является политизированной структурой. В работе на конкретных примерах исследованы способы реализации исторической политики в Польше.
Ключевые слова: историческая политика, политика памяти, Польша, Институт национальной памяти.

Abstract: Attention is focused on the policy of memory in Poland. Analyzed the attitude of the Poles to their historical past. It is established that the Institute of National Remembrance is a politicized structure. In the work on concrete examples explored the methods of realization of historical politics in Poland.
Key words: historical policy, memory policy, Poland, Institute of National Memory.

СПИСОК ЛІТЕРАТУРИ

1. Миллер А. Политика памяти в посткоммунистической Европе и ее воздействие на европейскую культуру памяти. URL:http://gefter.ru/archive/18391

2. Траба Р. Польские споры об истории XXI в. *Новое литературное обозрение*. 2012. С. 65–102.

3. Петровская О. В. Война за память: политические практики Польши. URL: https://riss.ru/images/pdf/journal/2014/2/12_.pdf

4. Гурьянова А. Э. Польские спецпереселенцы в СССР в 1940–1941 гг. URL: http://www.memo.ru/history/polacy/G_1.htm

5. Зотов Г. Печаль варшавянки. Почему в Польше нерады освобождению от фашизма. *Аргументы и факты.* URL: http://www.aif.ru/society/history/pechal_varshavyanki_pochemu_v_polshe_ne_rady_osvobozhdeniyu_ot_fashizma

6. Столя Д. Польский ИНП становится «Министерством памяти»? *Новое литературное обозрение*. 2012. С. 103–122.

7. День памяти «Проклятых солдат» в Польше. *ZvistkaPL*. URL: http://zvistka.pl/ru/2017/02/26/den-pamyati-proklyatyh-soldat-v-polshe/.

9. Саражска М. Историческая політика Польши: патриотические фильмы и настольные игры. URL:http://www.dw.com/ru/a-19151585

8. Махун С. Януш Куртыка: «Историческая политика – это дело государства». *ZN,UA*. URL: http://gazeta.zn.ua/POLITICS/yanush_kurtyka_istoricheskaya_politika__eto_delo_gosudarstva.html.

УДК 343.3/.7

КРИПТОВАЛЮТИ ТА BLOCKCHAIN-ТЕХНОЛОГІЇ У СУЧАСНІЙ ПРОТИВОПРАВНІЙ ДІЯЛЬНОСТІ

Н. Хак Сіддікі, Р. О. Мовчан

Анотація. На основі аналізу наукової літератури, вивчення матеріалів практики, нормативно-правових актів, покликаних забезпечувати правове регулювання обігу криптовалют в різних країнах, порушені актуальні питання, що впливають на особливості виявлення і розкриття злочинів пов'язаних з криптовалютами. Виділено основні злочинні схеми використання криптовалют.
Ключові слова: криптовалюта, обіг, контроль, відмивання, правоохоронна діяльність, анонімність, правове положення криптовалюти.

Одним із основних завдань сучасної юридичної доктрини є наукове забезпечення переведення електронних розрахунків у криптовалюті в правове поле, що ускладнюється через інноваційність криптовалют.

Аналіз матеріалів практики засвідчує, що криптовалюта є ігровим майданчиком для злочинця, тобто фактично масової гри у кішки-мишки з правоохоронними органами, оскільки як тільки правоохоронні органи краще пізнають злочинну поведінку, злочинці знаходять нові методи ухилення і все більш анонімні криптовалюти [1]. Оплата криптовалютою гарантує анонімність і технічно ускладнює виявлення злочину[2].

Слід зазначити, що поява BTC-банкоматів, -бірж, -банків створюють відчуття попиту і ліквідності біткойну (далі – BTC). Стрімкий ріст курсу BTC,нерегульована сфера обігу криптовалют робить криптовалюту потенційним кримінальним інструментом:

предметом вчинення кіберзлочинів та платіжним засобом організованих злочинних угруповань.

