УДК 346.9
DOI https://doi.org/10.32782/chc.v048.2023.8

Добровольська Володимира Володимирівна,
кандидат юридичних наук, доцент,
доцент кафедри господарського права і процесу
Національного університету «Одеська юридична академія»
ORCID ID: 0000-0002-9304-3792

ПРАВОВИЙ АСПЕКТ БЕЗПЕКИ ВІРТУАЛЬНИХ АКТИВІВ

Постановка проблеми. У сучасних умовах господарювання з'являються нові форми розрахунків, до яких можливо віднести віртуальні активи, зокрема криптовалюта та інші. Закон України «Про віртуальні активи» не набув чинності, але є своєчасним та забезпечує потреби суб'єктів господарювання щодо можливості використання різноманітних цифрових платіжних інструментів. Вітчизняні суб'єкти господарювання здійснюють чисельні фінансові операції з іноземними контрагентами та використовують цифрові кошти, у тому числі й криптовалюту, у порядку та на умовах визначеними нормами чинного законодавства.

Стан дослідження проблеми. Проблемам вивчення кібербезпечних фінансових заходів присвячували свої праці чисельні фахівці з ІТ – безпеки та юристи-правники, серед яких праці Х. Бугаєнко, Д. Василенко, О. Корчинської, В. Поповського, Д. Прокопович-Ткаченко та інших, але не вирішеними залишилося питання щодо визначення зазначених заходів у нормах чинного законодавства та їх застосування банками та іншими фінансовими установами як суб'єктами господарювання.

Метою статті є теоретично-нормативний аналіз безпеки здійснення обігу віртуальних активів, задля їх безпечного та конфіденційного використання.

Виклад основного матеріалу. У світлі зазначеного важливим є питання щодо безпечності цифрових розрахункових операцій, яку повинні забезпечити відповідні уповноважені органи та особи у межах своїх повноважень. Мова йдеться про фінансові віртуальні відносини між банками та клієнтом, перевагами яких є:

1. Зручність. Забезпечує автоматизовану підготовку таких документів, як платіжне доручення, меморіальний ордер, заявка на переказ валюти та інших документів. Шаблони для введення електронних документів використовуються згідно з типовими стандартами, які діють в Україні і максимально наближені до паперових. Як і паперові, електронні платіжні документи, що відправлені до банку, підписують посадові особи підприємства, але замість звичайного використовують електронний цифровий підпис.

2. Оперативність. При використанні системи «клієнт-банк» збільшується швидкість проходження платежів. Висока оперативність зумовлена тим, що платіжне доручення в електронному вигляді готується один раз, і це робить не операціоніст банку, а працівник підприємства. Крім того, не потрібно готувати первинні платіжні документи на паперових носіях. Замість них раз на тиждень готується реєстр електронних документів, внаслідок чого відпадає необхідність щоденно відвідувати банк для проведення безготівкових платежів, що, у свою чергу, економить час та гроші.

3. Мобільність. Система «клієнт-банк» дозволяє контактувати з банком без обмежень у часі, оскільки технічні можливості більшості програмних комплексів дозволяють цілодобово відправляти документи до банку та переглядати отримані звідти.

4. Безпека. Засоби захисту інформації в системі «клієнт-банк» при коректному їх використанні гарантують надійний захист від несанкціонованого доступу та модифікації інформації [1, с. 119].

Безпеку всіх фінансових операцій мають забезпечити банки та інші фінансові установи. Захист банківських установ від незаконного

