СЛЕДСТВЕННЫЙ КОМИТЕТ РОССИЙСКОЙ ФЕДЕРАЦИИ

МОСКОВСКАЯ АКАДЕМИЯ СЛЕДСТВЕННОГО КОМИТЕТА
РОССИЙСКОЙ ФЕДЕРАЦИИ

ИСПОЛЬЗОВАНИЕ КРИПТОВАЛЮТ В ПРОТИВОПРАВНЫХ ЦЕЛЯХ И МЕТОДИКА ПРОТИВОДЕЙСТВИЯ

материалы Международного научно-практического «круглого стола»

(Москва, 25 апреля 2019 года)

Москва, 2019

УДК 343
ББК 67.408
И 88

И 88 Использование криптовалют в противоправных целях и методика противодействия: материалы Международного научно-практического «круглого стола» (Москва, 25 апреля 2019 года) / под общ. ред. А.М. Багмета. – М.: Московская академия Следственного комитета Российской Федерации, 2019. – 129 с.

ISBN 978-5-6041504-7-4

УДК 343
ББК 67.408

Сборник сформирован по материалам, представленным на Международном научно-практическом «круглом столе», проведенном в Московской академии СК России 25 апреля 2019 года.

Форум проведен Московской академией СК России при участии представителей ведущих высших учебных заведений и сотрудников правоохранительных органов России а также иностранные гости, в том числе представители Республики Конго, Следственного комитета Республики Беларусь, прокуратуры Республики Казахстан

Сборник представляет интерес для юристов – учёных и практиков.

Редакционная коллегия обращает внимание на то, что научные подходы и идейные взгляды, изложенные в статьях сборника, отражают субъективные оценки их авторов.

ISBN 978-5-6041504-7-4

Международный научно-практический «круглый стол»
«Использование криптовалют в противоправных
целях и методика противодействия»
(25 апреля 2019 г.)

В Московской академии Следственного комитета 25 апреля 2019 года состоялся Международный научно-практический «круглый стол» на тему: «Использование криптовалют в противоправных целях и методика противодействия».

С приветственным словом к участникам форума обратился и.о. ректора Академии, кандидат юридических наук, доцент, генерал-майор юстиции **Анатолий Михайлович Багмет**: «Проведение этого научного мероприятия обусловлено необходимостью не только обсудить в рамках научного сообщества проблемы, вызвавшие появление таких относительно новых явлений, как технология блокчейн и криптовалюта, но и выяснить – насколько данные технологии могут быть использованы и, к сожалению, уже используются в криминальных целях. Безусловно, данные явления должны пресекаться самым решительным образом, а лица, виновные в их совершении, должны привлекаться к уголовной ответственности».

В рамках мероприятия выступил заместитель Председателя Следственного комитета Российской Федерации **Александр Вячеславович Федоров** с докладом «Ответственность юридических лиц за киберпреступления с применением криптовалют». Он подчеркнул необходимость тщательного изучения феномена

криптовалют и широкого использования криминалистических знаний в следственной практике при расследовании уголовных дел данной категории.

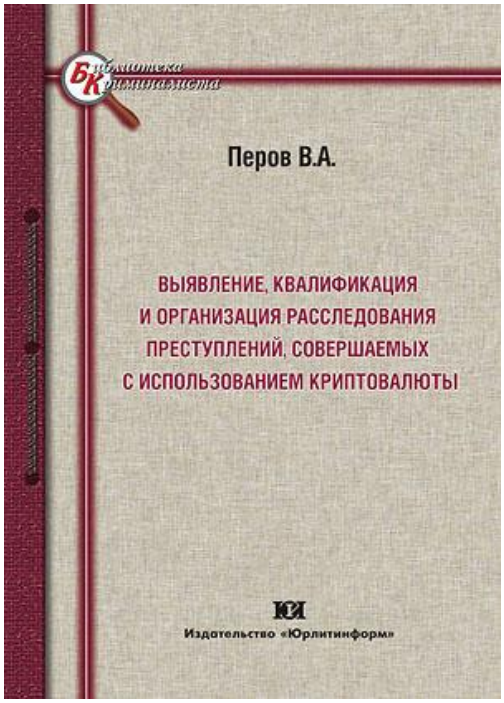
Это мнение поддержала авторитетный эксперт по криптовалютному рынку – профессор кафедры уголовного права, уголовного процесса и криминалистики Московского государственного института международных отношений (Университета) МИД России, руководитель рабочей группы Государственной Думы Федерального Собрания РФ по оценкам рисков оборота криптовалюты доктор юридических наук **Элина Леонидовна Сидоренко**, выступившая с докладом «Криминологические аспекты использования криптовалют».

В ходе проведения форума заведующим кафедрой предварительного расследования преступлений в сфере экономики **Валерием Александрович Перовым** была представлена на обсуждение участников разработанная им криминалистическая методика выявления лиц, совершающих преступления с использованием криптовалюты.

При обсуждении заявленного круга вопросов от участников форума поступали и обсуждались многочисленные вопросы относительно правоприменительной практики использования криптовалют при расследовании соответствующих уголовных дел.

В работе форума приняли участие ученые, представляющие ведущие вузы страны: Московский государственный университет им. М.В. Ломоносова, Московский государственный институт международных отношений (Университет) МИД России, Институт государства и права Российской академии наук, Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации, Российский технологический университет, Институт права и национальной безопасности Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации, Финансовый университет при Правительстве Российской Федерации. Кворум также составили сотрудники Следственного комитета Российской Федерации и представители государственных и общественных организаций (Банк России, ПАО «Сбербанк», ПАО «ВТБ», Министерство финан-

сов Российской Федерации, Росфинмониторинг, Министерство внутренних дел Российской Федерации, ПАО «Нэт Элемент», адвокатское сообщество), аспиранты и студенты вузов, а также иностранные гости, в том числе представители Республики Конго, Следственного комитета Республики Беларусь, прокуратуры Республики Казахстан



Участникам форума было представлено первое в Российской Федерации учебно-методическое пособие «Выявление, квалификация и организация расследования преступлений, совершаемых с использованием криптовалюты», подготовленное сотрудниками Академии.

А.В. Федоров

Ответственность юридических лиц за киберпреступления с применением криптовалют

В связи с развитием новых технологий весьма актуальными являются вопросы противодействия использованию криптовалют в противоправных целях и ответственности за такие деяния, а также разработка методик противодействия преступлениям, связанным с использованием криптовалют. Этой проблематике в последние годы посвящено много специальных работ[1], но, тем не менее, все еще остается в тени ряд важных вопросов, по объективным и субъективным причинам выпавших из поля зрения российских специалистов.

В частности, обсуждению вопросов борьбы с конкретным видом преступности, каковым является использование криптовалют в противоправных целях, должно предшествовать определение того, о какой именно преступности идет речь, кто при этом является субъектом соответствующих преступлений и субъектом уголовной ответственности.

Несомненно, что такая преступность относится к киберпреступности. В последние годы устоялось понимание киберпреступности как преступности в киберпространстве, то есть как совокупности преступлений, совершаемых с использованием компьютеров, информационных технологий и глобальных сетей, включая Интернет.

При этом такими преступлениями в Российской Федерации признаются исключительно соответствующие деяния физических лиц, тогда как во многих странах, каковых уже более 70, доктринально и законодательно признается наличие корпоративной преступности и введена уголовная ответственность юридических лиц за совершение преступлений, в том числе киберпреступлений[2].

Увеличение числа стран, установивших уголовную ответственность за киберпреступления, потребовало организации их международного сотрудничества в борьбе с этими преступлениями и принятия международных актов в указанной сфере.

---

[1] См., напр.: Овчинский В.С. Криминология цифрового мира М., 2018; Основы борьбы с киберпреступностью и кибертерроризмом: хрестоматия / сост. В.С. Овчинский. М., 2017; Долгиева М.М. Квалификация преступлений, совершаемых в сфере компьютерной информации в отношении криптовалюты // Современное право. 2018. № 11. С. 103-108; Перов В.А. Выявление, квалификация и организация расследования преступлений, совершаемых с использованием криптовалюты. М., 2017; Кучеров И.И. К вопросу о методике расследования преступлений, совершенных с использованием криптовалюты // Российский следователь. 2018. № 12. С. 17-21.

[2] Об этом, напр., см.: Голованова Н.А., Лафитский В.И., Цирина М.А. Уголовная ответственность юридических лиц в международном и национальном праве (сравнительно-правовое исследование) / Отв. ред. В.И. Лафитский. – М.: Статут, 2013; Уголовная и административная ответственность юридических лиц в России и во Франции: монография / Хабриева Т.Я., Федоров А.В., Беар-Туше М. и др. / под ред. А.В. Федорова. – М.: Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации, 2018.

К их числу, например, относится Будапештская Конвенция о преступности в сфере компьютерной информации 2001 г. (ETS № 185) с изменениями 2003 г.,[1] предусматривающая установление странами – участницами уголовной ответственности, в том числе юридических лиц, за четыре группы киберпреступлений:

- преступления против конфиденциальности, целостности и доступности компьютерных данных и систем[2];
- преступления, связанные с использованием компьютерных средств[3];
- преступления, связанные с содержанием размещаемых данных[4];
- преступления, связанные с нарушением авторского права.

Это далеко не исчерпывающий перечень, так как по мере развития науки и техники появляются новые виды преступлений. К их числу относятся и киберпреступления с использованием криптовалют.

Ряд авторов использует для обозначения таких преступлений термины «криптопреступность» и «криптопреступления»[5].

