

Научная статья
УДК 343.7
DOI 10.33184/pravgos-2022.3.25

Original article

ФИЛЬЧЕНКО Андрей Петрович
Академия управления МВД России,
Москва, Россия;
e-mail: apfilchenko@yandex.ru;
https://orcid.org/0000-0002-0099-731X

FILCHENKO Andrey Petrovich
Academy of Management of the Ministry
of Internal Affairs of Russia, Moscow, Russia.

ЖАНДРОВ Владимир Юрьевич
Московский университет МВД России
им. В.Я. Кикотя, Москва, Россия;
e-mail: vaisvladimir74@gmail.com;
https://orcid.org/0000-0002-1353-2837

ZHANDROV Vladimir Yuryevich
Vladimir Kikot Moscow University
of the Ministry of Internal Affairs of Russia,
Moscow, Russia.

ИСПОЛЬЗОВАНИЕ РЕЖИМА САНКЦИЙ И СИСТЕМЫ КОМПЛАЕНС В СНИЖЕНИИ РИСКОВ НЕЗАКОННЫХ ОПЕРАЦИЙ С ВИРТУАЛЬНЫМИ АКТИВАМИ: ЗАРУБЕЖНЫЙ И РОССИЙСКИЙ ОПЫТ

THE USE OF THE SANCTIONS REGIME AND COMPLIANCE SYSTEM TO REDUCE
THE RISKS OF ILLEGAL TRANSACTIONS INVOLVING VIRTUAL ASSETS:
FOREIGN AND RUSSIAN EXPERIENCE

Аннотация. Криминологически значимым следствием развития информационно-телекоммуникационных и цифровых технологий, появления использующих элементы криптографии нестандартных платежных средств стало увеличение рисков проведения незаконных операций, прежде всего легализации доходов от преступной деятельности и финансирования терроризма. Анонимность, с которой действуют представители высокотехнологичной преступности, заставляет правительства менять подходы к регулированию оборота виртуальных активов, искать новые управленческие, правовые и экономические инструменты, которые окажутся эффективными для выявления, предупреждения и минимизации ущерба от незаконных финансовых операций. Данные обстоятельства вызывают острую необходимость научного обоснования и последующей оценки организационного опыта разных стран в сфере контроля оборота виртуальных активов. Преимущества виртуальных активов, которые используются для ведения незаконной деятельности, требуют компенсации за счет расширения контролирующей функции государственного управления путем введения санкций и внедрения обеспечивающей их выполнение системы комплаенс для физических и юридических лиц, участвующих в производстве и обороте виртуальных активов. Цель: на основе анализа опыта США по применению санкций и внедрению обеспечивающей их выполнение системы комплаенс определить уязвимости и возможности данного подхода по установлению государственного контроля в сфере оборота виртуальных активов, оценить перспективы его использования в юрисдикции России. Методы: разграничения основных видов виртуальных активов использовался метод классификации, при формировании терминологии исследования – аксиоматический метод, для установления правовой природы санкций – метод юридического анализа, для оценки опыта США и России по внедре-

Abstract. Criminologically significant consequence of the development of information and telecommunications and digital technologies, the emergence of non-standard means of payment using elements of cryptography virtual currencies, has been an increase in the risks of illegal transactions, and, above all, the legalization of proceeds from criminal activity and terrorist financing. The anonymity with which high-tech criminals operate forces governments to change approaches to regulating the turnover of virtual assets, to look for new management, legal and economic tools that will be effective in identifying, preventing and minimizing damage from illegal financial transactions. These circumstances cause an urgent need for scientific justification and subsequent assessment of the organizational experience of different countries in the field of control of the turnover of virtual assets. The advantages of virtual assets that are used for conducting illegal activities require compensation by expanding the controlling function of state administration by imposing sanctions and implementing a compliance system that ensures their implementation for individuals and legal entities involved in the production and turnover of virtual assets. Purpose: based on the analysis of the US experience in applying sanctions and implementing the compliance system that ensures their fulfillment, to determine the vulnerabilities and possibilities of this approach of establishing state control in the sphere of virtual assets and to assess the prospects for its use in Russian jurisdiction. Methods: the classification method is used to distinguish the main types of virtual assets; the axiomatic method is used to form the terminology of the study; the legal analysis is used to establish the legal nature of sanctions; the method of comparative study of regulatory legal acts and related documents is used to assess the US and Russian experience in implementing the compliance system; the logical and expert-analytical methods are used to identify the advantages and vulnerabilities of sanctions. Results:

© Фильченко А.П., Жандров В.Ю., 2022

нию системы комплаенс – метод сравнительного изучения нормативных правовых актов и сопутствующих документов, для выявления преимуществ и уязвимостей санкционного контроля – логический и экспертно-аналитический методы. Результаты: авторы пришли к следующим выводам: контролирующая функция государства в отношении оборота всех видов виртуальных активов может быть расширена путем введения режима санкций в отношении участников обмена и конвертации виртуальных активов, полученных преступным путем; обеспечить эффективность применения санкций возможно путем внедрения в деятельность участников оборота виртуальных активов системы комплаенс, направленной, прежде всего, на преодоление анонимности в цифровой среде; уязвимостями системы санкционного и связанного с ним комплаенс-контроля являются постоянное усложнение введенных санкций и несформированность единой позиции разных органов и учреждений относительно перечня и статуса виртуальных активов в разных юрисдикциях, что в условиях кризиса международного права приводит к превосходству национальных инструментов контроля.

Ключевые слова: криптовалюта, виртуальная валюта, цифровая валюта, комплаенс, санкции, незаконные операции, легализация доходов, финансирование терроризма

Для цитирования: Фильченко А.П. Использование режима санкций и системы комплаенс в снижении рисков незаконных операций с виртуальными активами: зарубежный и российский опыт / А.П. Фильченко, В.Ю. Жандров // Правовое государство: теория и практика. – 2022. – № 3. – С. 171–183. DOI 10.33184/pravgos-2022.3.25.

the authors conclude that the controlling function of the state in relation to the turnover of all types of virtual assets can be expanded by introducing a sanctions regime against participants in the exchange and conversion of virtual assets acquired by criminal means; it is possible to ensure the effectiveness of sanctions by introducing a compliance system into the activities of participants in the turnover of virtual assets, aimed primarily at overcoming anonymity in digital environment; the vulnerabilities of the system of sanctions and related compliances control are the constant complication of the network of imposed sanctions and the lack of a unified position of different bodies and institutions regarding the list and status of virtual assets in different jurisdictions, which in a crisis of international law leads to the superiority of national control instruments.

Keywords: cryptocurrency, virtual currency, digital currency, compliance, sanctions, illegal transactions, money laundering, terrorist financing

For citation: Filchenko A.P., Zhandrov V.Yu. The use of the sanctions regime and compliance system to reduce the risks of illegal transactions involving virtual assets: foreign and Russian experience. *Pravovoe gosudarstvo: teoriya i praktika = The Rule-of-Law State: Theory and Practice*, 2022, no. 3, pp. 173–183. DOI 10.33184/pravgos-2022.3.25 (In Russian).