За попередніми оцінками, щорічно кількість випадків неправомірного заволодіння BTC збільшується в десятки разів, що в цілому можна порівняти з темпом легального обороту криптовалюти [3]. Криптовалюта стає предметом розкрадання та використання в сфері сексуальної експлуатації дітей в Інтернеті, спроб продажу людини, купівлі-продажу номерів кредитних карток.

Вартість криптовалют зростає в геометричній прогресії, що приваблює все більше українців. Громадяни України все частіше стають жертвами шахраїв під час операцій з криптовалютами, не маючи повноцінного захисту з боку правоохоронних органів [4].

За інформацією НБУ, СБУ та НПУ, відсутність контролю за обігом криптовалют та анонімність розрахунків створює потенційні передумови для їхнього використання з метою легалізації коштів, отриманих злочинним шляхом, оплати заборонених до вільного обігу товарів (наркотиків, зброї), дають можливість фінансування тероризму, зокрема на окупованих територіях України.

Однак у зв'язку з існуванням терористичної загрози в Україні впровадження криптовалют має свої особливості. Згідно звіту міжурядової організації FATF, яка займається розробкою світових стандартів у сфері протидії відмивання злочинних коштів та фінансуванню тероризму, відсутність правових регуляторів впливу на BTC дозволяє використання їх у злочинних цілях, зокрема спрямовувати на купівлю зброї.

Експерти Центру соціально-економічних досліджень «CASE Україна» підтвердили, що криптовалюта можна розглядатись як один із способів приховування доходів і ухилення від податків. Наприклад, можливо виправдати якісь високі витрати в майбутньому вдалим «інвестуванням» в криптовалюту декілька років тому.

Слід зазначити, що деякі експерти відзначають, що небезпека криптовалют як інструменту для незаконних операцій перебільшена, використання криптовалюти організованою злочинністю або для кримінальних цілей не перевищує 2 %. Отже, криптовалюта – це просто такий же інструмент, як і інші гроші для таких операцій.

Розглянемо, не вдаючись у технічні тонкощі, такі питання, як: предметна та правова сутність криптовалют.

Самою поширеною є крипто валюта BTC розроблена програмістом під псевдонімом Satoshi Nakamoto у 2008 році [5]. Технологію Blockchain використовують в основному для переказів BTC. Останнім часом широкого розповсюдження набули Ethereum, Litecoin, Monero, Cardano, які відрізняються одна від одної власним унікальним способом шифрування даних. На базі Ethereum створюються алькоіни.

Для повного поняття викладеного вище матеріалу, необхідно розкрити процес застосування.

Придбати криптовалюту можна за допомогою: майнінгу, BTC-обмінників, -бірж, -кранів, -торговельних майданчиків, -терміналів-самообслуговування.

Технологія Blockchain забезпечує основні принципи BTC: децентралізація, беземісійність, анонімність, прозорість, швидкість, захищеність від підробки, неможливість скасування транзакцій. Можна стверджувати, що сутність технології – це перебування інформації одночасно у всіх учасників системи без права контролю над нею.

На сьогодні на законодавчому рівні статус BTC закріплений, як: офіційний платіжний засіб та валюта (Японія), ліцензована діяльність (Канада), засіб обміну (ЕС), «сировинний товар» (Фінляндія), фінансовий актив (США), різновид приватних грошей (Німеччина), віртуальний товар (Китай), власність - BTC, транзакція - бартер (Австралія, Венесуела), фінансова піраміда (Індія), грошовий сурогат (Україна, РФ). Однак в деяких країнах операції з BTC є незаконними (Китай, РФ, Таїланд, Ісландія).

Кроки розвинутих країн є більш-менш послідовними стосовно регулювання криптовалют, однак пропозиції в Україні та РФ виглядають хаотичними. На сьогодні законодавство обох країн знаходиться в нерегульованій зоні.

В України досі невизначений статус криптовалюти, як і основні поняття, що пов'язані з нею («токен» і «Blockchain», майнінгу).

На початку січня 2018 р. відповідним органам влади було доручено визначити державного регулятора, порядок функціонування ринку та моніторингу транзакцій з використанням криптовалют і ідентифікації суб'єктів операцій,порядок оподаткування доходів від їх здійснення, а також розроблення механізму забезпечення доступу правоохоронних органів до даних криптовалютних бірж [6].