Выделяют несколько видов наиболее распространенных криптопреступлений. К ним обычно относят[1] совершенные с использованием криптовалют:

---

1 К числу таких актов также относится ряд актов Европейского Союза и Совета Европы, в частности, Директива (№ 2013/40/ЕС) Европейского парламента и Совета Европейского Союза 2013 г. «Об атаках на информационные системы и о замене Рамочного решения 2005/222/ПВД Совета ЕС» (Принята в г. Брюсселе 12.08.2013), во многом дублирующая Будапештскую конвенцию о преступности в сфере компьютерной информации 2001 г. и содержащая требование к государствам – членам ЕС по обеспечению привлечения юридических лиц к уголовной ответственности за киберпреступления, а также Рекомендация № CM/Rec(2018)7 Комитета министров Совета Европы «О соблюдении, защите и осуществлении прав детей в цифровой среде», предусматривающая необходимость определения соответствующих преступлений, совершенных в цифровой среде, и уголовной ответственности за них, в том числе юридических лиц.

2 К числу таких преступлений, в частности, относятся противозаконный (неправомерный) доступ к компьютерным данным и системам; неправомерный перехват компьютерных данных; неправомерное воздействие на компьютерные данные (умышленное повреждение, удаление, ухудшение качества, изменение или блокирование компьютерных данных); неправомерное воздействие на функционирование системы (умышленное создание неправомерно серьезных помех функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, ухудшения качества, изменения или блокирования компьютерных данных); противозаконное использование устройств (умышленные неправомерные производство, продажа, приобретение для использования, импорт, оптовая продажа или иные формы предоставления в пользование: 1) устройств, включая компьютерные программы, разработанных или адаптированных прежде всего для целей совершения правонарушений, 2) компьютерных паролей, кодов доступа или иных аналогичных данных, с помощью которых может быть получен доступ к компьютерной системе в целом или любой ее части, с намерением использовать их в целях совершения какого-либо из правонарушений.

3 В число таких преступлений входят подлог с использованием компьютерных технологий и мошенничество с использованием компьютерных технологий.

4 Например, преступления, связанные с детской порнографией.

5 Долгиева М.М. Криптопреступность как новый вид преступности: понятие, специфика // Современное право. 2018. № 10. С. 109-115; Сидоренко Э.Л. Криптопреступность как новое криминологическое явление // Общество и право. 2018. № 2(64). С. 15-21.

- легализацию (отмывание) доходов, полученных преступным путем[2];

- незаконный оборот наркотических средств, оружия и иных запрещенных либо ограниченных к обороту предметов[3];

- рабо- и секс-торговлю, детскую порнографию[4];

- кибермошенничества[5].

К указанной группе преступлений относится и использование вредоносных компьютерных программ в целях генерации (майнинга) криптовалют[6]. Одним из преступных способов майнинга криптовалюты является криптоджекинг (cryptojacking), заключающийся в скрытом использовании (без ведома владельцев) для майнинга ресурсов чужих компьютеров в фоновом режиме.

Кроме того, получили распространение коррупционные киберпреступления с применением криптовалют. Пример апреля 2019 г. – пресечение вымогательства одного миллиона долларов у семьи находящегося под следствием бывшего гендиректора «Издательство «Известия», когда деньги получались в биткоинах, а переговоры по их получению велись в Telegram. Имеют место требования выкупа с использованием криптовалют похищенных людей, а также выплат в криптовалюте в связи с угрозами взрывов или предания огласки «чувствительной» информации.

Таким образом, криптопреступления – это, как правило, не предусмотренные главой 28 УК РФ преступления в сфере компьютерной информации[7], а различ-

---

1 См.: Трунцевский Ю.В., Сухаренко А.Н. Противодействие использованию криптовалюты в незаконных целях: состояние и перспективы // Международное публичное и частное право. 2019. № 1. С. 43-47.

2 Об этом виде преступлений см., напр.: Лавроненко Р.А. Легализация преступных доходов, совершаемая в кредитно-финансовой системе с использованием криптовалюты // Безопасность бизнеса. 2018. № 5. С. 57-63; Ализаде В.А., Волеводз А.Г. Неприменение ст. 174¹ Уголовного кодекса РФ по делам о наркопреступлениях, совершенных с использованием криптовалюты, как следствие непонимания сущности легализации (отмывания) нового вида преступных активов // Наркоконтроль. 2018. № 1. С. 5-13; Ализаде В.А., Волеводз А.Г. Судебная практика применения ст. 174¹ УК РФ по делам о наркопреступлениях, совершенных с использованием криптовалюты // Наркоконтроль. 2017. № 4. С. 8-14.

3 Об этом см., напр.: Сидоренко Э.Л. Наркотики и криптовалюта: мировые криминологические тренды // Наркоконтроль. 2018. № 2. С. 8-13; Дворянкин О.А., Клочкова Е.Н. Криптовалюта – новый инструмент наркобизнеса // Наркоконтроль. 2018. № 4. С. 19-22; Баньковский А.Е., Деринг А.В. Актуальные проблемы незаконного оборота наркотических средств посредством сети Интернет: современное состояние и перспективы противодействия // Наркоконтроль. 2019. № 1. С. 11-16.

4 Ларина Е.С., Овчинский В.С. Криминал будущего уже здесь. М., 2018. С. 159-176.

5 Бычков В.В., Вехов В.Б. Специальные знания, обеспечивающие расследование преступлений, связанных с оборотом криптовалюты // Российский следователь. 2018. № 2. С. 8-11.

6 См., напр. Шадрина Т. Валюты-прилипалы. Плохо работает компьютер? На нем «печатают» биткоин // Российская газета. 2017. 21 июня. № 134(7300).

7 В главу 28 УК РФ входят ст. 272 «Неправомерный доступ к компьютерной информации», ст. 273 «Создание, использование и распространение вредоносных компьютерных программ», ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей», ст. 274¹ «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации».

ные иные преступления, совершаемые с использованием криптовалют и применением компьютеров, информационных технологий и глобальных сетей.

За совершение указанного рода криптопреступлений в Российской Федерации привлекаются к уголовной ответственности физические лица. При этом имеют место сложности с квалификацией содеянного и доказыванием совершения преступного деяния, так как в Российской Федерации понятие и статус криптовалюты (в том числе как объекта гражданских прав) нормативно не определены.

Имеется лишь разъяснение Пленума Верховного Суда Российской Федерации о том, что «исходя из положений статьи 1 Конвенции Совета Европы об отмывании, изъятии и конфискации доходов от преступной деятельности и о финансировании терроризма от 16 мая 2005 года с учетом Рекомендации 15 ФАТФ предметом преступлений, предусмотренных статьями 174 и 174[1] УК РФ, могут выступать в том числе и денежные средства, преобразованные из виртуальных активов (криптовалюты), приобретенных в результате совершения преступления»[1].

Когда такие преступления совершаются физическими лицами в интересах юридических лиц, в отдельных случаях возможно привлечение соответствующих юридических лиц к административной ответственности.

Возникает вопрос, достаточно ли в современных условиях уголовной ответственности физических лиц, совершающих киберпреступления в интересах юридических лиц, и административной ответственности юридических лиц в таких случаях, либо требуется установление уголовной ответственности и для юридических лиц, в интересах которых совершаются преступления физическими лицами.

Фактически стоит вопрос о признании или не признании юридического лица субъектом преступлений.

На наш взгляд, следует поддержать российских юристов, считающих, что во многих случаях «роль отдельного человека как преступника отходит на второй план, юридическое же лицо выдвигается на передний план в качестве реального преступника, незаконно получающего денежные или иные выгоды от преступной деятельности»[2].

В тоже время вопрос об уголовной ответственности юридических лиц и изучение корпоративной преступности, в том числе корпоративной киберпреступности, пока еще находятся на периферии научных исследований.

---

[1] См.: Постановление Пленума Верховного Суда Российской Федерации от 26 февраля 2019 года № 1 «О внесении изменений в постановление Пленума Верховного Суда Российской Федерации от 7 июля 2015 года № 32 «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем» // Бюллетень Верховного Суда Российской Федерации. 2019. № 4. С. 1.

[2] Голованова Н.А. Тенденции развития института уголовной ответственности юридических лиц за рубежом // Юридическая ответственность: современные вызовы и решения: материалы VIII Ежегодных научных чтений памяти профессора С.Н. Братуся. М., 2013. С. 153.

Объясняется это тем, что в Российской Федерации уголовная ответственность юридических лиц еще не предусмотрена, а так как преступность – уголовно-правовое явление, де-юре такой преступности нет.

То, что признается преступностью юридических лиц за рубежом, в российских реалиях рассматривается как деликты юридических лиц, то есть противоправные деяния, не являющиеся преступлениями.

Это объясняется рядом обстоятельств.

Во-первых, в нашей стране преступность традиционно отождествляется с деяниями физических лиц.

Во-вторых, в советское время, в условиях преобладания социалистической собственности на орудия и средства производства, изучение вопросов преступности юридических лиц и их ответственности по идеологическим причинам отторгалось, а зарубежный опыт установления такой ответственности оценивался с классовых позиций как направленный против прав трудящихся.

В-третьих, в период перехода от социалистических к рыночным отношениям акцентировалось внимание лишь на гражданско-правовой ответственности юридических лиц, а правонарушения с их участием зачастую воспринимались как неизбежное негативное явление периода первоначального накопления капитала, не требующее признания юридических лиц субъектами преступлений и административных правонарушений.