ВВЕДЕНИЕ

Появление цифровых объектов с функциями платежных средств существенно повлияло на финансовые операции во всем мире, изменив не только их структуру, но и саму технологию транзакций. Наряду с очевидными преимуществами новые формы расчетов значительно увеличили риски незаконной деятельности, связанной, прежде всего, с легализацией доходов, полученных преступным путем [1]. В отсутствие центрального регулятора операций с цифровыми объектами правительства ищут инструменты, которые позволят компенсировать контролирующую функцию за эмиссией и оборотом нетрадиционных платежных средств и противодействовать незаконной финансовой деятельности с использованием цифровых объектов.

ТЕРМИНОЛОГИЯ НОРМАТИВНОГО РЕГУЛИРОВАНИЯ

Одним из способов восстановления функции государственного контроля в этом отношении является признание цифровой

валюты официальным платежным средством. В совместном отчете Банка международных расчетов и ряда зарубежных национальных банков за 2020 г.¹ указывалось, что в отсутствие четкого определения «цифровая валюта центрального банка» большинство суверенных юрисдикций рассматривают ее как новую форму денег, с множеством полезных преимуществ. Среди них: технологическая эффективность денежных переводов и платежей; снижение транзакционных сборов; возможность любому гражданину получить бесплатный или недорогой банковский счет и, что самое важное, перспектива отслеживания местоположения единицы валюты. Последнее из указанных преимуществ значительно затрудняет уклонение от уплаты налогов и облегчает обнаружение преступной деятельности, поскольку позволяет представить доказательство в виде цифровой записи существующей транзакции.

¹ Central bank digital currencies: foundational principles and core features. Bank for International Settlements 2020 [Электронный ресурс]. URL: https://www.bis.org/publ/othp33.pdf?_x_tr_sl=en&_x_tr_tl=ru&_x_tr_hl=ru&_x_tr_pto=sc (дата обращения: 05.07.2022).

Первым платежным инструментом такого рода, эмитированным крупной экономикой мира, стал выпущенный в 2022 г. Народным банком Китая цифровой юань, выпуск которого стал результатом работы Института цифровой валюты, разработавшим Обоснование концепции цифровой фиатной валюты². Вслед за этим три суверенных центральных банка – Центральный банк Багамских островов, Восточно-Карибский центральный банк и Центральный банк Нигерии – также эмитировали собственные цифровые валюты. В свою очередь, Центральный банк России в начале 2022 г. приступил к тестированию платформы цифрового рубля и успешно провел первые переводы между гражданами³. Предполагается, что цифровые рубли будут использоваться, как и обычные купюры (монеты, банковские карты, электронные кошельки) с равным эквивалентом для наличного и безналичного расчетов.

Очевидно, что признание цифровой валюты допустимым платежным средством не способно связать официальными правилами обращение всех имеющих ценность виртуальных объектов. Спектр последних довольно широк, постоянно появляются новые виды криптографических конструкторов.

Как известно, разработка и запуск в 2009 г. первой децентрализованной платежной системы Bitcoin положило начало развитию целой индустрии и появлению нового термина «криптовалюта» [2, с. 355] – созданного с применением технологии блокчейн цифрового представления какого-либо актива (например, фиатных денежных средств). Приобретая новые формы, криптовалюты стали именоваться криптоактивами, которые по своим функциональным задачам разделились на те, которые используются в качестве платежей (Bitcoin, Altcoin, Stablecoin), и те, которые удостоверяют какие-либо имущественные права (Tokens). Часть названия «крипто-» объясняется использованием при создании актива криптографии, то есть специальной процедуры обеспечения конфиденциальности, аутентификации, шифрования и невозможности незаметного изменения

информации. Криптографический алгоритм служит для проверки и защиты транзакций, отражаемых в цифровом виде в системе распределенного реестра.

Термины «криптовалюта» и «криптоактив» стали широкоупотребимыми в обиходе российской публицистики, тогда как официальным термином зарубежного законодательства стал термин «виртуальная валюта». Напомним, что в 2013 г. Агентство по борьбе с финансовыми преступлениями Министерства финансов США (Financial Crimes Enforcement Network, далее – FinCEN) опубликовало Руководство по применению Правил для лиц, управляющих, обменивающих или использующих виртуальную валюту. Руководство определило данный объект как «средство обмена, которое работает как валюта в некоторых средах, но не обладает всеми атрибутами реальной валюты и не имеет статуса законного платежного средства ни в одной юрисдикции»⁴. Данное понятие было уточнено в докладе Европейского банковского управления (European Banking Authority) 2014 г.: «цифровое выражение стоимости, которое не выпускается центральным банком или государственным органом и не обязательно привязано к фиатной валюте, но принимается физическими или юридическими лицами в качестве средства обмена и может передаваться, храниться или продаваться в электронном виде»⁵.

В последующем понятие виртуальной валюты было расширено Директивой (ЕС) 2018/843 Европейского парламента и Совета от 30 мая 2018 г. о внесении поправок в Директиву (ЕС) 2015/849 «О предотвращении использования финансовой системы в целях отмывания денег или финансирования терроризма, а также о внесении изменений в Директивы 2009/138 / ЕС и 2013/36 / EU»: «цифровое представление стоимости, которое не выпущено или не гарантировано центральным банком или государственным органом, не обязательно привязано к законно установленной валюте и не обладает юридическим статусом валюты или денег, но принимается

4 Guidance FIN-2013-G001. March 18, 2013. Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencie [Электронный ресурс]. URL: <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf> (дата обращения: 05.07.2022).

5 EBA Opinion on 'virtual currencies'. 4 July 2014 [Электронный ресурс]. URL: <https://www.eba.europa.eu/sites/default/documents/files/documents/10180/657547/81409b94-4222-45d7-ba3b-7deb5863ab57/EBA-Op-2014-08%20Opinion%20on%20Virtual%20Currencies.pdf> (дата обращения: 05.07.2022).

2 Progress of Research & Development of E-CNY in China Working Group on E-CNY Research and Development of the People's Bank of China. July, 2021 [Электронный ресурс]. URL: <http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021072014364791207.pdf> (дата обращения: 05.07.2022).

3 Цифровой рубль: старт тестирования [Электронный ресурс]. URL: <https://cbr.ru/press/event/?id=12685> (дата обращения: 05.07.2022).

физическими или юридическими лицами в качестве средства обмена и которое может передаваться, храниться и продаваться в электронном виде»⁶. Сегодня в мире насчитывается более 1500 виртуальных валют [3, с. 9].

Как видно, по своему значению российский термин «криптовалюта» и зарубежный термин «виртуальная валюта» обозначают один класс объектов, имеющих одинаковый правовой режим (выпускаются и контролируются частным эмитентом и потому не подчиняются кредитно-денежной политике государства). В то же время криптовалюты могут быть централизованы (иметь единого администратора системы) или децентрализованы (когда специальный заданный программный алгоритм аутентифицирует транзакции, подтверждая подлинность переводов).