У числі криміногенних властивостей криптовалют називають анонімність, швидкість, дешеві і незворотні переклади, заплутані ланцюжки транзакцій, відсутність статусу криптовалюти, правил для бірж і пунктів обігу та ідентифікації власника криптовалютного гаманця; доступ з будь-якої точки світу через Інтернет; можливість для використання в якості «сховища» або здійснення міжнародних переказів грошових коштів; відносна безпека; можливість створення валют, повністю «заточених» під відмивання грошей; відсутність керівного органу; може використовувати слабкості в правовому режимі конкретних країн, а точніше, в законодавстві [7, 8].

Аналіз практики показує, що кожен з наведених нижче прецедентів з криптовалютами вносив поправки до законодавств країн світу та посилював контроль за обігом криптовалют:

– використання BTC в якості валюти для продажу та покупки,на торговельних інтернет майданчиках або інтернет-форумах у мережі TOR. Закриття майданчика Silk Road (США, 2013);

– створення централізованої криптовалюти тільки для злочинних цілей у платіжній системі Liberty Reserve [9];

– викрадення BTC з використанням TOR з сайту за допомогою підробки залишків на рахунках модераторів та користувачів. Власник сайту чорного ринку Sheep marketplace був затриманий після намагання відмити викраденні BTC (США, 2015 рік);

– заснування незаконних інвестиційних фінансових пірамід: Savings and Trust, (США, 2013 рік), LeadInvest.net (Техас, 2018 рік) [10,11].

– злам серверу BTC-банків та системи транзакцій користувачів, створення власного облікового запису у системі. Жертвами стали Flexcoin та Poloniex. Зловмисники перевели 896 BTC на власні рахунки (США, 2014 рік) [12];

– зараження кодом для майнінгу комп'ютерних систем, публічних хмарних сервесів, Урядові сайти США і Британії були заражені кодом для майнінгу Monero через шкідливу версію додатку для людей з проблемами зору (2018 рік) [13];

– використання для майнінгу Monero акаунтуTesla у хмарному сервісі Amazon та сервер південно-корейської компанії (2018 рік)[14];

– вимагання,за допомогою зараження вірусом, переказу коштів на крипто-гаманці за розблокування інформації на носії. Подібної атаки зазнали лікарні, банки та інші компанії по всьому світу (2018 рік) [15];

– викрадення ферм майнінгу. В Ісландії викрадено близько 600 ферм. Розмір збитків оцінюється майже в $ 2 млн. (2018 рік) [16];

– шантаж з вимаганням викупу у криптовалюті. Члени злочинної групи DD4BCшантажували онлайн-казино і фінансові організації Швейцарії, Нової Зеландії та Австралії (2016 рік) [17].

Протягом 2017 року в Україні відбулося кілька гучних затримань:

– виявлено «ферму» з 200 ПК для майнінгу в інституті Патона м. Києва тавідкрито кримінальне провадження за ч. 2, ст. 188-1 (Викрадення електричної або теплової енергії шляхом її самовільного використання), ст. 205 (Фіктивне підприємство) та ст. 212 (Ухилення від сплати податків, зборів) [18];

– викрито злочинну групу,члени якої шляхом обману та зловживання довірою, заволодівали чужими грошовими коштами в особливо великих розмірах, легалізували отримані кошти переведенням криптовалют в готівку;

– у м. Одесі затримано громадянина РФ, який легалізував гроші з використанням криптовалют, які потім перераховував до Криму та окуповану територію Донбасу;

– повідомлено про підозру організатору злочинної схеми заволодіння коштів інвесторів комерційного проекту з упровадження в Україні криптовалюти Swiscoin. Громадянам України висунуто підозру у вчиненні злочину, передбаченого ч. 4 ст. 190 КК України[19];

– заарештовано BTC-гаманці, вилучені у засновника найбільшого журналу про криптовалюти і блокчейн ForkLog А.Каплан;