Тем не менее, в отечественных криминологических исследованиях и работах по сравнительному правоведению стало получать признание фактическое наличие в Российской Федерации преступности юридических лиц в наднациональном её понимании как социальной реальности, требующей всестороннего изучения и адекватной реакции со стороны государства.

В этой связи следует отметить исследования И.М. Мацкевича, обосновывающего наличие с криминологической точки зрения такого субъекта преступления как юридическое лицо[1]. Первым же из российских ученых в 1991 г. поставил вопрос о необходимости установления уголовной ответственности юридических лиц профессор А.В. Наумов[2].

В Российской Федерации уже установлена и получила доктринальное обоснование административная ответственность юридических лиц. Она применяется в установленных законом случаях при совершении административных правонарушений или преступлений физическими лицами от имени или в интересах соответствующих юридических лиц.

Наряду с этим, по нашему мнению, должна быть сформулирована позиция и по вопросу уголовной ответственности юридических лиц.

---

[1] Мацеевич И.М. Причины экономической преступности: учебное пособие. М., 2017. С. 31-32.

[2] Об этом см.: Федоров А.В. Вопросы уголовной ответственности юридических лиц в трудах профессора Анатолия Валентиновича Наумова // Вестник Московской академии Следственного комитета Российской Федерации. 2019. № 1. С. 23-30.

Такая ответственность, как уже было отмечено, предусмотрена рядом международных договоров, участницей части из которых является Российская Федерация[1].

С учетом зарубежного опыта ввести в Российской Федерации уголовную ответственность юридических лиц за совершение преступлений, в том киберпреступлений, не представляет сложности.

Настало время для завершения доктринальной разработки, официального признания российской теоретической концепции уголовной ответственности юридических лиц и её закреплении в соответствующих законодательных решениях.

Следует отказаться от исключительно административной ответственности юридических лиц, ибо она не может компенсировать отсутствие возможности привлечения их к уголовной ответственности. Так, если противоправные деяния физических лиц являются уголовно наказуемыми, то и взаимосвязанное с ними деяние юридического лица должно признаваться преступлением, а не административным правонарушением, на что фактически указывается в решениях Конституционного Суда Российской Федерации[2] и Европейского суда по правам человека[3].

Установление уголовной ответственности юридических лиц будет соответствовать современным стратегиям противодействия преступности и международным стандартам, вписываться в процесс имплементации положений международных актов об ответственности юридических лиц.

Это весьма важно и актуально для борьбы с киберпреступностью, так как ряд зарубежных стран весьма успешно формирует практику привлечения к уголов-

---

[1] См., напр.: Федоров А.В. Международно-правовое регулирование вопросов уголовной ответственности юридических лиц // Журнал зарубежного законодательства и сравнительного правоведения. 2015. № 3. С. 367-381; Федоров А.В. О выполнении положений международных договоров об установлении уголовной ответственности юридических лиц // Вестник Академии Следственного комитета Российской Федерации. 2015. № 3. С. 17 – 22; Федоров А.В. Рекомендательные акты СНГ об уголовной ответственности юридических лиц в контексте новых вызовов и угроз // Расследование преступлений: проблемы и пути их решения. 2018. № 4 (22). С. 13-20.

[2] Конституционным Судом Российской Федерации признано, что правонарушения юридических лиц могут представлять общественную опасность, сопоставимую с общественной опасностью преступлений, а в некоторых случаях – и более высокую. См.: Определение Конституционного Суда Российской Федерации от 5 июня 2014 г. № 1308-О «Об отказе в принятии к рассмотрению жалобы общества с ограниченной ответственностью «Приоритет» на нарушение конституционных прав и свобод частью 1 статьи 19.28 Кодекса Российской Федерации об административных правонарушениях» // Вестник Конституционного Суда Российской Федерации. 2014. № 6.

[3] Исходя из значительных размеров санкций за ряд административных правонарушений юридических лиц Европейский Суд по правам человека, определяет такого рода правонарушения юридических лиц как преступления и констатирует необходимость проведения уголовно-правового расследования по соответствующим делам. См.: Постановление ЕСПЧ от 20 сентября 2011 г. по делу «ОАО «Нефтяная компания ЮКОС» против Российской Федерации (Жалоба № 14902/04) // Приложение к Бюллетеню Европейского Суда по правам человека. Российская хроника Европейского Суда. Специальный выпуск. №3/2012.

ной ответственности юридических лиц, зарегистрированных или работающих на территории Российской Федерации, в том числе за киберпреступления, а Российская Федерация не может принять адекватные «зеркальные» меры в отношении иностранных юридических лиц по причине отсутствия законодательно установленной возможности их привлечения к уголовной ответственности.

Литература

1. Ализаде В.А., Волеводз А.Г. Неприменение ст. 174[1] Уголовного кодекса РФ по делам о наркопреступлениях, совершенных с использованием криптовалюты, как следствие непонимания сущности легализации (отмывания) нового вида преступных активов // Наркоконтроль. 2018. № 1. С. 5-13.
2. Ализаде В.А., Волеводз А.Г. Судебная практика применения ст. 174[1] УК РФ по делам о наркопреступлениях, совершенных с использованием криптовалюты // Наркоконтроль. 2017. № 4. С. 8-14.
3. Баньковский А.Е., Деринг А.В. Актуальные проблемы незаконного оборота наркотических средств посредством сети Интернет: современное состояние и перспективы противодействия // Наркоконтроль. 2019. № 1. С. 11-16.
4. Бычков В.В., Вехов В.Б. Специальные знания, обеспечивающие расследование преступлений, связанных с оборотом криптовалюты // Российский следователь. 2018. № 2. С. 8-11.
5. Голованова Н.А. Тенденции развития института уголовной ответственности юридических лиц за рубежом // Юридическая ответственность: современные вызовы и решения: Материалы для VIII Ежегодных научных чтений памяти профессора С.Н. Братуся / Отв. ред. Н.Г. Доронина, – М.: Институт законодательства и сравнительного правоведения при Правительстве РФ: ИНФРА-М, 2013. С. 153 – 163.
6. Голованова Н.А., Лафитский В.И., Цирина М.А. Уголовная ответственность юридических лиц в международном и национальном праве (сравнительно-правовое исследование) / Отв. ред. В.И. Лафитский. – М.: Статут, 2013. – 312 с.
7. Дворянкин О.А., Клочкова Е.Н. Криптовалюта – новый инструмент наркобизнеса // Наркоконтроль. 2018. № 4. С. 19-22.
8. Долгиева М.М. Квалификация преступлений, совершаемых в сфере компьютерной информации в отношении криптовалюты // Современное право. 2018. № 11. С. 103-108.
9. Долгиева М.М. Криптопреступность как новый вид преступности: понятие, специфика // Современное право. 2018. № 10. С. 109-115.
10. Кучеров И.И. К вопросу о методике расследования преступлений, совершенных с использованием криптовалюты // Российский следователь. 2018. № 12. С. 17-21.
11. Лавроненко Р.А. Легализация преступных доходов, совершаемая в кредитно-финансовой системе с использованием криптовалюты // Безопасность бизнеса. 2018. № 5. С. 57-63.

12. Ларина Е.С., Овчинский В.С. Криминал будущего уже здесь. – М.: Книжный мир, 2018. – 512 с.
13. Овчинский В.С. Криминология цифрового мира: учебник для магистратуры. – М.: Норма; ИНФРА-М, 2018. - 352 с.
14. Основы борьбы с киберпреступностью и кибертерроризмом: хрестоматия / сост. В.С. Овчинский. – М.: Норма, 2017. – 528 с.
15. Перов В.А. Выявление, квалификация и организация расследования преступлений, совершаемых с использованием криптовалюты: учеб.-медодич. Пособие. М.: Юрлитинформ, 2017. – 200 с.
16. Сидоренко Э.Л. Криптопреступность как новое криминологическое явление // Общество и право. 2018. № 2(64). С. 15-21.
17. Сидоренко Э.Л. Наркотики и криптовалюта: мировые криминологические тренды // Наркоконтроль. 2018. № 2. С. 8-13.
18. Трунцевский Ю.В., Сухаренко А.Н. Противодействие использованию криптовалюты в незаконных целях: состояние и перспективы // Международное публичное и частное право. 2019. № 1. С. 43-47.
19. Уголовная и административная ответственность юридических лиц в России и во Франции: монография / Хабриева Т.Я., Федоров А.В., Беар-Туше М. и др. / под ред. А.В. Федорова. – М.: Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации, 2018. – 200 с.
20. Федоров А.В. Вопросы уголовной ответственности юридических лиц в трудах профессора Анатолия Валентиновича Наумова // Вестник Московской академии Следственного комитета Российской Федерации. 2019. № 1. С. 23-30.
21. Федоров А.В. Международно-правовое регулирование вопросов уголовной ответственности юридических лиц // Журнал зарубежного законодательства и сравнительного правоведения. 2015. № 3. С. 367-381.
22. Федоров А.В. О выполнении положений международных договоров об установлении уголовной ответственности юридических лиц // Вестник Академии Следственного комитета Российской Федерации. 2015. № 3. С. 17 – 22.
23. Федоров А.В. Рекомендательные акты СНГ об уголовной ответственности юридических лиц в контексте новых вызовов и угроз // Расследование преступлений: проблемы и пути их решения. 2018. № 4 (22). С. 13-20.

А.М. Багмет

К вопросу выявления и расследования преступлений, совершаемых с использованием криптовалюты

Аннотация. Автором рассматриваются криминалистические и уголовно-процессуальные проблемы, возникающие при выявлении преступлений, связанных с использованием криптовалюты и осуществлением предварительного расследования соответствующих уголовных дел.