Основными преимуществами криптовалюты принято считать удобство в международных расчетах и значительное снижение стоимости транзакции за счет отсутствия посредников в виде банков [4, с. 130]. Однако все эти выгоды достигаются за счет нахождения рассматриваемых активов вне законодательства, регулирующего борьбу с отмыванием преступных доходов и финансированием терроризма (далее – ПОД/ФТ). Выпадая из-под контроля и государственного администрирования, система обеспечения крипторасчетов повышает риски осуществления незаконных операций.

Вовлечение все большего числа лиц в инвестиции и торговлю криптоактивами стимулирует правительства различных стран на поиск инструментов, позволяющих снизить криминальные риски в этой сфере. Как показала политическая практика, официальные регуляторы располагают выбором одного из двух подходов воздействия на данную отрасль.

Первого подхода придерживаются государства, принявшие решение ввести криптоактивы в сферу правового регулирования и сформировать соответствующую нормативно-правовую базу, позволяющую применять к их обороту налогообложение [5, с. 53] и законодательные средства по борьбе с отмыванием преступных доходов и финансированием терроризма. Так, в сентябре 2021 г. Сальвадор принял Bitcoin в качестве

законного платежного средства⁷. Согласно Отчету Управления глобальных юридических исследований Юридической библиотеки Конгресса США в 2021 г. 103 юрисдикции, включая государства – члены Европейского союза (за исключением Болгарии), применяли к криптовалютам налоговое законодательство и нормы ПОД/ФТ как отдельно, так и в рамках одного законодательного акта⁸.

Второй подход заключается в прямом или косвенном запрете государствами оборота криптоактивов при одновременном использовании инструментов деанонимизации проводимых транзакций. Сегодня в мире насчитывается 9 юрисдикций с абсолютным запретом на использование криптовалют и 42 – с неявным запретом⁹.

Оборот как легализованных, так и не признанных в качестве допустимых платежных средств видов виртуальной валюты привлекает внимание организаций, разрабатывающих международные стандарты для финансовых структур в части противодействия отмыванию преступных доходов и финансированию терроризма. Основные правила ПОД/ФТ в настоящее время формирует межправительственная организация Financial Action Task Force (далее – FATF), которая для этих целей в октябре 2018 г. включила в специальный глоссарий новый термин «виртуальные активы» – «цифровое представление стоимости, которое может быть продано или передано в цифровом виде, а также может быть использовано для оплаты или инвестиционных целей»¹⁰. Как видно, понятие виртуального актива перешагнуло границы виртуальной валюты, поскольку по своему технологическому исполнению виртуальный актив необязательно должен быть основан на структуре распределенного реестра и в него могут быть включены, например, артефакты сетевых компьютерных игр.

⁷ В Сальвадоре вступил в силу закон о признании биткойна официальным платежным средством [Электронный ресурс]. URL: <https://tass.ru/ekonomika/12316283> (дата обращения: 05.07.2022).

⁸ Regulation of cryptocurrency around the world : Albania, Algeria, Angola, Anguilla, Antigua and Barbuda, Argentina, Australia, Azerbaijan, Bahamas, Bahrain, Bangladesh, Belarus, Belgium / prepared by the Staff of the Global Legal Research Directorate. November, 2021. Washington, D.C.: The Law Library of Congress, Global Legal Research Directorate, 2021 [Электронный ресурс]. URL: <https://www.loc.gov/item/2021687419> (дата обращения: 05.07.2022).

⁹ Там же.

¹⁰ Glossary – Financial Action Task Force (FATF) [Электронный ресурс]. URL: <https://www.fatf-gafi.org/glossary/u-z/> (дата обращения: 07.07.2022).

⁶ Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance) [Электронный ресурс]. URL: <https://lexpance.org/eu/32018L0843/> (дата обращения: 05.07.2022).

«Поставщиком услуг виртуальных активов» глоссарий обозначил любое физическое или юридическое лицо, которое не подпадает под действие Рекомендаций FATF и в качестве бизнеса осуществляет одно или несколько из следующих действий или операций от имени другого физического или юридического лица: 1) обмен между виртуальными активами и фиатными валютами; 2) обмен между одной или несколькими формами виртуальных активов; 3) передачу виртуального актива (проведение транзакции от имени другого физического или юридического лица, которая перемещает виртуальный актив с одного адреса или учетной записи виртуального актива на другой); 4) хранение и (или) управление виртуальными активами или инструментами, позволяющими контролировать виртуальные активы; 5) участие/предоставление финансовых услуг, связанных с предложением эмитента и (или) продажей виртуального актива¹¹.

Предложенные FATF определения «виртуального актива» и «поставщика услуг виртуальных активов» свидетельствуют о значительных подвижках в официальной позиции организации. Признание высокорискованными с точки зрения отмывания денег и финансирования терроризма сделок по обмену виртуальных активов между собой, а также на фиатные валюты привело к отмене Руководства FATF по риск-ориентированному подходу к виртуальным валютам 2015 г.¹² и принятию нового Руководства 2019 г., которое не только признало появление новых рисков в сфере регулирования ПОД/ФТ, но и расширило круг провайдеров услуг в криптосфере¹³.

ГОСУДАРСТВЕННЫЕ ПОДХОДЫ

Лавинообразное приумножение видов виртуальных активов, увеличение объема транзакций с ними побуждает национальные контролирующие органы реагировать на возникающие в связи с этим значительные криминальные риски. Учитывая, что виртуальные активы используют в своей преступной

деятельности представители так называемой высокотехнологичной преступности [6, с. 122], большинство юрисдикций с развитыми финансовыми рынками поступательно вводят ограничительные меры, направленные на преодоление анонимности в цифровой среде¹⁴.

Вынужденная необходимость государств препятствовать отмыванию преступных доходов, торговле людьми и наркотиками, финансированию терроризма и распространению оружия массового поражения объективно сближает оба подхода в попытках контролировать оборот виртуальных активов, будь то легализация отдельных видов криптовалют или их полный запрет. Такое сближение становится очевидным на фоне стремления привести национальные законодательства в соответствие с нормами ПОТ/ФТ в части регулирования оборота виртуальных активов. Значение данной работы определяются тем, что ограниченные возможности по деанонимизации всех участников операций с виртуальными активами не просто опасно, но создает вызов для действующей глобальной системы ПОД/ФТ и потому обуславливает необходимость ее совершенствования¹⁵.

Шагом революционного значения на пути формирования ответа новым вызовам стало опубликование 21 сентября 2021 г. Управлением по контролю за иностранными активами Министерства финансов США (далее – OFAC) Рекомендации о потенциальных санкционных рисках за содействие выплатам с помощью программ-вымогателей¹⁶ (далее – Рекомендация). Не являясь законом, имея статус консультативного заключения, данный документ тем не менее разъяснил порядок реагирования государственных органов

14 Jurisdictions move towards full implementation of standards for financial market infrastructures. Press release Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions. 08 April, 2020 [Электронный ресурс]. URL: https://www-bis-org.translate.google.com/press/p200408.htm?x_tr_sl=en&x_tr_tl=ru&x_tr_hl=ru&x_tr_pto=op,sc (дата обращения: 07.07.2022).