цифрового втручання можливо визначити як інформаційна безпека банку, адже майже кожен сучасний банк повинен використовувати всі існуючи засоби захисту, які у сукупності складають таке поняття як «кібербезпека банківської установи». Для належного, добового й гарантованого забезпечення кібербезпеки банк повинен долучати фахівців відповідного рівня, які будуть спроможні своїми знаннями і досвідом застосовувати механізми і засоби захисту банківської інформації, послуг, продуктів. Механізми і засоби захисту банківських даних визначені нормами чинного спеціального банківського законодавства та є предметом дослідження й аналізу у фаховій літературі. Так, на думку фахівців «в ідеалі системи кіберзахисту повинні не тільки виступати бар'єром для всіх відомих видів кіберзагроз, але і вміти ідентифікувати досі невідомі види кібератак до того, як вони могли б завдати шкоди банку та його клієнтам. Зазвичай система кібербезпеки банку являє собою комплексне програмне рішення, яке базується на низці технологій, здатних захистити інформаційний простір банку від окремих видів та типів загроз залежно від їх характеру дії та сфери виникнення. Використання цілого портфелю технологій дає змогу максимально мінімізувати наявний загальний рівень кіберризику, оскільки немає єдиної технології, яка б ефективно спрацьовувала проти усіх можливих типів загроз [2, с. 21][1].

Також діє НБУ Положення, яке розроблено відповідно до Законів України «Про Національний банк України», «Про основні засади забезпечення кібербезпеки України», з урахуванням Стратегії кібербезпеки України, затвердженої Указом Президента України від 26 серпня 2021 року № 447/2021, Національного стандарту України ДСТУ ISO/IEC 27001:2015 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою» [3].

На сучасному етапі використання та удосконалення інформаційно-електронних технологій банківські установи широко їх застосовують, а деякі їх них взагалі існують суто у цифровому просторі. Тобто, через Інтернет банки надають свої банківські послуги, невичерпний перелік яких встановлений нормами чинного законодавства, зокрема, спеціальним законодавчим актом – законом України «Про банки і банківську діяльність» [4]. Фахівці зазначають, що саме «банківські інтернет-послуги набувають в Україні дедалі більшої популярності: в середньому кількість клієнтів, що користуються послугами через Інтернет, зростає на 3 тисяч осіб щомісячно. Це збільшує дохід (обсяг банківських операцій) банку в середньому на 1098 тис грн. На базі проведених нами маркетингових досліджень новостворений вебсайт банку у перші чотири місяці після введення його в експлуатацію (перший етап) використовується лише на 40 %. На другому етапі його використання сягає 100 %» [5, с. 69]. Ч. 2 ст. 9 Закону України «Про віртуальні активи» містить обов'язок учасника ринку віртуальних активів до проведення операцій з віртуальними активами ознайомитися з особливостями функціонування систем забезпечення обороту віртуальних активів, в яких планується проведення операцій з віртуальними активами. Тобто, мова йдеться про забезпечення сучасного, якісного та надійного механізму захисту обігу віртуальних активів.

Вітчизняна банківська система представляє собою досить чітку структуру підпорядкування головному державному органу – Національному Банку України, який у межах своїх повноважень, у тому числі, приймає акти щодо створення та існування веб-сайтів. Тобто, чисельні нормативні відомчі акти НБУ також містять положення щодо веб-сайтів банківських установ, так, набрала чинності постанова Правління Національного банку України «Про затвердження Положення про інформаційне забезпечення банками клієнтів щодо банківських та інших фінансових послуг» від 28 листопада 2019 р. № 141. Усі банки повинні надавати повну інформацію про кредити та депозити на веб-сайті в єдиному уніфікованому форматі [6].

Існує «велика кількість програмних засобів, котрі дозволяють знайти віруси, вилучити їх та поновити пошкоджену інформацію. Антивірусним засобом називається програмний продукт, який виконує одну або декілька з наступних функцій: захист файлової структури від знищення; знаходження вірусів; знешкодження вірусів [7, с. 123].

Автентифікація – це «перевірка приналежності суб'єкту чи об'єкту доступу пред'явленого їм ідентифікатора; перевірка справжності. Ідентифікація на основі біометричних даних – це засіб автоматичного розпізнавання особистості на базі унікальних фізичних або поведінкових параметрів. Ідентифікація виконується за допомогою порівняння отриманих біометричних характеристик і шаблонів, що зберігаються у базі даних» [8, с. 262].