На основании требований действующего законодательства и сложившейся правоприменительной практики, предлагается основа соответствующей криминалистической методики, базирующейся на изучении функциональных принципов криптовалют и системе сложившихся в процессе их использования закономерностей.

Ключевые слова: технология блокчейн, криптовалюта, следственные органы, предварительное расследование, криптокошельки, криминалистическая техника, криминалистическая методика, криминалистическая тактика.

Сегодня, когда высокие технологии активно пронизывают все сферы человеческой деятельности возникает насущная необходимость не только в их изучении и обсуждении соответствующих проблем в рамках научного сообщества, но и выработку соответствующих практических рекомендаций, направленных на противодействие противоправного использования указанных технологий. И такие проблемы существуют. Так такие относительно новые явления как технология блокчейн и криптовалюта, должны не только изучаться, но необходимо выяснять насколько данные технологии могут быть использованы, а подчас к сожалению уже используются в криминальных целях. Все мы прекрасно знаем, что сегодня используя криптовалюту незаконно приобретаются предметы запрещенные к гражданскому обороту или ограниченные в гражданском обороте. То есть незаконным путем приобретается оружие, наркотические средства, поддельные документы, осуществляется незаконное финансирование экстремистских и террористических организаций.

Безусловно данные явления должны пресекаться самым решительным образом, а лица виновные в их совершении должны привлекаться к уголовной ответственности.

Для этого необходимо определить какие обстоятельства имеют значение для расследования конкретного уголовного дела и главное какими доказательствами в данном случае можно указанные обстоятельства подтвердить. Каким образом данные доказательства могут быть получены и зафиксированы является одним из ключевых вопросов в данной тематике. Каким образом определить владельцев анонимных криптокошельков? Как доказать их причастность к совершенным преступлениям? Каким образом данные доказательства могут быть получены и кем? Как данные доказательства соотносятся с требованиями действующего законодательства? На эти конкретные вопросы необходимо получить ответы. И не просто ответы теоритического плана, а ответы позволяющие эффективно применить полученные знания в практической следственной деятельности.

Только таким образом может быть достигнуто взаимодействие между теорией и практикой. Только таким образом может быть решен вопрос практического обучения, когда происходит обмен теоритическими и практическими знаниями в результате которого и рождается то единственно правильное понимание самой сути права, его целей и задач в какой бы области данное право не применялось.

Обсуждаемые сегодня вопросы крайне сложны и зачастую не имеют однозначного толкования, а обсуждаемые проблематика относится не только к области права, но и к области высоких технологий, развитие которых не всегда может быть предсказуемым.

Тем не менее указанными технологиями необходимо овладевать, именно для использования их в практических целях. И может быть сегодня кто-нибудь скажет, что подобного рода уголовных дел мало и нет необходимости этому учиться.

На это можно ответить только одно. В век высоких технологий учиться нужно всегда. Потому, что то, что сегодня кажется не столь нужным, редким, интересным только для специалистов указанной области, завтра обретает общемасштабный характер. И к этому надо быть готовым. Возбудив уголовного дело следователь должен четко представлять, как его расследовать, должен планировать свои действия, определяться с кругом доказательств и возможностями их получения, а не думать о том, где бы пройти соответствующее обучение. Все это в полной мере относится к криптовалютному рынку. Следователи уже сейчас должны быть готовы к тому, что подобного рода уголовные дела будут находится в их производстве, чтобы уметь эффективно их расследовать.

Руководством Следственного комитета Российской Федерации прилагаются огромные усилия для внедрения в практику расследования уголовных дел современной криминалистической техники, равно как и использование при расследовании современных криминалистических методик.

Все это должно апробироваться и внедрятся в жизнь. Мы не можем стоять в стороне, наблюдая за происходящим в надежде использовать полученный кем-то другим соответствующий научный опыт. Наука сегодня развивается стремительными темпами и игнорирующие этот процесс сегодня, завтра могут отстать навсегда.

Только активизация научной деятельности в сфере высоких технологий к которым без сомнения относятся и технология блокчейн и криптовалюта помогут не только их пониманию, но должны воспрепятствовать их криминализации, защитить права и законные интересы законопослушных граждан и организаций, работающих на криптовалютном рынке.

Не остается в стороне и Московская академия Следственного комитета Российской Федерации в которой проводится научно-исследовательская работа в том числе по выработке новейших криминалистических методик выявления и расследования преступлений с использованием криптовалюты.

Список использованных источников

1. Конституция Российской Федерации
2. Уголовно-процессуальный кодекс Российской Федерации
3. Уголовный кодекс Российской Федерации
4. Федеральный закон «О Следственном комитете Российской Федерации» от 28.12.2010 № 403-ФЗ
5. А.И. Бастрыкин. «След в след». Российская газета - Федеральный выпуск № 236 (7104)
6. А.М. Багмет. «К вопросу о совершенствовании курсов повышения квалификации по криминалистической тактике в Академии Следственного комитета Российской Федерации». Журнал «Вестник академии Следственного комитета Российской Федерации» № 3/2015. Стр. 23-26.
7. В.А. Перов. «Выявление, квалификация и организация расследования преступлений, совершаемых с использованием криптовалюты». М: Издательство Юрлитинформ. 2017, 200 стр.

Н.Н. Беломытцев

Криптовалюта как предмет хищения путем использования компьютерной техники

Аннотация. В условиях развития цифровой экономики уже невозможно отрицание существования электронно-цифрового имущества, обладающего всеми традиционными признаками присущими имуществу в традиционном ее понимании. Рассмотрены статус криптовалют в белорусском законодательстве как предмета и средства совершения преступления. Цель работы — поиск универсального алгоритма квалификации хищения виртуальной валюты и, как следствие дальнейшей разработки на его основе методики расследования хищений путем использования компьютерной техники.

Ключевые слова: хищение путем использования компьютерной техники, криптовалюта, предмет хищения, преступления против собственности.

Современное общество, стремится все более облегчить и упростить свой уклад жизни, стараясь не только автоматизировать, но и передать некоторые процессы жизнедеятельности всевозможным программно-техническим средствам. Более того создает искусственную «виртуальную» реальность не только ради удобства коммуникации, но и для проведения досуга, своеобразного отдыха. В связи с этим видится закономерным появление своеобразной электронно-цифровой валюты, которой стала криптовалюта. Криптовалюта, как своеобразный денежный инструмент является электронно-цифровой записью или условными числовыми единицами к которым обращаются участниками частных электронных платежных систем для расчетов друг с другом. Криптовалюта – это разновидность нефиатных (частных) электронных денег, эмиссия и учет которых основывается на криптографических методах, платёжная система ко-

торая функционирует децентрализовано в распределенной компьютерной сети, где платежные единицы представлены в виде определенных электронных монет, курс которых в подавляющем большинстве случаев формируется балансом спроса и предложения[12].

Действительно она, по сравнению с обычными платёжными инструментами имеет ряд преимуществ, таких как анонимность ее пользователей, независимость от какой-либо финансовой системы, удобство перевода и использования, невозможность подделки и т.д. Вместе с тем в ряде государств до настоящего времени правовой статус криптовалют каким-либо образом не закреплён. В связи с чем, в условиях стремительного развития электроно-цифровой торговли и популяризации новых средств платежа преступные посягательства, связанные с оборотом криптовалюты, приобретают в последнее время массовый и системный характер (начиная от получения вознаграждения за преступные деяния, «отмывания денег» и заканчивая ее хищением), представляя тем самым существенную угрозу национальном и международном интересам.

В этой связи, руководством Республики Беларусь был предпринят ряд мер по урегулированию деятельности в сфере оборота криптовалют. В частности, 28.03.2018 вступил в силу декрет №8 «О развитии цифровой экономики». Декрет «легализировал» оборот криптовалют в Беларуси. Резиденты парка высоких технологий вправе заниматься майнингом и осуществлять деятельность биржи криптовалют и криптообменного пункта, а также иную деятельность с использованием цифровых знаков (криптовалют или токенов). До 1 января 2023 г. не признаются объектами налогообложения обороты, прибыль (доходы, выручка) от различных операций с токенами. Теперь физические лица вправе владеть токенами, осуществлять майнинг; обменивать токены, приобретать и отчуждать их за белорусские рубли, иностранную валюту, электронные деньги, а также дарить и завещать токены, при этом данная деятельность не признается предпринимательской. Токены и доходы от операций с ними не подлежат декларированию физическими лицами[3]. Вместе с тем, не смотря на инновационность данного декрета, правовой статус криптовалют для уголовно-правовой сферы декретом четко не определен, что создает определенные трудности в деятельности органов уголовного преследования при даче уголовно-правовой оценки общественно опасным деяниям, предметом которых выступают криптовалюты и как следствие самому процессу дальнейшего расследования.

---

[1] Ализаде В.А., Волеводз А.Г. Судебная практика по делам о преступлениях преступных сообществ (преступных организаций) в сфере незаконного оборота наркотиков, совершенных с использованием информационно-телекоммуникационной сети Интернет и криптовалюты // Библиотека криминалиста. – 2017. – № 6., с. 281

[2] Филатова М.А. Анализ криптовалюты в мировой финансовой системе с позиции уголовного права (на примере Bittcoin) // Уголовное право в эпоху финансовоэкономических перемен: материалы IX Российского конгресса уголовного права, Москва, 29-30 мая 2014 г. / Моск. гос. ун-т; редкол.: В.С.Комиссаров (отв. ред.) [и др.]. – М., 2014, с. 216-223

[3] Официальный интернет-портал Президента Республики Беларусь. Декрет № 8 от 21 декабря 2017 г. О развитии цифровой экономики http://president.gov.by.