15 Криптовалюты: тренды, риски, меры: доклад для общественных консультаций. Информация Центрального Банка Российской Федерации, 2022 г. [Электронный ресурс]. URL: https://cbr.ru/Content/Document/File/132241/Consultation_Paper_20012022.pdf (дата обращения: 05.07.2022).

16 Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments. 2021. September. Department of the treasury. Washington, D.C. [Электронный ресурс]. URL: https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf (дата обращения: 30.06.2022).

11 Там же.

12 Guidance for a Risk-Based Approach to Virtual Currencies. FATF [Электронный ресурс]. URL: <https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf> (дата обращения: 07.07.2022).

13 Виртуальные активы и провайдеры услуг виртуальных активов: руководство по применению риск-ориентированного подхода. FATF. Июнь, 2019 [Электронный ресурс]. URL: <https://www.fatf-gafi.org/media/fatf/documents/recommendations/MUMCFM-FATF-Guidance-RBA-VA-VASPs.pdf> (дата обращения: 07.07.2022).

США на выявленные риски незаконных финансовых операций в связи с использованием вредоносного программного обеспечения. Согласно Рекомендации государственные органы США оставляют за собой право применять законодательство о санкциях против криптовалютных бирж, уличенных в содействии выплатам киберпреступникам денежных средств путем конвертации виртуальных активов, полученных в результате использования для вымогательства специального программного обеспечения – RaaS (англ. ransomware-as-a-service – программа-вымогатель как услуга).

СПЕЦИАЛИЗИРОВАННЫЙ СПИСОК

Достаточным основанием для введения ограничений (санкций) является размещение OFAC данных физического или юридического лица в «Списке особо назначенных граждан и заблокированных лиц» (далее – SDN)¹⁷, где перечисляются субъекты, с которыми гражданам, постоянным жителям США, включая юридических лиц, запрещено вести бизнес. Обновление SDN сопровождается размещением на официальном сайте OFAC всей необходимой информации, поясняющей внесение дополнений.

Список неоднороден и включает две основные категории лиц: 1) исполнителей атак, использующих программы-вымогатели; 2) тех, кто способствует транзакциям активов, полученных с использованием программ-вымогателей. В целом санкции могут быть направлены на любого участника индустрии – технологические компании, обменники, администраторов, майнеров, поставщиков кошельков и пользователей.

Так, в число исполнителей атак OFAC включила российскую киберпреступную организацию Evil Corp и в декабре 2019 г. ввела против нее санкции за разработку и распространение вредоносного программного обеспечения Dridex¹⁸, с помощью которого происходило заражение компьютеров и собирались учетные данные для входа в сотни банков и финансовых учреждений в более чем

17 Specially Designated Nationals And Blocked Persons List (SDN). U.S. Department of the Treasury [Электронный ресурс]. URL: <https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists> (дата обращения: 07.07.2022).

18 Суд США в рамках «дела Bugat» запретил трем россиянам использовать вредоносное ПО [Электронный ресурс]. URL: https://rapsinews.ru/international_news/20200113/305301592.html (дата обращения: 07.07.2022).

40 странах, что привело к краже более 100 млн долларов¹⁹.

Однако в большей степени Рекомендация направлена на применение санкционных инструментов в отношении лиц, оказывающих содействие платежам, проводимым в связи с использованием программ-вымогателей – криптовалютных бирж и обменников виртуальной валюты. Главная цель документа – воспрепятствовать криминальной спайке криптоагрегаторов с кибервымогателями на этапе конвертации виртуальных активов в фиатную валюту. При обналачивании виртуальных активов киберпреступники наиболее уязвимы, что используется Министерством финансов США для их выявления и последующей борьбы с преступной деятельностью.

Для отслеживания незаконных операций с виртуальными активами используются программные инструменты, специально разрабатываемые аналитическими компаниями (Chainalysis, Coinfirm, An Chain, Crystal, Ciphertrace, Elliptic, Titanium и др.). Современные технологические возможности позволяют проследить цепочку совершенных транзакций и установить учетную запись бенефициара до определения его учетной записи на криптобирже или обменнике виртуальной валюты, где финансовые правила требуют от пользователей подтверждения своей личности.

РЕЖИМ САНКЦИЙ

Законодательство США в качестве санкций предусматривает ряд ограничений, основными из которых являются:

а) аннулирование лицензии на ведение деятельности, связанной с оборотом виртуальных активов;

б) запрет на ведение с подпадавшим под санкции лицом какой-либо коммерческой деятельности;

в) запрет сотрудничества санкционируемого с официальными органами государственного контроля;

г) замораживание активов лица, на которое наложены санкции.

Некоторые санкции могут носить характер секторальных запретов, предусматривающих ограничение на проведение финансовых операций с конкретными предприятиями

19 Treasury Department Sanctions Evil Corp, the Russian Cybercriminal Group Behind the Dridex Malware [Электронный ресурс]. URL: https://home-treasury.gov.translate.google.com/news/press-releases/sm845?_x_tr_sl=en&_x_tr_tl=ru&_x_tr_hl=ru&_x_tr_pto=sc (дата обращения: 07.07.2022).

определенных отраслей, а также запрет на предоставление какой-либо помощи объектам контроля.

Следование нормативному регулированию США в части, касающейся оборота криптоактивов, может быть достаточно непростой задачей, сопряженной с рядом жестких требований: регистрация на федеральном уровне, внедрение программ по борьбе с отмытием доходов и получение лицензии на переводы денежных средств на уровне штата. При этом универсальной лицензии для работы по всей стране не существует, поскольку у правительств штатов имеются разные подходы к определению и регулированию виртуальных валют. Десять таких государственно-территориальных образований активно внедряют криптоиндустрию, в трех штатах введены достаточно жесткие требования, но большинство относится нейтрально к данной отрасли²⁰.

Так, федеральное законодательство США, регулирующее криптовалюту как товар, предписывает фирмам, осуществляющим ее оборот, быть зарегистрированными как предприятия, занимающиеся переводом или конверсией денежных средств, с регистрацией и получением соответствующей лицензии MSB²¹, в каждом штате, кроме Монтаны. Получение лицензии MSB в США – необходимая процедура для ведения финансовой деятельности. Главным регулятором здесь выступает Закон США о банковской тайне (BSA)²², а основным контролирующим и надзорным органом – FinCEN.