– у квітні 2016 році злочинному угрупованню висунуто підозру у вчиненні злочинів, передбачених ч. 3, ч. 4 ст. 190 (шахрайство), ч. 5 ст. 185 (крадіжка), ч. 2 ст. 361-1 (поширення шкідливих програм), ч. 2 ст. 200 (незаконні дії з платіжними документами), ч. 2 ст. 361 (несанкціоноване втручання в роботу ПО) КК України. Кіберзлочинці за допомогою розповсюдження шкідливого ПЗ в інформаційній системі Банку Кредит Дніпро створили несанкціонований платіжний документ на переказ 950,8 тисячі доларів на рахунок компанії в китайському банку. Після гроші перевели в готівку [20].

Далі розглянемо, які сліди злочину можуть бути виявлені у ході слідства.

Blockchain є одним із найбільш інноваційних підходів фіксації доказів, який забезпечує моніторинг складних транзакцій і безперестанної записі підозрілих транзакцій в системі: які адреси відправляють і отримують транзакції, включаючи точний час і кількість. Однак, для застосування цього методу потрібно: визначення статусу криптовалюти та контролюючий орган; введення ідентифікації власника крипто-гаманця, яке дозволить усунути проблему визначення кількості рахунків у однієї конкретної особи.

Учасник настільки анонімний, наскільки анонімний його зв'язок із електронним гаманцем. Предметом моніторингу для кіберполіції можуть бути підозрілі та аномальні транзакції обміну криптовалюти на «реальні гроші», так як це головна мета злочинця в кінцевому підсумку. Інструментарій аналітики транзакцій може використовуватись для проведення судово-медичної експертизи. Однак доступ декількох пристроїв і місць ускладнює перевірку власника облікового запису та особу, яка зробила конкретну угоду.

Правоохоронні органи застосовують програмні засоби для моніторингу користувачів BTC, аналітичні системи, які ефективно віднаходять злочинні транзакції та оповіщають про це. Злочинці розуміють, що базова технологія BTC може працювати проти них і все частіше використовують анонімні варіанти криптовалют, відомі як анонімні «альткойни». Вони використовують технологію з нульовим рівнем захисту, яка видаляє будь-яку ідентифікаційну інформацію з реєстратора блокчін. (Zcash, Monero і Dash) [21]. Згідно доповіді Поліцейського агентства Europol «криптовалюти, такі як monero, ethereum і Zcash, набирають популярність у цифровому підпіллі». На даний час monero є фаворитом атак у вигляді викупу, атак на сайти для масштабного майнінгу криптовалюти.

Вивчення наукової літератури та української і світової практики дозволило умовно виділити основні напрямки використання криптовалют в злочинних цілях:

І. Застосування власної або існуючої криптовалюти для злочинних цілей в якості знаряддя злочинного посягання (в якості грошових коштів при купівлі зброї, наркотичних засобів, психотропних речовин, дитячої порнографії, контрактів за наймані вбивства, ботнетів та інших заборонених предметів, легалізація злочинних доходів, фінансування тероризму та ін.):

– створення торгівельних інтернет майданчиків або інтернет-форумів у мережі TOR;

– створення власної платіжної системи для злочинних цілей;

– доходи від злочинної діяльності обмінюються на біржах, кошти надходять в кредитний кооператив, а потім переводяться на офшорні рахунки;

– у незаконній мережевій торгівлі отримана криптовалюта обмінюється на товарних біржах, потім перекладається на карти і знімається в банкоматі;

– використовується гаманець, в які не знайомі один з одним люди переводять віртуальні гроші, потім та ж сума чужих BTC частинами повертається відправнику. Зв'язок між зловмисником і злочинними грошима таким чином розривається;

– фальшиві інтернет магазини імітують операційну діяльність.

– розміщення оголошень в мережі для збору фінансів для тероризму;

– використання сайтів віртуальних азартних ігор для фінансування тероризму.

II. Розгляд криптовалюти як предмета злочинного посягання (розкрадання криптовалюта з рахунків, інтернет-шахрайство, вимагання викупу у криптовалюті та ін.).