[1] Яровенко Г. М., Ковач В. О. Перспективи застосування технології блокчейн у системах кібербезпеки банків. *Підприємництво та інновації*. 2020. Вип 12. С. 206–214.

Для «вирішення задач автентифікації та авторизації в безпроводових телекоммунікаційних системах і мережах, які побудовано відповідно до специфікації міжнародних стандартів серії IEEE 802.16, використовуються засоби протоколу EAP (Extensible Authentication Protocol), криптографічного протоколу RSA (Rivest, Shamir і Adleman), а також засоби протоколу управління ключами PKM (Privacy and Key Management protocol) для безпечного розподілу ключової інформації Протоколи автентифікації і авторизації призначено для забезпечення вимог сервіс-провайдерів (NSP, Network Service Provider) та користувачів. Основними застосовуваними механізмами є протоколи RSA та/або EAP із певними функціями розподілу ключів. Саме властивості формованих ключів авторизації і визначають рівень безпеки телекомунікаційних систем і мереж при наданні безпроводового доступу» [9, с. 122].

На сьогоднішній день розроблено достатньо велику кількість протоколів автентифікації, зокрема для застосування у Інтернет-платіжних системах. Проте, більшість з них не володіють усіма необхідними властивостями для проведення взаємної автентифікації як покупця, так і продавця. Також у них не враховано той факт, що Інтернет є абсолютно незахищеним середовищем, а платіжна картка є досить ризиковим платіжним засобом, і саме тому повинні ставитися досить високі вимоги до розробки схем таких протоколів.

Також, на сьогоднішній день «все більшої популярності серед цифрових методів антикризового управління та підтримки фінансової стійкості банківської установи застосовуються інструменти, що базуються на технологіях штучного інтелекту. На сьогоднішній день штучний інтелект (Artificial Intelligence, AI) представляє собою групу технологій, базис яких утворюють експертні системи, машинне навчання та обробка природних мов, віртуалізації та роботизованої автоматизації, великі дані, управління знаннями. AI є потужним технологічним інструментом, який кардинально дозволяє змінити природу банківської системи, покращити систему взаємовідносин на основі довіри та дозволяє клієнтам мати більш значущі взаємодії з нами. Впровадження AI в банківську діяльність найбільш поширене в таких напрямках як автоматизація обслуговування клієнтів, трансакційної аналітики, виявлення шахрайства та управління ризиками» [10, с. 190].

Поряд із технологіями, які вже активно використовуються у системах кібербезпеки, можна виділити технологію блокчейн, яка є відносно новою та перспективною. Допоки вона не знайшла широкого розповсюдження, але її використання, на нашу думку, в системах забезпечення кіберзахисту банку змогла б суттєво підвищити рівень їхньої ефективності. Блокчейн став широко відомим завдяки активному розвитку криптовалют, більшість з яких базується саме на цій технології. Нині по всьому світі вже є низка стартапів, які намагаються реалізовувати та тестувати концепції різноспрямованих проектів на базі технології блокчейн. Зокрема, її починають використовувати під час побудови прогресивних систем електронного голо-сування, ведення різних глобальних реєстрів (наприклад, реєстрів нерухомості, земельних ділянок), у маркетингових системах, у системах управління ланцюгами поставок тощо [11, с. 16].

Технологія блокчейн, яку ще називають технологією розподілених реєстрів, є досить універсальним інструментом, який може бути використаним для вирішення широкого спектру завдань. До основних її переваг відносять децентралізованість, повну прозорість, конфіденційність, захищеність від несанкціонованого доступу та реалізацію компромісу. Всі вищенаведені переваги можуть бути спрямованими на вирішення наявних проблем забезпечення кібербезпеки банків [12].

Досить розповсюдженим є криптографічний захист інформації. Так, на думку В. В. Поповського, саме «криптографічні методи вирішують два завдання – забезпечення конфіденційності інформації шляхом позбавлення зловмисника можливості видобути інформацію з каналу зв'язку та забезпечення цілісності інформації шляхом недопущення зміни інформації та внесення в неї неправдивого змісту» [13, с. 12].