В этой связи, одной из главных задач правоохранительных органов состоит в пресечении и расследовании имущественных преступлений, которыми на наш взгляд и являются хищения криптовалют, т.к. виновные посягают именно на отношения собственности. При этом мы исходим из того, что криминалистика является наукой прикладной, призванной обеспечить ход расследования конкретных уголовных дел. В данном случае криптовалюта представляет для нас интерес как один из элементов криминалистической характеристики – предмет преступного посягательства хищения путем использования компьютерной техники.

Поэтому следователю первоначально необходимо определить предмет преступного посягательства, что будет способствовать установлению ряда других важных обстоятельств дела (некоторые данные о личности лица, совершившего преступление, о действиях лиц, оказывающих содействие в преступной деятельности, способе совершения преступления, степени осведомленности преступника об обстановке совершения преступления и т.д.). Более того, согласного п. 4 ч. 1 ст. 89 УПК Республики Беларусь характер и размер вреда, причиненного преступлением, является обстоятельством, подлежащим доказыванию по уголовному делу. Кроме этого, при анализе п. 1 примечания к гл. 24 УК Республики Беларусь при расследовании хищения путем использования компьютерной техники (ст.212 УК) также подлежит установлению и сам факт умышленного противоправного безвозмездного завладения чужим имуществом или правом на имущество с корыстной целью.

Рассматривая предмет преступного посягательства, Р.С. Белкин отмечал, что точное выявление и описание связей предмета посягательства с типичным преступником, типичными способами совершения преступления и типичной следовой картиной, обстановкой совершения преступления, несомненно, будет служить целям раскрытия преступления [1] Подчеркивая важность исследования предмета хищения при рассмотрении его как одного из элементов криминалистической характеристики преступлений, В.К. Гавло писал, что особое значение приобретают данные о предмете преступного посягательства (вещи, предметы, ценности), которые имеют материализованную оболочку и доступны для восприятия извне, для измерения и фиксации. Они могут выступать в качестве следообразующих и следовоспринимающих объектов, что важно для установления места, времени, способа, орудий и других обстоятельств совершения и сокрытия преступлений с помощью специально разрабатываемых для определенной ситуации методов расследования [2].

В связи с вышеизложенным, для более эффективного противодействия в борьбе с преступностью в сфере оборота криптовалют необходимо более глубже, полно и всесторонне изучить предметы, процессы и явления, на которые предполагается оказывать воздействие. При этом не любой предмет обстанов-

[1] Белкин Р.С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики. М., 2001. С.223.

[2] Гавло В.К. Теоретические проблемы и практика применения методики расследования отдельных видов преступлений / под общ. ред. А.Н. Васильева. Томск: Изд-во Томского ун-та, 1985. С.200-201.

ки, взаимодействующий с лицом, совершившим преступление, можно отнести к предмету посягательства, а только тот, который непосредственно связан с наступлением неблагоприятных последствий, в нашем случае криптовалютой. При совершении хищений путем использования компьютерной техники виновное лицо воздействует на всевозможные предметы. Так, для хищения имущества, принадлежащего какому-либо финансовому учреждению (например криптобиржам) или хищений с криптокошельков, преступник использует программно-технические средства (ноутбук, ПК, смартфон и т.п.), сетевое оборудование, электронно-цифровые носители информации и иное, чтобы завладеть криптовалютой, однако, несмотря на то, что преступник воздействует на указанное, предметом его преступного посягательства будет лишь то имущество (криптовалюта), которым он завладел преступным путем, в рассматриваемом случае выраженное в электронно-цифровой записи об имуществе или «компьютерная информация выраженная в «записях на счетах» [1].

Вместе с тем, в настоящий момент, квалификация действий виновных по противоправному завладению криптовалютами не является единообразной, в действительности имеющие все признаки хищения путем использования компьютерной техники. Так, например действия по завладению криптовалютами в некоторых случаях квалифицируются по ст. 349 УК (несанкционированный доступ к компьютерной информации) либо по ст. 212 УК. Например, в Гомельском городском отделе СК 04.07.2017 было возбуждено уголовное дело по признакам преступления, предусмотренного ч. 2 ст. 212 УК, в отношении неустановленного лица, которое 31.03.2017 примерно в 14 часов осуществило несанкционированный доступ на аккаунт Р. принадлежащий П. на сайте btc-e.com в глобальной сети интернет, который предназначен для проведения обменных валютных операций посредством условной единицы биткойн, после чего осуществило перевод на электронный кошелек 1***gwz 4,3477 биткойн, тем самым причинило П. имущественный ущерб.

В свою очередь Заводским (г. Минска) РОСК 07.03.2018 возбуждено уголовное дело по признакам преступления, предусмотренного ч. 2 ст. 349 УК, в отношении неустановленного лица, которое, не имея права доступа к мультикошельку криптовалют (bitcoin, ethereum, bitcoin cash) Ж., зарегистрированному на сайте blockchain.info, осуществило несанкционированный доступ к указанному мультикошельку и хранящейся на нем информации и совершило операции с его использованием, в результате чего похитило денежные средства криптовалют в сумме 0,88567655 (bitcoin cash) и 1,49178322 (ethereum), принадлежащие Ж., причинив имущественный вред на общую сумму 6 312 рублей. Но уже схожие действия лица Фрунзенским (г. Минска) РОСК квалифицированы по ч. 3 ст. 212 УК [2].

---

[1] Макаревич, А.В. Парадигма уголовно-правовой оценки хищений, совершаемых с использованием информационных систем :дис. … канд. юрид. наук : 12.00.08 / А.В. Макаревич. – Минск., 2014. С.97.

[2] Информационный бюллетень Следственного комитета Республики Беларусь № 2 (10), 2018 тема номера: «расследование уголовных дел о преступлениях в сфере информационных технологий» о практике расследования преступлений против информационной безопасности.

На наш взгляд, в случае, когда данные действия квалифицируются по ст.349 УК, упускается сама суть данного противоправного деяния. В первую очередь виновный посягает именно на отношения собственности, все остальное связано только со способом посягательства, и основное его деяние все равно остается за рамками квалификации. В любом случае, за 2018 г. в республике зарегистрировано лишь шесть уголовных дел о преступлениях, предметом которых являлись криптовалюты (УСК по г. Минску — пять, УСК по Гомельской области — одно). По указанным уголовным делам в настоящее время отсутствуют вступившую в силу приговоры суда.

В рамках проводимого исследования методики расследования хищений путем использования компьютерной техники, необходимо выработать единый подход в правоприменении и выборе на его основе комплекса мер, направленных на совершенствование методики расследования новых объектов правоотношений — криптовалют, не являющихся имуществом в традиционном понимании.

Многие годы незыблемым является постулат, что предметом хищения может быть только имущество, отвечающее следующим признакам:

экономическому (обладает объективной экономической стоимостью);

юридическому (правовому) – предмет должен быть чужим для виновного;

физическому (материальному, фактическому, вещному) – предмет должен быть материален, иметь физическую форму, быть вещью [1].

Если рассмотреть два первых признака предмета преступления против собственности – экономический и юридический, то приходим к выводу о том, что криптовалютам несомненно присущ экономический признак, поскольку на законодательном уровне (указанный декрет №8) закрепляет их оборот и иные экономические сделки с ними (майнинг, обмен на офсетные и электронные деньги и т.д.). Определение наличия юридического признака у криптовалюты не вызывает затруднений, т.к. являются для виновного чужими.

При рассмотрении третьего признака, применительно к криптовалюте, необходимо отметить, что она в программно-технических средствах владельцев представлена ничем иным как «электрический заряд», «электромагнитное поле», которые по своей сути являются материальным объектом, либо физически может представлять собой набор магнитных «меток»[2] и поэтому, по нашему мнению, являет собой ничто иное как материальный объект. По сути являясь

---

[1] Винокуров, В. Причинение имущественного ущерба как критерий признания предметов и информации предметами преступлений против собственности / В. Винокуров // Уголов. право. – 2008. – № 4. – С. 13–19; Научно-практический комментарий к Уголовному кодексу Республики Беларусь / Н.Ф. Ахраменка [и др.] ; под ред. А.В. Баркова, В.М. Хомича. – 2-е изд., с изм. и доп. – Минск : Гос. ин-т упр. и соц. технологий Белорус.гос. ун-та, 2010. С. 439; Уголовное право. Особенная часть : учебник / под ред. Л.В. Иногамовой-Хегай, А.И. Рарога, А.И. Чучаева – 2-е изд., испр. и доп. – М. : Юрид. фирма «Контракт» : Инфра-М, 2008. С. 188.

[2] Стрельцов, А.А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы / А.А. Стрельцов ; Ин-т проблем информ. безопасности. – Минск :Беллитфонд, 2005. С. 178.

определенной электронно-цифровой информацией, ее смысловая (семантическая) составляющая, не может существовать без набора данных – совокупности знаков, сигналов, в которых она выражается и которые представляют собой определенное «физическое состояние»[1].

Криптовалюта своего рода имеет материальную природу ещё и вследствие того, что компьютер по своей сути «может работать только с материальными образами материальных объектов», более того, с конечным множеством этих объектов, поскольку компьютер «не работает с бесконечными множествами» [2], что еще раз подтверждает «пространственную ограниченность» что вновь указывает на «телесность».