– викрадення криптовалюти з рахунків модераторів та користувачів сайту за допомогою підробки залишків;

– злам серверу BTC банків та системи транзакцій користувачів;

– шантаж підприємства або особи поширенням секретних або особистих даних та вимагання викупу у криптовалюті;

– шантаж у вигляді викупу у криптовалюті за розблокування державних сайтів;

– зараження шкідливим ПЗ ransomware (шифрує данні на усіх носіях в мережі та вимагає криптовалюту для відновлення доступу до даних;

– заснування незаконної інвестиційної фінансової піраміди;

– фішингові сайти криптовалютних бірж, блокчейн-стартапів, гаманців та ICO проектів. Користувача просять перевести кошти на електронний гаманець шахраїв або ввести данні свого секретного ключа;

III. Розгляд криптовалюти, як інструменту інформаційної війни:

– втручання в стратегічні інформаційні системи держави з метою впливу на курс криптовалюти, а отже і на безпеку держави;

– маніпуляція громадською думкою найманим активістом (просування соціальної або політичної справи).

IV. Майнінг криптовалют:

– за допомогою зараження шкідливим ПЗ: ПК користувача, комп'ютерних систем, публічних хмарних сервісів, реклами на YouTube;

– викрадення ферм криптовалют;

– самовільне використання електроенергії та підключення «ферм» на державних підприємствах.

Повноцінний захист громадян України під час операцій з криптовалютами залежить від того,як швидко законодавець зможе визначити «зону гарантованої свободи» користувачів.

Законодавство це статика, а технологія - це завжди динаміка.

Аннотация. На основе анализа научной литературы сути угроз оборота криптовалют, изучение практики, нормативно-правовых актов правового регулирования криптовалют в разных странах, затронуты актуальные вопросы, влияющие на особенности выявления и раскрытия преступлений, связанных с криптовалютою. Выделены основные преступные схемы использования криптовалют .

Ключевые слова: криптовалюта, отмывании, правоохранительная деятельность, анонимность, правовое положение криптовалют.

Annotation. On the basis of the analysis of the scientific literature, the essence of the threats to turnover is the crypto-currency, the study of practice, regulatory legal acts of the legal regulation of crypto-currencies in different countries, the topical issues affecting the specifics of the detection and disclosure of crimes related to crypto-currencies are discussed; criminal schemes for using the crypto-currencies are examined.

Key words: cryptovolume, circulation, laundering, law enforcement activity, legal status of cryptography.

СПИСОК ЛІТЕРАТУРИ

1. Jason Bloomberg: Using Bitcoin Or Other Cryptocurrency To Commit Crimes? Law Enforcement Is Onto You. URL: https://www.forbes.com/sites/jasonbloomberg/ 2017/12/28/using-bitcoin-or-other-cryptocurrency-to-commit-crimes-law-enforcement-is-onto-you/#43cb50593bdc.

2. Internet Crime Report 2016 FBR. URL: https://pdf.ic3.gov/2016_IC3Report.pdf.

3. Кіберполіція висловилась стосовно криптовалют. URL: https://news.finance.ua/ru/news/-/419473/kiberpolitsiya-postavila-ultimatum-otnositelno-kriptovalyut.

4. Кокаин и взятки: эксперт рассказал, как преступники в Украине используют Bitcoin. URL: https://www.segodnya.ua/economics/kriptovalyuta/kokain-i-vzyatki-ekspert-rasskazal-kak-prestupniki-v-ukraine-ispolzuyut-bitcoin-1115901.html.

5. Батоев В. Б.,Семенчук В. В. Использование криптовалюты в преступной деятельности: проблемы выявления / Законодательство: состояние и пути совершенствавания. *Труды академии МВД России*. 2017. № 2(42). С. 10.

6. Рада нацбезпеки визначить порядок функціонування в Україні ринку криптовалют. URL: https://news.finance.ua/ua/news/-/418306/rada-natsbezpeky-vyznachyt-poryadok-funktsionuvannya-v-ukrayini-rynku-kryptovalyut.

7. Commonwealth. URL: http://thecommonwealth.org/sites/default/files/pressrelease/documents/P14195_ROL_Virtual_Currencies_D_Tait_V5_LoRes.pdf.