После регистрации фирмы, осуществляющей операции с виртуальными активами, в FinCEN и получения лицензии в тех штатах, где она намеревается работать, организация обязана на постоянной основе самостоятельно отслеживать любые законодательные изменения на федеральном уровне и на уровне

20 Money Transmitter Registration And Licensing: U.S. Cryptocurrency Entities. A Brief Overview of the Cryptocurrency Industry. February 24, 2021 [Электронный ресурс]. URL: https://www-sia-partners-com.translate.goog/en/news-and-publications/from-our-experts/money-transmitter-registration-and-licensing-us?_x_tr_sl=en&_x_tr_tl=ru&_x_tr_hl=ru&_x_tr_pto=sc (дата обращения: 06.07.2022).

21 Fact Sheet on MSB Registration Rule. Glossary. An official website of the United States Government [Электронный ресурс]. URL: https://www-fincen-gov.translate.goog/fact-sheet-msb-registration-rule?_x_tr_sl=en&_x_tr_tl=ru&_x_tr_hl=ru&_x_tr_pto=sc (дата обращения: 05.07.2022)

22 The Bank Secrecy Act of 1970 (BSA). U.S. Legislation [Электронный ресурс]. URL: <https://www-fincen-gov/resources/statutes-and-regulations/bank-secrecy-act> (дата обращения: 05.07.2022).

субъекта. Это строгое обязательство, так как изменение нормативных документов может осуществляться достаточно быстро, без каких-либо консультаций и заблаговременного предупреждения. В этой связи криптоагрегаторы обязаны постоянно отслеживать открытые интернет-ресурсы Министерства финансов США, а также порталы отчетности лицензируемых штатов.

В Кодексе Соединенных Штатов Америки, в разделе 18 «Преступления и уголовный процесс», предусмотрена уголовная ответственность за нарушение лицензии, выданной на операции по переводу. Наказание предполагает наложение крупного денежного штрафа либо лишение свободы сроком до 5 лет²³. Подобная ситуация может сложиться в случае, если лицо не прошло регистрацию в FinCEN или работает в штате без соответствующей лицензии. При этом термин «не лицензируемый бизнес по переводу денег» в диспозиции статьи рассматривается достаточно широко, охватывая всю деятельность, которая каким-либо образом или в какой-либо степени влияет на межгосударственную или иностранную торговлю.

Весьма значимо обстоятельство: Министерство финансов США не принимает во внимание международно-правовую юрисдикцию объекта санкционного контроля, которая не имеет значения для исполнения запретов. Достаточным основанием введения ограничений считается факт причинения ущерба гражданам США. Любая транзакция, совершенная вопреки требованиям Закона о международных чрезвычайных экономических полномочиях (IEEPA)²⁴, включая транзакцию лица, не являющегося гражданином США, но которая заставляет гражданина США нарушать какие-либо запреты на санкции, основанные на этом законе, также рассматривается как запрещенная.

Демонстрацией обеспечения соблюдения наложенных санкций на объект, расположенный в другой юрисдикции, стало включение в SDN внебиржевого криптовалютного брокера SUEXOTC S.R.O. (далее – Suex), также

23 U.S. Code. Title 18. Part I. Chapter 95. § 1960. – Prohibition of unlicensed money transmitting businesses [Электронный ресурс]. URL: https://www-law-cornell-edu.translate.goog/uscode/text/18/1960?_x_tr_sl=en&_x_tr_tl=ru&_x_tr_hl=ru&_x_tr_pto=sc (дата обращения: 06.07.2022).

24 The International Emergency Economic Powers Act (IEEPA), Title II of Pub.L. 95–223, 91 Stat. 1626, enacted October 28, 1977 [Электронный ресурс]. URL: <https://www-congress-gov/bill/95th-congress/house-bill/7738> (дата обращения: 06.07.2022).

известного как «Успешный обмен»²⁵. Данный агрегатор имел регистрацию в Чехии (Прага), а его фактическое местонахождение было определено Министерством финансов США в России (Москва)²⁶. Указом Президента США № 13694 от 1 апреля 2015 г.²⁷ введен запрет американским гражданам на любые формы взаимодействия с данной компанией.

Основанием для введения ограничений послужило аналитическое исследование IT-компании Chainalysis, проведенное во взаимодействии с государственным американским финансовым органом. Согласно предоставленным данным, Suex конвертировал криптовалюту на сотни миллионов долларов, большая часть которой поступала из незаконных и высокорискованных источников. В одной только криптовалюте Bitcoin депозитные адреса агрегатора, размещенные на крупных биржах, получили более 160 млн долларов от участников программ-вымогателей, мошенников и операторов рынка DarkNet. Расследование Chainalysis показало, что Suex переводил криптовалюту в наличные денежные средства в филиалах, расположенных в Москве и Санкт-Петербурге, а также, возможно, в других офисах за пределами России. По мнению аналитиков Chainalysis, Suex являлся одним из самых крупных и активных сервисов, предоставлявших незаконные услуги по отмыванию денег для всех преступлений, связанных с криптовалютой²⁸. Таким образом, введенные Министерством финансов США санкции в отношении Suex имели целью поставить под контроль операции, связанные с конвер-

тацией незаконно полученной криптовалюты в фиатную, и сделали весьма затруднительным для киберпреступников процесс перевода и размещения похищенных денежных средств на криптоагрегаторах.

Особого внимания заслуживает пример проведенного 5 апреля 2022 г. мероприятия при участии Министерства юстиции США, Федерального бюро расследований, Управления по борьбе с наркотиками, Налоговой службы по уголовным делам, Службы расследований национальной безопасности США и Федеральной уголовной полиции Германии в отношении HydraMarket (далее – Hydra) – крупнейшего маркетплейса русскоязычного криминального сегмента DarkNet. В рамках осуществленных мероприятий по предотвращению распространения вредоносных киберпреступных сервисов, а также сбыта наркотиков с использованием Интернета на территории ФРГ были отключены серверы Hydra и конфискованы виртуальные активы в Bitcoin на сумму 25 млн долларов США. По мнению государственных органов США, маркетплейс Hydra, открытый в 2015 г., являлся самым крупным в мире рынком торговли запрещенными веществами, предоставляя в числе прочих и различные хакерские услуги, включая программы-вымогатели. Согласно проведенному расследованию, доходы от последнего вида незаконной деятельности составили 8 млн долларов, которые прошли через виртуальные счета Hydra. Отмечено, что порядка 86 % Bitcoins, незаконно полученных российскими биржами виртуальных валют в 2019 г., поступило именно от Нудра. До действий правоохранительных органов США выручка Hydra резко выросла с менее чем 10 млн долларов в 2016 г. до более 1,3 млрд долларов в 2020 г. Такой рост прибыли был возможен из-за связи Hydra с российскими незаконными финансами²⁹.

Помимо самого Hydra Управление по контролю за иностранными активами Министерства финансов США включило в SDN биржу виртуальной валюты GARANTEX EUROPE OU (далее – Garantex)³⁰. Государственными органами США объявлено, что основанная

25 Treasury Takes Robust Actions to Counter Ransomware. U.S. Department of the Treasury. Press Releases. September 21, 2021 [Электронный ресурс]. URL: https://home-treasury.gov.translate.googleusercontent.com/news/press-releases/jy0364?x_tr_sl=en&x_tr_tl=ru&x_tr_hl=ru&x_tr_pto=sc (дата обращения: 06.07.2022).