Подводя итог изложенному, в связи с тем, что криптовалюта представляет собой ничто иное как структурированный набор электронно-цифровых данных, имеющих материальную природу, обладающих экономическими и юридическими признаками, является ничем иным как предметом хищения, путем использования компьютерной техники. Именно данной нормой (ст.212 УК) законодатель установил ответственность за хищение имущества, которое имеет указанную специфичность вещного признака.

Существует необходимость в выработке единых подходов к квалификации противоправных деяний, предметом которых выступают криптовалюты. По нашему мнению, в тех случаях, когда криптовалюта похищается путем несанкционированного доступа к месту их хранения, данные преступные деяния необходимо квалифицировать в первую очередь по ст.212 УК и проводить ряд мер по раскрытию и расследованию хищений путем использования компьютерной техники.

Литература

1. Ализаде В.А., Волеводз А.Г. Судебная практика по делам о преступлениях преступных сообществ (преступных организаций) в сфере незаконного оборота наркотиков, совершенных с использованием информационно-телекоммуникационной сети Интернет и криптовалюты // Библиотека криминалиста. – 2017. – № 6., с. 281.
2. Белкин Р.С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики. М., 2001. С. 237.
3. Винокуров, В. Причинение имущественного ущерба как критерий признания предметов и информации предметами преступлений против собственности / В. Винокуров // Уголов. право. – 2008. – № 4. – С. 13–19.
4. Гавло В.К. Теоретические проблемы и практика применения методики расследования отдельных видов преступлений / под общ. ред. А.Н. Васильева. Томск: Изд-во Томского ун-та, 1985. С.214.

[1] Мазур, М. Качественная теория информации : пер. с пол. / М. Мазур ; предисл. А.В. Солодова. – М. : Мир, 1974. С. 33.

[2] Евменов, В.П. Интеллектуальные системы управления : учеб. пособие / В.П. Евменов. – М. :Либроком, 2009. С. 91.

5. Евменов, В.П. Интеллектуальные системы управления : учеб. пособие / В.П. Евменов. – М. :Либроком, 2009. – 304 с.
6. Информационный бюллетень Следственного комитета Республики Беларусь № 2 (10), 2018 тема номера: «расследование уголовных дел о преступлениях в сфере информационных технологий» о практике расследования преступлений против информационной безопасности.
7. Мазур, М. Качественная теория информации : пер. с пол. / М. Мазур ; предисл. А.В. Солодова. – М. : Мир, 1974. – 239 с.
8. Макаревич, А.В. Парадигма уголовно-правовой оценки хищений, совершаемых с использованием информационных систем :дис. … канд. юрид. наук : 12.00.08 / А.В. Макаревич. – Минск., 2014. – 120 л.
9. Научно-практический комментарий к Уголовному кодексу Республики Беларусь / Н.Ф. Ахраменка [и др.] ; под ред. А.В. Баркова, В.М. Хомича. – 2-е изд., с изм. и доп. – Минск : Гос. ин-т упр. и соц. технологий Белорус.гос. ун-та, 2010. – 1064 с.
10. Официальный интернет-портал Президента Республики Беларусь. Декрет № 8 от 21 декабря 2017 г. О развитии цифровой экономики http://president.gov.by/ru/official_documents_ru/view/dekret-8-ot-21-dekabrja-2017-g-17716/ Режим доступа 17.04.2019.
11. Стрельцов, А.А. Правовое обеспечение информационной безопасности России: теоретические и методологические основы / А.А. Стрельцов ; Ин-т проблем информ. безопасности. – Минск : Беллитфонд, 2005. – 304 с.
12. Уголовное право. Особенная часть : учебник / под ред. Л.В. Иногамовой-Хегай, А.И. Рарога, А.И. Чучаева – 2-е изд., испр. и доп. – М. : Юрид. фирма «Контракт» : Инфра-М, 2008. – 800 с.
13. Филатова М.А. Анализ криптовалюты в мировой финансовой системе с позиции уголовного права (на примере Bittcoin) // Уголовное право в эпоху финансово-экономических перемен: материалы IX Российского конгресса уголовного права, Москва, 29-30 мая 2014 г. / Моск. гос. ун-т; редкол.: В.С.Комиссаров (отв. ред.) [и др.]. – М., 2014, с. 216-223.

С.С. Бурынин

Цифровые финансовые активы как предмет взятки

Аннотация. В статье приводится анализ использования цифровых финансовых активов в преступных целях, в частности, коррупционных. С указанной целью проанализировано как действующее законодательство в данной сфере так и законопроекты. Кроме того, исследована судебная практика о преступлениях с использованием цифровых финансовых активов, мнения представителей научного сообщества по указанной проблематике. Предложены возможные способы отнесения цифровых финансовых активов к предмету взятки, в том числе, оценки их стоимости.

***Ключевые слова*:** цифровой финансовый актив, криптовалюта, токен, объекты гражданских прав, оценочная экспертиза, взятка, коррупция, беловоротничковая преступность.

Развитие цифровой экономики диктует новые правила осуществления финансовых операций. Указанное относится не только к осуществлению подавляющего большинства финансовых операций в безналичной форме, но и к созданию цифровых финансовых активов. Сразу необходимо оговориться, что легального определения понятия цифрового финансового актива в настоящее время не существует.

Как стремительно развивается цифровая экономика так в ногу с ней шагает и преступность. Схемы совершения преступных деяний постоянно совершенствуются. Преступники пытаются подстроиться под действующие реалии всех жизненных процессов.

Несмотря на то, что понятия «цифровая экономика», «цифровые финансовые активы» взывают к «высокой материи» в преступной среде использование указанных средств замечено отнюдь не в «беловоротничковой преступности». Так, исходя из анализа судебной практики, большая часть приговоров за преступления с использованием цифровых финансовых активов вынесены по уголовным делам, связанным с незаконным оборотом наркотиков.

О чем это может свидетельствовать? Вполне возможно, что действительно основной массив преступлений с использованием цифровых финансовых активов связан с незаконным оборотом наркотиков. Но «беловоротничковая преступность» не зря является видом высокоинтеллектуальной преступности, чтобы находится на максимальном уровне латентности.

Из этого следует, что наличие финансовых активов, которые просты в обращении, обезличены, а значить не оставляют следов их перемещения и не привязаны к конкретному физическому или юридическому лицу, является «идеальным» предметом для преступных посягательств, а также средством для совершения преступлений.

В силу указанных обстоятельств, свидетельствующих о такой «привлекательности» цифровых финансовых активов, отсутствие судебной практики из разряда «беловоротничковой преступности» может указывать только на их латентность, а не отсутствие как таковой.

Вместе с тем, отсутствие соответствующей судебной практики может быть также вызвано правовым вакуумом в сфере регулирования использования цифровых финансовых активов.

Наибольшие опасения вызывает использование цифровых финансовых активов в качестве предмета взятки.

По мнению П.С. Яни цифровые финансовые активы не могут являться предметом взятки, так как они не имеют фиксированного стоимостного выражения[1]. Данная точка зрения находит подтверждение на практике. В частности, при отсутствии фиксированного стоимостного выражения имущества, услуги и тд., следствию необходимо использование специальных знаний. Для установления указанных обстоятельств необходимо проведение оценочной экспертизы. Вме-

[1] Румак В. В отличие от мошенничества, состав злоупотребления полномочиями можно назвать "резиновым" [Интервью с П.С. Яни] // Закон. 2018. № 10. С. 6 - 16.

сте с тем, единой методики экспертной оценки стоимости цифровых финансовых активов не существует.

Отсутствию единой методики оценки во многом способствует спорность отнесения цифровых финансовых активов к объектам гражданских прав. Так как к объектам оценки относятся только объекты гражданских прав, в отношении которых законодательством Российской Федерации установлена возможность их участия в гражданском обороте[1].

Из диспозиций ст.ст. 290-291.2 УК РФ следует, что предметом взятки (посредничества во взяточничестве) могут быть деньги, ценные бумаги, иное имущество, незаконное оказание услуг имущественного характера, предоставление иных имущественных прав. Указанное вытекает из положений ст. 128 ГК РФ, определяющей объекты гражданских прав. Судебная практика также идет по пути определения предмета взятки исключительно исходя из объектов гражданских прав[2].

В юридическом сообществе существуют мнения об отнесении цифровых финансовых активов к объектам гражданских прав, в частности к категории «иное имущество»[3]. Кроме того, некоторая судебная практика также идет по пути признания цифровых финансовых активов объектами гражданских прав, применяя аналогию закона и относя их к категории «иное имущество» (ст.ст. 6, 128 ГК РФ)[4].

Делая первые шаги в направлении правового регулирования цифровых финансовых активов законодатель уточнил понятие «иного имущества» в ст. 128 ГК РФ указав: «…иное имущество, в том числе имущественные права (включая безналичные денежные средства, бездокументарные ценные бумаги, цифровые права)…». Также в ГК РФ вводится ст. 141.1 закрепляющая понятие «цифровые права» - как названные в таком качестве в законе обязательственные и иные права, содержание и условия осуществления которых определяются в соответствии с правилами информационной системы, отвечающей установленным законом признакам[5].

---

[1] Приказ Минэкономразвития России от 20.05.2015 № 297 "Об утверждении Федерального стандарта оценки "Общие понятия оценки, подходы и требования к проведению оценки (ФСО № 1)".

[2] Постановление Пленума Верховного Суда РФ от 09.07.2013 N 24 (ред. от 03.12.2013) "О судебной практике по делам о взяточничестве и об иных коррупционных преступлениях".