8. Виртуальные валюты: отчет ФАТФ. URL: http://www.eurasiangroup.org/files/FATF_docs/Virtualnye_valyuty_FATF_2016.pdf.

9. Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies. The United States Senate Committee on Homeland Security and Governmental Affairs, November 18, 2013. P. 21.

10. Подпольные деньги вывели из обращения. URL: http://www.kommersant.ru/doc/2200186.

11. Арестован создатель Sheep Marketplace, укравший биткоинов на $40 млн. URL: https://coinspot.io/world/arestovan-sozdatel-sheep-marketplace-ukravshij-bitcoin-na-40-mln/.

12. Texas State Securities Board cease-and-desist order. URL: https://ru.scribd.com/document/372516170/Texas-State-Securities-Board-cease-and-desist-order?irgwc=1&content=10079&campaign=Skimbit%2C%20Ltd.&ad_group=100652X1574425Xd51d070a8c85e0a0400952a62ffa2331&keyword=ft750noi&source=impactradius&medium=affiliate#from_embed.

13. Уязвимость в системе транзакций между пользователями позволила похитить Bitcoin на $600 тысяч URL: http://www.securitylab.ru/news/450258.php.

14. URL: https://news.finance.ua/ua/news/-/420397/uryadovi-sajty-ssha-i-brytaniyi-zarazyly-kodom-dlya-majningu-kryptovalyut.

15. Хакери зламали хмарне сховище Tesla і майнили через нього криптовалюту. URL: http://osvita.mediasapiens.ua/web/cybersecurity/khakeri_zlamali_khmarne_skhovische_tesla_i_maynili_cherez_nogo_kriptovalyutu/.

16. Північнокорейські хакери зламують комп'ютери для майнінгу криптовалют. URL: http://detector.media/infospace/article/133419/2018-01-02-pivnichnokoreiski-khakeri-zlamuyut-kompyuteri-dlya-maininguu-kriptovalyut-analitik/.

17. В Ісландії викрадено 600 ферм для майнінгу. URL: https://news.finance.ua/ua/news/-/421915/v-islandiyi-vykradeno-600-ferm-dlya-majningu-bitkojna.

18. Bitcoin Extortion Group DD4BC Now Targeting Financial Services. URL: https://www.coindesk.com/bitcoin-extortion-group-dd4bc-now-targeting-financial-services/.

19. У Луцькому політеху вилучили техніку для майнінгу криптовалюти. URL: https://news.finance.ua/ua/news/-/420269/u-lutskomu-politehu-vyluchyly-tehniku-dlya-majningu-kryptovalyuty.

20. Хакери пограбували один з українських банків. URL: http://vgolos.com.ua/news/hakery_pograbuvaly_odyn_z_ukrainskyh_bankiv_290499.html.

23. The Criminal Underworld Is Dropping Bitcoin for Another Currency. URL: https://www.bloomberg.com/news/articles/2018-01-02/criminal-underworld-is-dropping-bitcoin-for-another-currency.

УДК: 347.94

ЕЛЕКТРОННІ ДОКАЗИ В ЦИВІЛЬНОМУ ПРОЦЕСІ: ПРОБЛЕМИ ЗАСТОСУВАННЯ НА ПРАКТИЦІ

С. О. Чорний, О. І. Антонюк

Анотація. У статті розглядаються проблемні питання використання електронних доказів в цивільному процесі. Зокрема, проаналізовано проблеми на рівні законодавчого регулювання, що стосуються подання як оригіналів електронних доказів, так і їх копій до суду. Виявлено проблеми щодо порядку та особливостей дослідження електронних доказів, їх оцінки судом, що можуть виникнути на практиці, і запропоновано шляхи вирішення таких проблем.

Ключові слова: доказування, засоби доказування, електронні докази, електронний документ, цивільний процес.

Вступ. Постановка проблеми. В умовах стрімкого розвитку інформаційних технологій, активного відкриття та використання нових можливостей обміну інформацією в мережі Інтернет набуває все більш важливого значення достатньо нова форма існування