26 Publication of Updated Ransomware Advisory; Cyber-related Designation. U.S. Department of the Treasury. September 21, 2021 [Электронный ресурс]. URL: https://home-treasury.gov.translate.googleusercontent.com/policy-issues/financial-sanctions/recent-actions/20210921?x_tr_sl=en&x_tr_tl=ru&x_tr_hl=ru&x_tr_pto=sc (дата обращения: 05.07.2022).

27 Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities. Executive Order. April 01, 2015 [Электронный ресурс]. URL: https://obamawhitehouse.archives.gov.translate.googleusercontent.com/press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m?x_tr_sl=en&x_tr_tl=ru&x_tr_hl=ru&x_tr_pto=op,sc (дата обращения: 07.07.2022).

28 Chainalysis in Action: OFAC Sanctions Russian Cryptocurrency OTC Suex that Received Over \$160 million from Ransomware Attackers, Scammers, and Darknet Markets. September 22, 2021 [Электронный ресурс]. URL: <https://blog.chainalysis.com/reports/ofac-sanction-suex-september-2021> (дата обращения: 06.07.2022).

29 U.S. Department of the Treasury. Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex. Press Releases. April 5, 2022 [Электронный ресурс]. URL: https://home-treasury.gov.translate.googleusercontent.com/news/press-releases/jy0701?x_tr_sl=en&x_tr_tl=ru&x_tr_hl=ru&x_tr_pto=sc (дата обращения: 06.07.2022).

30 U.S. Department of the Treasury. Specifically Designated Nationals List Update. May 04, 2022 [Электронный ресурс]. URL: <https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20220405> (дата обращения: 06.06.2022).

в 2019 г. и зарегистрированная изначально в Эстонии указанная биржа фактически осуществляла свою деятельность на территории России. Однако в феврале 2022 г. Garantex лишилась лицензии на предоставление услуг по обмену виртуальной валюты по причине нарушений законодательства в сфере ПОД/ФТ, выявленных Службой финансовой разведки Эстонии. Так, было обнаружено взаимодействие между Garantex и виртуальными кошельками, используемыми для криминальной деятельности, с транзакциями на сумму более 100 млн долларов, в том числе около 2,6 млн долларов – с Hydra.

Введенные в отношении Hydra и Garantex санкции выразились в блокировании действий со всем имуществом и интересом в собственности физических или юридических лиц, находящихся в США или под контролем лиц США. Все финансовые операции, включающие в себя внесение любого вклада или предоставление средств, товаров, услуг любым заблокированным лицом или в его пользу, а также получение любого вклада или предоставление средств, товаров, совершаемые лицами из США или в пределах США, находятся под запретом.

СИСТЕМА КОМПЛАЕНС

Организационно-правовая деятельность Министерства финансов США со всей очевидностью показывает решительность, с которой государственный аппарат намерен активизировать работу по продвижению санкционной политики. Выделяемые для этого значительные административные и материальные ресурсы способствуют углублению межведомственного взаимодействия органов и учреждений. Гарантией же эффективности санкционного режима является вменение обязанности администратору ресурса внедрять систему комплаенс, предусматривающую осуществление внутреннего контроля за доставкой платежа, полученного, например, в результате использования программы-вымогателя. Невыполнение данной обязанности всегда влечет ответственность, даже если администратор не знал или не имел оснований знать, что он участвовал в сделке, которая была запрещена законами и правилами о санкциях, вводимыми OFAC. Таким образом, механизм комплаенса становится обязательным, заставляет администратора криптобиржи или обменника виртуальной валюты получать сведения и удостоверяться

в получателе средств платежа. Тем самым комплаенс нивелирует уклонение от санкций с помощью виртуальной валюты [7, с. 42].

Чтобы помочь общественности в разработке эффективной программы соблюдения санкций, в 2019 г. OFAC опубликовало «Концепцию обязательств Управления по контролю за иностранными активами по соблюдению требований»³¹. Документ настоятельно рекомендует организациям, подпадающим под юрисдикцию США, а также иностранным организациям, которые ведут бизнес в Соединенных Штатах или с ними, лицам из США или использующим товары/услуги американского происхождения применять риск-ориентированный подход к соблюдению санкций путем разработки, внедрения и регулярного обновления программы соблюдения санкций (SCP). Каждая программа вне зависимости от особенностей и условий применения должна включать пять основных компонентов: (1) обязательства руководства, (2) оценка рисков, (3) внутренний контроль, (4) тестирование и аудит, (5) обучение. Согласно официальной позиции, все перечисленные условия в полной мере распространяются и на компании, аффилированные с криптоагрегаторами – организациями, занимающимися предоставлением услуг по киберстрахованию, цифровой криминалистике, реагированию на киберинциденты, а также предоставляющими финансовые услуги, включающие обработку платежей с выкупом.

Функционирование системы комплаенс-контроля обеспечивается криптоагрегаторами путем выполнения рекомендаций по внедрению в деятельность специализированных программ, позволяющих в автоматическом режиме проводить оценку рисков, связанных с нарушением наложенных санкций. Расширяя сферу предупреждения рисков, 9 марта 2022 г. Президент США издал «Исполнительный указ об обеспечении ответственного развития цифровых активов»³², в котором наряду с описанием государственной стратегии по развитию цифровых технологий отмечена опасность возможного использования

31 A Framework for OFAC Compliance Commitments. Department of the treasury. Washington, D.C. 20220 [Электронный ресурс]. URL: https://home.treasury.gov/system/files/126/framework_ofac_cc.pdf (дата обращения: 07.07.2022).

32 Executive Order on Ensuring Responsible Development of Digital Assets. March 09, 2022. Presidential Actions [Электронный ресурс]. URL: <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/> (дата обращения: 07.07.2022).

виртуальных активов в качестве инструмента для обхода режима финансовых санкций. В развернутых правилах по недопущению обхода санкций, введенных против внешней деятельности России, Министерство финансов США предписывает своим гражданам, где бы они ни находились, в ходе совершения сделок с виртуальной валютой руководствоваться инструкциями OFAC³³, а также рекомендациями FinCEN от 7 марта 2022 г.³⁴

Исходя из понимания, что находящиеся под санкциями лица могут использовать виртуальные активы вкупе с инструментами анонимизации, суть принятых инструкций и правил сводится к ряду комплаенс-требований. Организации, предоставляющие услуги по обороту криптоактивов, должны проводить тщательную комплексную проверку для изучения всех потенциальных угроз, включая глобальные операций клиентов, деловых партнеров и сотрудников из регионов, находящихся под санкциями.