В законодавстві під криптографічним захистом інформації виокремлює «вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо» [14]. Банки укладають чисельні договори з клієнтами, як фізичними так і юридичними особами, з приводу розміщення та\або запозичення коштів в національній та\або іноземній валютах.

Висновки. Таким чином, у сучасному світі, на тлі модернізації та інформаційно-новітніх глобалізаційних процесів все більш актуальними стають питання щодо захисту інформації, у тому числі й банківської. Саме кібербезпека банківських установ є сучасним напрямком розвитку як НБУ так і інших органів, метою якої є надій-

ний захист персональних даних клієнтів банку, їх коштів, у тому числі й цифрової форми та іншої банківської інформації. Безпека здійснення обігу віртуальних активів представляє собою систему, змістом якої є різноманітні засоби, які направлені на запобігання, попередження та виявлення шахрайських дій щодо фінансово-розрахункових операцій, розкриття особистих даних їх суб'єктів, відомостей щодо кількості та різновидів коштів тощо.

ЛІТЕРАТУРА:

1. Рогач, І. Ф. Інформаційні системи у фінансово-кредитних установах : навч. посіб. 2-ге вид., перероб. і доп. / І. Ф. Рогач, М. А. Сендзюк, В. А. Антонюк. К. : КНЕУ, 2011. 239 с.
2. Яровенко Г. М., Ковач В. О. Перспективи застосування технології блокчейн у системах кібербезпеки банків. *Підприємництво та інновації*. 2020. Вип 12. С. 206–214.
3. Про затвердження Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об'єктів критичної інфраструктури в банківській системі України : постанова Правління Національного банку України від 12.08.2022 р. № 1781. URL: http//www.zakon.rada.gov.ua
4. Про банки і банківську діяльність : Закон України від 07.12.2000 р. URL: http//www.zakon.rada.gov.ua
5. Корчинська О., Веселова М. Ефективність застосування сучасних інформаційних технологій у маркетинговій діяльності банків. *Вісник Академії праці, соціальних відносин і туризму*. 2017. № 1. С. 64–70.
6. Про затвердження Положення про інформаційне забезпечення банками клієнтів щодо банківських та інших фінансових послуг : постанова Правління Національного банку України від 28 листопада 2019 р. № 141. URL: http//www.zakon.rada.gov.ua
7. Комп'ютерна техніка та інформаційні технології : електронний підручник / під ред. Голуб О. С. та ін. 2013. URL: http://www.shevchenkove.org.ua/
8. Бугаєнко Х. А., Горбенко І. Д. Аналіз трьох біометричних методів автентифікації особи. *Прикладная радиоэлектроника*. 2012. Т. 11, № 2. С. 262–266.
9. Прокопович-Ткаченко Д. І. Дослідження протоколів автентифікації та авторизації доступу в безпроводових телекомунікаційних системах та мережах. *Системи озброєння і військова техніка*. 2013. № 1(33). С. 119–130.
10. Трансформаційні процеси у фінансовому секторі національної економіки: теорія, методологія та моделювання : монографія / за заг. ред. О. І. Барановського. Київ : ДВНЗ «Ун-т банківської справи», 2017. 488 с.
11. Casino F., Dasaklis T.K., Patsakis C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*. 2019. Vol. 36. P. 55–81.
12. Bahou A. J. Blockchain and Applications in Information Security. Information Systems Security Association. URL: https://issa-midtn.org/resources/ pdf (дата звернення: 15.06.2023).
13. Поповский В. В. Основы криптографической защиты информации в телекоммуникационных системах. Ч. 1. Х. : Компания СМИТ, 2010. 190 с.
14. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05 липня 1994 р. *Відомості Верховної Ради України.* 1994. № 31. Ст. 286.