[3] Перов В.А. Квалификация действий лиц, совершающих преступления с использованием криптовалюты на территории Российской Федерации // Российский следователь. 2018. № 4. С. 54-57; Ильяшенко Е.А. О перспективах привлечения к уголовной ответственности за использование криптовалют в преступных целях // Российский следователь. 2018. № 8. С. 51-54.

[4] Постановление Девятого арбитражного апелляционного суда от 15.05.2018 № 09АП-16416/2018 по делу № А40-124668/2017 // Архив Девятого арбитражного апелляционного суда.

[5] Федеральный закон от 18.03.2019 № 34-ФЗ "О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации" (вступает в силу с 01.10.2019).

Указанная правовая дефиниция имеет явно бланкетный характер и какой-либо конкретизации не вносит, за исключением однозначного отнесения цифровых прав к имуществу, а следовательно к объектам гражданских прав. Вместе с тем, остается не ясным являются ли цифровые финансовые активы разновидностью цифровых прав?

Данные законодательные новеллы по всему явились «плацдармом» для следующего пакета поправок в законодательство о правовом статусе цифровых финансовых активов.

Так, уточняя положения ГК РФ о цифровых правах законодателем вырабатываются основные положения, регулирующие отношения, возникающие при создании, выпуске, хранении и обращении цифровых финансовых активов, а также осуществлении прав и исполнении обязательств по сделкам с ними. Согласно пояснительной записке к законопроекту «О цифровых финансовых активах» его целями является законодательное закрепление в российском правовом поле определений наиболее широко распространенных в настоящее время финансовых активов, создаваемых и/или выпускаемых с использованием цифровых финансовых технологий, к которым законопроект относит распределенный реестр цифровых транзакций, а также создание правовых условий для привлечения российскими юридическими лицами и индивидуальными предпринимателями инвестиций путем выпуска токенов, являющихся одним из видов цифровых финансовых активов[1].

Из предложенного в законопроекте понятия «цифрового финансового актива» следует, что таковым является имущество в электронной форме, созданное с использованием шифровальных (криптографических) средств. Права собственности на данное имущество удостоверяются путем внесения цифровых записей в реестр цифровых транзакций. К цифровым финансовым активам относятся криптовалюта, токен. Цифровые финансовые активы не являются законным средством платежа на территории Российской Федерации[2].

Таким образом, если указанные законодательные новеллы будут приняты в предложенной в проекте формулировке, фактически цифровые финансовые активы станут одним из видов имущества. Соответственно цифровые финансовые активы однозначно будут отнесены к объектам гражданских прав, а значит они смогут является предметом взяточничества.

Вместе с тем, вопрос определения их стоимостного выражения по-прежнему останется открытым. Правоприменители окажутся в ситуации когда de jure состав преступления в виде взяточничества будет, а de facto не один эксперт не возьмется за оценку стоимостного выражения взятки в виде цифровых финансовых активов. Учитывая, что цифровые финансовые активы не являются законным средством платежа на территории Российской Федерации, то и под положения о валютном контроле они не подпадают. Кроме того, Центральный

[1] Проект Федерального закона № 419059-7 "О цифровых финансовых активах" (подготовлен Минфином России) // http://sozd.duma.gov.ru/bill/419059-7.

[2] См. там же.

Банк Российской Федерации в данном случае вряд ли будет устанавливать курс цифровых финансовых активов по аналогии с валютами[1].

Сложность в расчёте их стоимости вызывает специфичность данного вида активов. К примеру, у них отсутствуют регулярные денежные потоки, дивидендные выплаты или конечная стоимость, которую можно было бы рассчитать. Расчет стоимости цифровых финансовых активов исходя из котировок специализирующихся на них торговых площадок (бирж) также не будет являться достоверным. Цифровые финансовые активы не имеют строго определенной структуры рынка. Торговые площадки (биржи) публикуют совершенно разные цены. Также не ограничено и само количество данных площадок, участников рынка, а следовательно и предложенных цен. В свете этого объективно установить среднею или наименьшую стоимости цифровых финансовых активов будет просто невозможно.

Одной из возможных для применения методик для оценки стоимости цифровых финансовых активов является предложенная экспертом в области цифровых финансовых активов Крисом Берниске. Она имеет название: «Уравнение обмена» – это макроэкономическая модель, описывающая соотношение денежной массы, скорости денежного обращения, уровня цен и показателя расходов. С указанной целью он предлагает устанавливать цену ресурсов, предоставляемых криптосетью, и их количество, при перемножении которых получится денежная сумма, характеризующая собой обмен актива на доступ к облачному хранилищу. Отслеживать соответствующие транзакции он предлагает с помощью блокчейна. Но для этого нужно знать адрес кошелька или хэш транзакции[2].

Из этого следует, что передача и получение взятки исключительно в виде цифровых финансовых активов приведет к определенной сложности в установлении денежного эквивалента предмета взятки.

Однако важно заметить, что к данному случаю будет относится установление договоренности о передаче и получении взятки только в виде цифровых финансовых активов без предварительной либо последующей конвертации их в денежный эквивалент.

Допустим в случае выдвижения взяткополучателем требования о передаче ему взятки в определенной сумме денежных средств, но конвертированных в цифровые финансовые активы, предметом взятки все равно останутся денежные средства. Конвертация их в цифровые финансовые активы и соответственно передача взяткополучателю фактически лишь ключей доступа к ним будет ничем иным как попытка скрыть следы передачи денежных средств.

По аналогичному пути пошла судебная практика по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого пре-

[1] "Положение об установлении и опубликовании Центральным банком Российской Федерации официальных курсов иностранных валют по отношению к рублю" (утв. Банком России 18.04.2006 № 286-П).

[2] [Электронный ресурс] https://medium.com/@cburniske/cryptoasset-valuations-ac83479ffca7.

ступным путем. Так, исходя из положений статьи 1 Конвенции Совета Европы об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности и о финансировании терроризма от 16 мая 2005 года и с учетом Рекомендации 15 ФАТФ предметом преступлений, предусмотренных ст.ст. 174 и 174.1 УК РФ, могут выступать в том числе и денежные средства, преобразованные из виртуальных активов (криптовалюты), приобретенных в результате совершения преступления[1].

В указанных случаях оценка цифровых финансовых активов как таковых не потребуется, достаточно будет лишь установить стоимость имущества либо сумму денежных средств, конвертированных в них, которые и будут предметом преступления (либо средством для совершения преступления).

Информационное поле пестрит разнообразными заголовками о коррупционных происшествиях с использованием цифровых финансовых активов. Так, один из них заявляет: «В Москве проведена беспрецедентная операция по очищению ФСБ России от коррупционеров. По подозрению в вымогательстве одного миллиона долларов арестованы два следователя по особо важным делам. Деньги они получили в биткоинах, а все переговоры с целью конспирации вели в Telegram. Но даже эти конспиративные меры не помогли. Задержали офицеров сотрудники Управления собственной безопасности (УСБ) ФСБ России». Издание утверждает, что к одному из обвиняемых по уголовному делу, находящемуся в производстве следователей ФСБ России, обратился бывший сотрудник ФСБ России с требованием передачи ему одного миллиона долларов в криптовалюте за благоприятные условия содержания в СИЗО «Лефортово» и за минимизацию юридических последствий. В ходе проведенных оперативно-розыскных мероприятий удалось задокументировать факт передачи денежных средств специалисту по биткоинам и перевода их в криптовалюту, а затем и получение вымогателем[2].

Приведенный пример из СМИ раскрывает определенную технологию осуществления преступной деятельности с помощью цифровых финансовых активов. Однако важным составляющим в данном случае все равно является «жажда наживы» в виде денежных средств в конкретной сумме, а перевод их в криптовалюту лишь способом сокрытия следов преступления. Вместе с тем, представляется, что если бы требования были выдвинуты о передаче в определённом количестве, к примеру, биткоинов, без указания на их стоимость в денежном эквиваленте, то в реалиях действующего законодательства говорить о том, что они явились бы предметом преступления не пришлось. Хотя бы из-за отсутствия возможности объективно установить их стоимость и вовсе однозначную относимость к объектам гражданских прав.

Хочется верить, что указанные законодательные новеллы значительным образом повлияют на правоприменительную практику, в частности, на выявление

[1] Постановление Пленума Верховного Суда РФ от 07.07.2015 № 32 (ред. от 26.02.2019) "О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем".

[2] [Электронный ресурс] https://lenta.ru/articles/2019/04/20/sledaki2/.

и расследование преступлений с использованием цифровых финансовых активов, в том числе коррупционных.

Е.Г. Быкова
А.А. Казаков

Проблемы правовой оценки перевода полученной в результате незаконного оборота наркотических средств криптовалюты в фиатные деньги

Аннотация. В статье анализируется практика по уголовным делам о преступлениях, связанных с незаконным сбытом наркотических средств, сопровождающимся их обменом на криптовалюту. Неоднозначны выводы судов относительно правовой оценки по ст. 174.1 УК РФ перевода криптовалюты в фиатные деньги. Авторы приходят к выводу, что обмен криптовалюты на денежные средства, находящиеся в обращении на территории РФ, может квалифицироваться по ст. 174.1 УК РФ только при доказанности специальной цели, указанной в диспозиции названной статьи уголовного закона. В противном случае обналичивание криптовалюты не требует отдельной правовой оценки.

Ключевые слова: криптовалюта, биткоин, легализация, незаконный оборот наркотических средств, фиатные деньги, цель совершения преступления, 174.1 УК РФ, 228.1 УК РФ.

