторі: конфіскація криптоактивів, одержаних злочинним шляхом. *Реалізація державної антикорупційної політики в міжнародному вимірі:* матеріали VI Міжнар. наук.-практ. конференції (м. Київ, 9-10 груд. 2021 р.). Київ: НАВСУ, 2021. С. 221-223. URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/14978/1/materialy_konf_korup_081221.pdf (дата звернення: 15.05.2025).
6. Динту В.А., Мітрофанов А.А. Bitcoin у системі легалізації доходів, одержаних злочинним шляхом. *Наукові праці Національного університету «Одеська юридична академія».* 2017. Т. 19. URL: http://npnuola.onua.edu.ua/index.php/1234/article/view/524/495; DOI: https://doi.org/10.32837/npnuola.v19i0.524 С. 122-129 (дата звернення: 10.05.2025).
7. Никифорчук Д.Й., Чемерис Д. Д. Проблемні питання протидії криптовалютній злочинності в Україні. *Шляхи реформування кримінальної поліції: вітчизняний та зарубіжний досвід*: матеріали Міжнар. наук.-практ. круглого столу (м. Київ, 18 лют. 2022 р.). Київ: Нац. акад. внутр. справ, 2022. С. 138-139. URL: https://elar.navs.edu.ua/server/api/core/bitstreams/631128de-e64c-454c-bfb8-baa9a86c9cbe/content (дата звернення: 03.05.2025).
8. Панченко Є.В. Досвід кіберполіції в розслідуванні злочинів пов'язаних із віртуальними активами. *Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України:* матеріали міжвід. наук.-практ. конференції (м. Київ, 17 листоп. 2023 р.). Київ: Нац. акад. внутр. справ України, 2023. С. 92-97. URL: https://elar.navs.edu.ua/server/api/core/bitstreams/08ddbcd2-3419-4ddb-af7c-7f6a3d01d9c0/content (дата звернення: 03.05.2025).
9. Панченко Є.В. Криптовалюти й електронні гроші як інструменти фінансової активності кіберзлочинців. *Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України:* міжвідомч. наук.-практ. конференція (м. Київ, 1 листоп. 2024 р.). Київ: НАВСУ, 2024. С. 85-89. URL: https://elar.navs.edu.ua/server/api/core/bitstreams/82ef550b-2b39-4375-a5d1-c9bc136b0a2a/content (дата звернення: 03.05.2025).
10. Пісний В.І. Розслідування легалізації (відмивання) майна, одержаного службовою особою у вигляді неправомірної вигоди: дис. на здобуття ступеня доктора філософії за спеціальністю 081 – Право; Національна академія внутрішніх справ, Київ, 2024, 312 с.
11. Федчишина В.В. Криптовалюта й блокчейни криптовалюти як інструменти корупції: реалії інституціалізації. *Реалізація державної антикорупційної політики в міжнародному вимірі:* матеріали VII Міжнар. наук.-практ. конференції (м. Київ, 8-9 груд. 2022 р.). Київ: НАВСУ, 2022. С. 101-111. URL: https://www.navs.edu.ua/files/antykoruptsia/2022/materialy_konf_081222.pdf#page=112 (дата звернення: 02.05.2025).
12. Фрідман-Козаченко М.М. Криптовалюта як інструмент легалізації (відмивання) доходів, одержаних злочинним шляхом в умовах воєнного стану. *Розвиток юридичної науки в умовах воєнного стану:* матеріали Міжнар. наук.-практ. конференції (м. Київ, 17 трав. 2023 р.). Вінниця: ТОВ «ТВОРИ», 2023. С. 222-226.
13. Досвід країн Європейського Союзу щодо протидії злочинам, пов'язаним з корупцією, та захисту фінансових інтересів держави: аналіт. огляд / І. Кржечковськис, В.В. Тацієнко, С.С. Чернявський та ін. Київ: Нац. акад. внутр. справ, 2016. 280 с.
14. Досвід країн Європейського Союзу щодо виявлення та розслідування відмивання злочинних доходів із використанням цифрової валюти (криптовалюти): методичні рекомендації / С.С. Чернявський, І. Кржечковськис, В. В. Тацієнко та ін. Київ: НАВСУ, Консультативна комісія ЄС в Україні, 2017. 84 с.
15. Халін О.В. Розслідування легалізації (відмивання) доходів, одержаних злочинним шляхом: дис. канд. юрид. наук: 12.00.09; Класичний приватний університет. Запоріжжя, 2017. 238 с.
16. Актуальні методи, способи, інструменти легалізації (відмивання) злочинних доходів та фінансування тероризму (сепаратизму) (затв. Наказом Державна служба фінансового моніторингу України від 20.12.2021 № 146). Київ: Державна служба фінансового моніторингу України. 2021. 117 с.

17. Далецька Ю. БЕБ викрило масштабний конвертцентр криптовалют, вилучили понад 150 мільйонів. *Цензор.НЕТ: інтернет портал (https://censor.net/ua/about)* від 03.01.2023. URL: https://censor.net/n3391014 (дата звернення: 13.05.2025).
18. Дячкіна А. ВАКС заарештував колишнього очільника Держспецзв'язку на 2 місяці. *Українська правда. Економічна правда (https://epravda.com.ua/)* від 23.11.2023. URL: https://epravda.com.ua/news/2023/11/23/706903/ (дата звернення: 25.03.2025).
19. Апеляційна палата залишила арештованою криптовалюту ексголови Держспецзв'язку. *Слово і діло. Аналітичний портал. (https://www.slovoidilo.ua)* від 13.11.2024. URL: https://www.slovoidilo.ua/2024/11/13/novyna/polityka/apelyaczijna-palata-zalyshyla-areshtovanoyu-kryptovalyutu-eksholovy-derzhspeczzvyazku (дата звернення: 25.03.2025).