Так, участники оборота виртуальных активов обязуются обеспечить наличие и функционирование средств контроля know your customer (англ. – знай своего клиента) и anti-money laundering (англ. – борьба с отмыванием денег) в их соответствии отраслевым финансовым требованиям, указанным в нормативных актах. С целью выявления подставных компаний и виртуальных активов, используемых для сокрытия прав собственности и финансовых потоков, криптоагрегаторам рекомендуется использовать следующие автоматизированные банковские системы: скрининг геолокации, программы достоверной идентификации контрагентов клиента, мониторинг IP-адресов, а также обновляемые программы проверки списков OFAC. При этом операция будет отнесена к разряду подозрительных, если:

– транзакции клиента инициируются или отправляются на IP-адреса из ненадежных источников, из криптоадресов, ранее помеченных как подозрительные, а также находящиеся под санкциями юрисдикций, и т. п.;

33 Russian harmful foreign activities sanctions. 1021. Do the prohibitions of Executive Order (E.O.) 14024 and other Russia-related sanctions extend to virtual currency? U.S. Department of the Treasury [Электронный ресурс]. URL: <https://home.treasury.gov/policy-issues/financial-sanctions/faqs/1021> (дата обращения: 07.07.2022).

34 FinCEN Advises Increased Vigilance for Potential Russian Sanctions Evasion Attempts. FIN-2022-Alert001. March 7, 2022 [Электронный ресурс]. URL: <https://www.fincen.gov/sites/default/files/2022-03/FinCEN%20Alert%20Russian%20Sanctions%20Evasion%20FINAL%20508.pdf> (дата обращения: 07.07.2022).

– транзакции клиента связаны с криптовалютными адресами, внесенными в список особо обозначенных граждан и заблокированных лиц OFAC;

– клиент использует биржу виртуальных активов или иностранный бизнес по обслуживанию денег в юрисдикции с высоким уровнем риска (Россия, Иран и др.);

– клиент получает виртуальный актив из внешнего кошелька и немедленно инициирует несколько быстрых сделок между несколькими криптовалютами без очевидной цели, после чего следует транзакция вне платформы, в возможной попытке запутать транзакцию;

– программное обеспечение для отслеживания цепочки блоков определяет, что клиент прямо или косвенно подтвержден транзакциями кода CVC (англ. – проверка карты), связанной с атакой программ-вымогателей³⁵.

Использование указанных инструментов в рамках комплаенс-контроля позволяет выявлять попытки участников операций и аффилированных с ними лиц обойти финансовые санкции и препятствовать осуществлению конвертации виртуальных активов, полученных преступным путем (прежде всего, от применения программ-вымогателей), в фиатную валюту.

Уязвимости режима санкций и системы комплаенс

Используемый США режим санкций и связанный с ним комплаенс-контроль не лишены уязвимостей, две из которых являются основными.

Первая уязвимость состоит в постоянном усложнении введенных санкций. В условиях расширения возможностей и усиления внимания фискальных органов к проблеме оборота виртуальных активов такое усложнение создает повышенную регуляторную проблему рисков и для граждан США, и для взаимодействующих с ними субъектов бизнеса, особенно финансовых учреждений и финтех-компаний.

Вторая уязвимость следует из несформированности единой позиции разных органов и учреждений относительно перечня и статуса виртуальных активов, подлежащих контролю. На административном и ведомственном уровне криптовалюту как объект контроля рассматривают сразу несколько федеральных органов: Комиссия по торговле товарными фьючерсами (CFTC), Комиссия по ценным

35 Там же.

бумагам и биржам США (SEC), Федеральная торговая комиссия (FTC), Налоговая служба США (IRS), Управление валютного контроля (OCC), Федеральный резерв (FED) и FinCEN.

При формировании позиции по регулированию виртуальных активов каждый из перечисленных регуляторов исходит из специфики выполнения им поставленных задач. В одних случаях криптовалюта представляется как ценная бумага, в других – как товар, в третьих – как собственность. Так, в своих правилах FinCEN разъяснило, что с точки зрения законодательства о денежных переводах оно не проводит различий между фиатной и виртуальной валютой³⁶. Согласно информации этого надзорного органа основной операцией, осуществляемой подпадающими под контроль лицензиатами, является денежный перевод, представляющий собой прием виртуальной валюты от одной стороны другой стороне и наоборот, либо даже обычный прием криптовалюты клиентов от имени продавца. При этом частные лица и предприятия, которые обменивают криптовалюту на товары и услуги и наоборот, под нормативное регулирование правил FinCEN не подпадают. Таким образом, виртуальный актив в зависимости от использования может рассматриваться как товар либо фиатная валюта, что затрудняет контроль за выполнением санкций.

Российский опыт

Российская Федерация следует глобальному мировому тренду, направленному на контроль оборота виртуальных активов с помощью национальных законодательных инструментов. Сегодня в стране последовательно формируется нормативная правовая база, в которой определяется глоссарий, порядок выпуска и обращения виртуальных активов, закрепляются требования по идентификации, учету и сертифицированию участников цифровой индустрии.

Согласно докладу председателя Правительства РФ М.В. Мишустина, представленного Государственной Думе в 2022 г., объем хранимых российскими гражданами виртуальных активов превышает 10 трлн рублей. При этом официальная позиция в отношении криптовалюты как законного средства платежа

остаётся осторожной³⁷. Тем не менее в вопросе регулирования оборота виртуальных активов органы власти продолжают законодательную деятельность, направленную на стимулирование инвестиций в данную отрасль и создание соответствующей инфраструктуры.

Значимыми шагами на данном пути стали разработанные Министерством финансов РФ законопроекты: «О цифровой валюте»³⁸ и «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О цифровой валюте»³⁹. Указанные проекты появились в связи с поручением Правительства РФ в целях необходимости создания нормативной правовой базы для осуществления легальной деятельности, связанной с совершением операций с цифровыми валютами и их выпуском. Среди предлагаемых Минфином России мер указаны:

- установление требования к биржам и обменникам, осуществляющим оборот цифровых валют (включая иностранные), об осуществлении регистрации на территории России с одновременным созданием их специального реестра. При этом сама деятельность криптоагрегаторов предполагает лицензирование и контроль специально уполномоченным органом Правительства РФ;

- принятие условия конвертации криптовалюты в фиатные деньги и обратно только через расчетный счет, открытый в российском банке. Таким образом предполагается идентифицировать владельца виртуального актива как в ходе регистрации клиента на криптоплатформе, так и в ходе открытия им банковского счета;

- введение процедуры ПОД/ФТ всеми участниками оборота цифровых валют, информирование подразделений финансовой разведки о выявленных подозрительных транзакциях. Биржи и обменники будут обязаны вести

37 В криптокошельках россиян больше 10 трлн рублей [Электронный ресурс]. URL: <https://rg.ru/2022/04/07/mishustin-v-kriptokoshelkah-rossiian-bolshe-10-trln-rublej.html> (дата обращения: 07.07.2022).