Добровольська Володимира Володимирівна

ПРАВОВИЙ АСПЕКТ БЕЗПЕКИ ВІРТУАЛЬНИХ АКТИВІВ

Стаття присвячена аналітично-змістовній характеристиці забезпечення безпеки здійснення обігу віртуальних активів, тобто їх належному й правомірному використанню як засобу платежу.

Законодавче вітчизняне забезпечення використання й обігу віртуальних активів знаходиться на етапі становлення. Закон України «Про віртуальні активи» не набув чинності у зв'язку із змінами податкового законодавства, але факт його розробки свідчить про актуальність та сучасність його положень. Важливим питанням використання й обігу віртуальних активів є дієве та практичне забезпечення їх безпеки, яка тісно пов'язана із кібербезпекою фінансового цифрового простору.

Суб'єктами, які забезпечують кібербезпеки є Національний банк України як головний регулятор всіх фінансово-розрахункових операцій та інші банки та фінансові установи, які на підставі ліцензії мають право правомірно їх здійснювати. Зазначені суб'єкти повинні здійснювати всі заходи кібербезпеки, які є сучасними та гарантують збереження цифрових активів та інформацію про їх обіг й використання. Таким засобами є автентифікація, антивірусні програми, технологія блокчейн та інші засоби. Об'єктами зазначеної безпеки є веб-сайти відповідних банківських та інших фінансових установ, які й застосовують різноманітні її засоби проти кібератак та крадіжки інформації щодо нарахування та використанні цифрових коштів, у тому числі й криптовалюти. Також, об'єктами кібербезпеки є банківські рахунки, як розрахункового та к й депозитного характеру, на яких знаходяться цифрові кошти, у тому числі й криптовалюта. Рахунки містять інформацію про кількість коштів та відомості щодо персональних даних власника рахунка. Банки застосовують заходи кібербезпеки як для віртуальних активів так й для рахунків з метою забезпечення їх зберігання та конфіденційності. Система заходів кібербезпеки банків та інших фінансових установ представляє собою сукупність різноманітних антивірусних та антишахрайських засобів, які діють постійно та забезпечують їх збереження та нерозголошення.

Ключові слова: банківська установа, віртуальні активи, криптовалюта, суб'єкти господарювання, фінансовий цифровий простір, технологія блокчейн, кібербезпека, веб сайт, криптографічний протокол, автентифікація, чинне законодавство.

Dobrovolska Volodymyra

LEGAL ASPECT OF SECURITY OF VIRTUAL ASSETS

The article is devoted to the analytical and substantive characteristics of ensuring the security of the circulation of virtual assets, that is, their proper and legitimate use as a means of payment.

Legislative domestic support for the use and circulation of virtual assets is at the stage of formation. The Law of Ukraine «On Virtual Assets» did not enter into force due to changes in tax legislation, but the fact of its development indicates the relevance and modernity of its provisions. An important issue of the use and circulation of virtual assets is the effective and practical provision of their security, which is closely related to the cyber security of the financial digital space.

Subjects that provide cyber security are the National Bank of Ukraine as the main regulator of all financial and settlement operations and other banks and financial institutions that, based on a license, have the right to legally carry them out. The specified entities must implement all cyber security measures that are modern and guarantee the preservation of digital assets and information about their circulation and use. Such means are authentication, antivirus programs and other means. The objects of this security are the websites of relevant banking and other financial institutions, which use various of its means against cyber-attacks and theft of information regarding the accrual and use of digital funds, including cryptocurrency. Also, the objects of cyber security are bank accounts, both settlement and deposit, on which digital funds, including cryptocurrency, are located. Accounts contain information on the amount of funds and information on the personal data of the account holder. Banks apply cyber security measures to both virtual assets and accounts to ensure their storage and confidentiality. The system of cyber security measures of banks and other financial institutions is a set of various anti-virus and anti-fraud tools that operate constantly and ensure their preservation and non-disclosure.

Key words: banking institution, virtual assets, cryptocurrency, business entities, financial digital space, blockchain technology, cyber security, website, cryptographic protocol, authentication, current legislation.