20. Пресслужба Київської міської прокуратури. Понад 71 млн грн несплачених податків та легалізація доходів через махінації на ринку криптовалют – 7 особам повідомлено про підозру. *Офіційний сайт Київської міської прокуратури (https://kyiv.gp.gov.ua)* від 13.10.2022. URL: https://kyiv.gp.gov.ua/ua/news.html?_m=publications&_t=rec&id=321327&fp=2660 (дата звернення: 17.05.2025).
21. Ялівець Г. НАБУ вперше передало до суду справу про хабар у біткоїнах, підозрюють «слугу народу» Одарченка. *Цензор.НЕТ: Інтернет портал (https://censor.net/ua)* від 16.04.2024. URL: https://censor.net/biz/news/3484691/nabu_vpershe_peredalo_do_sudu_spravu_pro_habar_u_bitkoyinah_pidozryuyut_slugu_narodu_odarchenka (дата звернення: 13.05.2025).
22. Далецька Ю. Правоохоронці викрили прикордонника, який намагався дати хабар в криптовалюті на $355 тисяч. *Цензор.НЕТ: Інтернет портал (https://censor.net/ua)* від 28.03.2025. URL: https://censor.net/n3543721 (дата звернення: 13.05.2025).
23. НБУ визнав діяльність онлайн-сервісу BitCapital незаконною. *Судово-юридична газета (https://sud.ua)* від 04.02.2025. URL: https://sud.ua/uk/news/ukraine/322421-nbu-priznal-deyatelnost-onlayn-servisa-bitcapital-nezakonnoy (дата звернення: 25.03.2025).
24. Ризики тероризму та сепаратизму. Київ: Державна служба фінансового моніторингу України. 2017. 83 с.
25. Типологічне дослідження відмивання доходів від податкових злочинів (затв. Наказом Державної служби фінансового моніторингу України від 12.12.2020 № 122). Київ: Державна служба фінансового моніторингу України. 2021. 78 с.
26. Дитину, яку батьки ґвалтували на камеру в Кривому Розі, оглядають лікарі. *Сайт BBC News Україна (https://www.bbc.com)* від 14.06.2018. URL: https://www.bbc.com/ukrainian/news-44479844 (дата звернення: 25.03.2025).
27. У Кривому Розі подружжя за криптовалюту продавало порно з чотирирічною донькою. *Сайт онлайн-медіа ТСН (https://tsn.ua/)* від 13.06.2018 URL: https://tsn.ua/ukrayina/u-krivomu-rozi-podruzhzhya-za-kriptovalyutu-prodavalo-porno-z-chotiririchoyu-donkoyu-1170705.html (дата звернення: 25.03.2025).
28. Кіберполіція викрила злочинну групу у створенні та продажі дитячого порно. *Офіційний вебпортал Національної поліції України (https://npu.gov.ua)* від 20.12.2019. URL: https://npu.gov.ua/news/kiberpolitsiya-vikrila-zlochinnu-grupu-u-stvorenni-ta-prodazhi-dityachogo-porno (дата звернення: 25.03.2025).
29. Дитяче порно за криптовалюту. *Сайт «11 канал» (https://11tv.dp.ua/about)* від 23.12.2019. URL: https://11tv.dp.ua/news/dp/20191223-dytyache-porno-za-kryptovalyutu.html (дата звернення: 25.03.2025).
30. Ходоренко А. У блоках Bitcoin виявили сліди дитячої порнографії. *Сайт журналу NV техно (https://techno.nv.ua)* від 21.03.2018. URL: https://techno.nv.ua/ukr/it-industry/u-blokakh-bitcoin-vijavili-slidi-ditjachoji-pornohrafiji-2459119.html (дата звернення: 25.03.2025).
31. Поліція впроваджує нові методи розслідування викрадень людей та їх повернення за криптовалюту (інтерв'ю начальника Департаменту карного розшуку Нацполіції Сергія Тіхонова). *Вебпортал МВС України (ttps://mvs.gov.ua)* від 26.01.2018. URL: https://mvs.gov.ua/uk/press-center/news/Policiya_vprovadzhu_novi_metodi_rozsliduvannya_vikraden_lyudey_ta_ih_povernennya_za_kriptovalyutu_FOTO_11863 (дата звернення: 25.03.2025).
32. Ризики відмивання коштів та фінансування тероризму у світі віртуальних активів. Типологічний звіт. Страсбург: MONEYVAL. 2023. 45 с.

33. СБУ ліквідувала підпільну криптоферму, яка викрадала електроенергію на прифронтових територіях сходу України. *Офіційний сайт Служби безпеки України (https://ssu.gov.ua/novyny)* від 19.07.2022. URL: https://ssu.gov.ua/novyny/sbu-likviduvala-pidpilnu-kryptofermu-yaka-vykradala-elektroenerhiiu-na-pryfrontovykh-terytoriiakh-skhodu-ukrainy (дата звернення: 25.03.2025).
34. Нацполіція спільно з ФБР ліквідувала мережу сервісів для обміну криптовалюти, здобутої злочинним шляхом. *Офіційний сайт Департаменту кіберполіції Національної поліції України (https://cyberpolice.gov.ua/)* від 02.05.2025 URL: https://cyberpolice.gov.ua/news/naczpolicziya-spilno-z-fbr-likviduvala-merezhu-servisiv-dlya-obminu-kryptovalyuty-zdobutoyi-zlochynnym-shlyaxom-1266/ (дата звернення: 25.03.2025).