38 О цифровой валюте : проект нормативно-правового акта Минфина России от 17.02.2022. ID проекта 02/04/02-22/00125083 [Электронный ресурс]. URL: <https://regulation.gov.ru/projects#nra=125083> (дата обращения: 07.03.2022).

39 внесения изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О цифровой валюте» : проект нормативно-правового акта Минфина России от 17.02.2022. ID проекта 02/04/02-22/00125084 [Электронный ресурс]. URL: <https://regulation.gov.ru/projects#nra=125084> (дата обращения: 07.03.2022).

36 Guidance FIN-2013-G001. March 18, 2013. Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencie [Электронный ресурс]. URL: <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf> (дата обращения: 06.07.2022).

реестры с указанием адресов – идентификаторов каждого обладателя цифровых валют;

– закрепление понятия цифрового майнинга и фискального механизма налоговых органов.

Указанные меры по своему содержанию и направленности свидетельствуют о начале формирования в российском правовом поле системы контроля выпуска и оборота виртуальных активов.

ЗАКЛЮЧЕНИЕ

Проведенное сравнительно-правовое исследование позволяет сформулировать ряд значимых для уголовной политики современной России положений.

1. Интересы предупреждения легализации преступно нажитых доходов и финансирования терроризма предполагают расширение контролирующей функции государства в отношении оборота всех видов виртуальных активов – как легализованных (цифровая валюта), так и не признанных в качестве допустимых платежных средств (криптовалюта, токены, игровые артефакты и т. д.).

2. Ограниченные возможности государственного контроля за оборотом виртуальных активов могут быть компенсированы введением режима санкций в отношении участников обмена и конвертации виртуальных активов,

полученных преступным путем (прежде всего, криптобирж и обменников криптовалюты), независимо от международно-правовой юрисдикции.

3. Выполнение санкционного режима может быть достигнуто путем внедрения в деятельность участников оборота виртуальных активов системы комплаенс, направленной, прежде всего, на преодоление анонимности в цифровой среде.

4. Компании и физические лица, не исполняющие санкции, должны нести юридические, репутационные и коммерческие риски. При формировании данной системы необходимо принимать во внимание уязвимости режима санкций и комплаенс-контроля: (1) постоянное усложнение введенных санкций, увеличивающее вероятность их несоблюдения и (2) несформированность единой позиции разных органов и учреждений относительно перечня и статуса виртуальных активов в разных юрисдикциях, снижающее согласованность контроля и в условиях кризиса международного права неизбежно приводящее к превосходству национальных инструментов.

Данные положения должны учитываться при формировании дальнейших законодательных инициатив российских органов государственной власти в сфере определения статуса разных видов виртуальных активов и контроля за их оборотом.

СПИСОК ИСТОЧНИКОВ

1. Vondráčková A. Regulation of Virtual Currency in the European Union // Charles University in Prague Faculty of Law Research Paper. – 2016. – № 3. URL: <http://dx.doi.org/10.2139/ssrn.2896911>.

2. Родичева В.Б. Криптовалюта: история происхождения и развитие / В.Б. Родичева // Российские регионы в фокусе перемен : сборник докладов XII Международной конференции. – Екатеринбург, 2018. – С. 355–357.

3. Dabrowski M. Virtual Currencies and Their Potential Impact on Financial Markets and Monetary Policy / M. Dabrowski, L. Janikowski // CASE Research Paper. – 2018. – № 495. – 46 p.

4. Кочергин Д.А. Место и роль виртуальных валют в современной платежной системе / Д.А. Кочергин // Вестник Санкт-Петербургского университета. Экономика. – 2017. – Т. 33, вып. 1. – С. 119–140.

5. Кочергин Д.А. Международный опыт налогообложения криптоактивов / Д.А. Кочергин, Н.В. Покровская // Экономический журнал ВШЭ. – 2020. – № 1. – С. 53–84.

6. Высокотехнологичная преступность: новые вызовы для общества, государства и бизнеса : материалы круглого стола Комитета гражданских инициатив // Индекс безопасности. – 2016. – Т. 22, № 1 (116). – С. 121–136.

REFERENCES

1. Vondráčková A. Regulation of Virtual Currency in the European Union. Charles University in Prague Faculty of Law Research Paper, 2016, no. 3. Available at: <http://dx.doi.org/10.2139/ssrn.2896911>.

2. Rodicheva V.B. Cryptocurrency: history of origin and development. Rossijskie regiony v fokuse peremen. Sbornik dokladov XII Mezhdunarodnoj konferencii [Russian regions in the focus of change. Collection of reports of the XII International Conference]. Yekaterinburg, 2018, pp. 355–357. (In Russian).

3. Dabrowski M., Janikowski L. Virtual Currencies and Their Potential Impact on Financial Markets and Monetary Policy. CASE Research Paper, 2018, no. 495. 46 p.

4. Kochergin D.A. The roles of virtual currencies in the modern payment system. Vestnik Sankt-Peterburgskogo universiteta. Ekonomika = St Petersburg University Journal of Economic Studies, 2017, vol. 33, iss. 1, pp. 119–140. (In Russian).

5. Kochergin D.A., Pokrovskaja N.V. International Experience of Taxation of Cryptoassets. Ekonomicheskij zhurnal VSHE = HSE Economic Journal, 2020, no. 1, pp. 53–84. (In Russian).

6. High-tech crime: new challenges for society, state and business. Materials of the round table of the Committee of

7. Kirkpatrick K. Virtual currency in sanctioned jurisdictions: stepping outside of SWIFT / K. Kirkpatrick, C. Savage, R. Johnston, M. Hanson // Journal of Investment Compliance. – 2019. – Vol. 20, № 2. – P. 39–44.

Civil Initiatives. Indeks bezopasnosti = Safety Index, 2016, vol. 22, no. 1 (116), pp. 121–136. (In Russian).

7. Kirkpatrick K., Savage C., Johnston R., Hanson M. Virtual currency in sanctioned jurisdictions: stepping outside of SWIFT. Journal of Investment Compliance, 2019, vol. 20, no. 2, pp. 39–44.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Фильченко Андрей Петрович – доктор юридических наук, профессор, заместитель начальника кафедры уголовной политики Академии управления МВД России;

Жандров Владимир Юрьевич – кандидат юридических наук, доцент кафедры оперативно-разыскной деятельности и специальной техники Московского университета МВД России им. В.Я. Кикотя.

INFORMATION ABOUT THE AUTHOR

Filchenko Andrey Petrovich – Doctor of Law, Professor, Deputy Head of the Department of Criminal Policy, Academy of Management of the Ministry of Internal Affairs of Russia;

Zhandrov Vladimir Yuryevich – Candidate of Sciences (Law), Associate Professor of the Department of Operative Investigative Activities and Special Equipment, Vladimir Kikot Moscow University of the Ministry of Internal Affairs of Russia.

Статья поступила в редакцию 19.06.2022; одобрена после рецензирования 14.07.2022; принята к публикации 15.07.2022. The article was submitted 19.06.2022; approved after reviewing 14.07.2022; accepted for publication 15.07.2022.