Развитие экономики привело к появлению специфического цифрового инструмента - криптовалюты. Как только она получила распространение на территории Российской Федерации, среди юристов начались непрекращающиеся дискуссии относительно ее правового статуса[1]. В этой связи еще в 2014 году на состоявшемся в Генеральной прокуратуре РФ межведомственном совещании была сформирована позиция, согласно которой криптовалюта представляет собой денежные суррогаты и не может применяться гражданами и юридическими лицами. Поскольку она не обеспечена реальной стоимостью, то ее обладатели лишены возможности защищать свои интересы в судебном и административном порядке[2].

Специалисты Федеральной службы по финансовому мониторингу также высказывали опасения по поводу оборота криптовалют, подчеркивая, что факти-

[1] См.: Перов В.А. Уголовно-правовые аспекты использования криптовалюты в России // Вестник Московской академии Следственного комитета Российской Федерации. 2017. № 3. С. 78-81; Быкова Е.Г., Казаков А.А. О правовой оценке противоправного безвозмездного изъятия криптовалюты // Уголовное право. 2018. № 2. С. 16-19; Маркунцов С.А. Квазифинансовые инструменты как новые объекты уголовно-правовой охраны: постановка проблемы // Уголовное право: стратегия развития в XXI веке: материалы XV Международной научно-практической конференции. М.: РГ-Пресс, 2018. С. 590-595; Уфимцева В.А. Уголовно-правовые риски использования криптовалюты // Уголовное право: стратегия развития в XXI веке: материалы XVI Международной научно-практической конференции. - Москва: РГ-Пресс, 2019. С. 140-146.

[2] См.: В Генеральной прокуратуре Российской Федерации состоялось совещание по вопросу правомерности использования анонимных платежных систем и криптовалют // https://www.genproc.gov.ru/smi/news/genproc/news-86432/ (дата обращения 23.04.2019).

ческое нахождение криптовалют вне правового поля не позволяет задействовать правовые механизмы обеспечения исполнения обязательств сторонами сделки. К примеру, если оплата произведена, но услуга или товар не получены, то нет гарантий возврата такого платежа[1].

На проблемах, связанных с распространением таких систем, акцентировал внимание Председатель Следственного комитета Российской Федерации А.И. Бастрыкин[2].

Вопрос о необходимости законодательного регулирования правового статуса криптовалюты обсуждался на совещании при Президенте РФ В.В. Путине. Глава государства ставил задачу перед профильными ведомствами о необходимости детальной проработки указанного вопроса в кратчайшие сроки, чтобы исключить риски для граждан и бизнеса[3].

Однако до настоящего момента вопрос о правовом статусе криптовалюты остается открытым. На рассмотрении в Государственной Думе находится законопроект «О цифровых финансовых активах». Этот документ не предполагает регламентацию оборота основных криптовалют (например, биткоина). Вместе с тем в соответствии с рекомендациями ФАТФ (международной группы разработки финансовых мер по борьбе с отмыванием денег), высказанными в адрес России, данный вопрос должен быть урегулирован на национальном уровне в течение 2019 года[4].

В практике имеется резонансное решение, в котором арбитражный суд признал криптовалюту иным имуществом и включил в конкурсную массу должника[5].

При рассмотрении гражданско-правовых споров о взыскании неосновательного обогащения с тех лиц, которые осуществляли привлечение денежных средств для приобретения криптовалюты, принимаются решения об отказе в удовлетворении исковых требований. Суды исходят из того, что криптовалюта является денежным суррогатом, в связи с чем правоотношения сторон по вопросу ее приобретения основаны на риске[6].

---

[1] См.: Информационное сообщение Федеральной службы по финансовому мониторингу от 06.02.2014 «Об использовании криптовалют» // http://www.fedsfm.ru/news/957 (дата обращения 23.04.2019).

[2] См., например, Бастрыкин А.И. Следственный комитет Российской Федерации в авангарде борьбы с коррупцией и финансовыми нарушениями // Расследование преступлений: проблемы и пути их решения. 2016. № 2. С. 12; Интервью Председателя Следственного комитета Российской Федерации Александра Бастрыкина «Российской газете» // URL: https://sledcom.ru.

[3] См.: Совещание по вопросу использования цифровых технологий в финансовой сфере 10.10.2017 // http://kremlin.ru.

[4] Закон об использовании криптовалют в России должны принять до конца года // https://www.rbc.ru.

[5] Постановление Девятого арбитражного апелляционного суда г. Москвы № 09АП-16416/2018 от 15.05.2018 по делу № А40-124668/2017 // URL: http://kad.arbitr.ru.

[6] См., например, Решение Калининского районного суда г. Челябинска от 04.12.2018 по делу № 2-4009/2018; Решение Советского районного суда г. Уфы от 04.10 2018 по делу № 2-7321/2018; Апелляционное определение Ульяновского областного суда от 31.07.2018 по делу

Вместе с тем информация о криптовалютах признается запрещенной к распространению на территории РФ, поскольку "возможность бесконтрольного трансграничного перевода денежных средств и их последующего обналичивания служит предпосылкой потенциального вовлечения криптовалют в схемы, направленные на легализацию (отмывание) доходов, полученных преступным путем"[1].

Как видится, такие решения зачастую обоснованы. Практика показывает, что в последнее время все чаще криптовалюта используется в качестве платежного средства при осуществлении незаконного оборота наркотических средств. Данное обстоятельство часто устанавливается при расследовании преступления, предусмотренного ст. 228 УК РФ[2]. В связи с тем, что в настоящее время отсутствует законодательный запрет на оборот криптовалюты, ее использование для оплаты приобретаемого запрещенного вещества не требует отдельной правовой оценки по иным составам преступления.

Иная ситуация складывается при расследовании преступления, предусмотренного ст. 228.1 УК РФ. В соответствии с разъяснениями, содержащимися в п. 13 Постановления Пленума Верховного Суда РФ от 15.06.2006 № 14 «О судебной практике по делам о преступлениях, связанных с наркотическими средствами, психотропными, сильнодействующими и ядовитыми веществами»[3] под незаконным сбытом предметов названного преступления понимается "незаконная деятельность лица, направленная на их возмездную либо безвозмездную реализацию (продажа, дарение, обмен, уплата долга, дача взаймы и т.д.) приобретателю".

Если в результате возмездного отчуждения наркотического средства приобретатель расплатился со сбытчиком криптовалютой, то последний чаще всего осуществляет операции по ее переводу в фиатные деньги. Органы предварительного расследования оценивают эти действия по ст. 174.1 УК РФ.

Фактические обстоятельства, которые следствие рассматривает как легализацию (отмывание) денежных средств, приобретенных лицом в результате совершения преступления, как правило, представляют собой однотипную схему. Лицо, получившее за сбыт наркотического средства, криптовалюту, подыскивает в интернете сайт и осуществляет ее обмен на денежные средства, находящиеся в обращении на территории РФ. Электронные деньги зачисляются на неперсонифицированные виртуальные счета и переводятся оттуда на счета бан-

---

№ 33-3142/2018; Апелляционное определение Самарского областного суда от 30.08.2018 по делу № 33-10148/2018 // URL: https://bsr.sudrf.ru (дата обращения 23.04.2019).

[1] См., например, Решение Железнодорожного районного суда г. Екатеринбурга от 13.07.2018 по делу № 2а-2103/18; Решение Анапского городского суда Краснодарского края от 20.12. 2017 по делу № 2 – 4762/2017; Решение Наримановского районного суда Астраханской области от 30.07.2018 по делу № 2а-696/2017; Решение Смольнинского районного суда г. Санкт-Петербурга от 06.09.2016 г. по делу № 2-4208/16 // URL: https://bsr.sudrf.ru (дата обращения 23.04.2019).

[2] См., например, приговор Каменского районного суда Свердловской области от 01.10.2018 по делу № 1-97/2018; приговор Орджоникидзевского районного суда г. Екатеринбурга от 13.02.2019 по делу № 1-160/2019 // URL: https://bsr.sudrf.ru (дата обращения 23.04.2019).

[3] Российская газета. 2006. 28 июня.

ковских карт, принадлежащие лицам, не осведомленным о преступном происхождении денег (родственникам, знакомых, иным лицам, которые являются номинальными владельцами карты). В дальнейшем субъект преступления либо просит владельцев карты обналичить эти денежные средства и передать ему, либо осуществляет платежи, приобретая необходимые ему товары и (или) оплачивая в безналичной форме какие-либо услуги.

Суды по-разному оценивают указанные обстоятельства. Как правило, если судебное разбирательство осуществляется в особом порядке, то суд соглашается с квалификацией содеянного субъектом по совокупности преступлений, предусмотренных соответствующей частью ст. 228.1 УК РФ (по эпизодам незаконного сбыта наркотических средств за криптовалюту) и ст. 174.1 УК РФ (по эпизоду перевода криптовалюты в фиатные деньги)[1].

Отчасти эта позиция является справедливой, поскольку 26.02.2019[2] пункт первый Постановления Пленума Верховного Суда РФ от 07.07.2015 № 32 «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем»[3] был дополнен абзацем третьим, разъясняющим, что "предметом преступлений, предусмотренных ст. 174 и 174.1 УК РФ, могут выступать денежные средства, преобразованные из виртуальных активов (криптовалюты), приобретенных в результате совершения преступления". Необходимость формирования позиции высшей судебной инстанции по данному вопросу ранее обосновывалась в научных публикациях, посвященных исследуемой проблеме[4].

Несмотря на уточненную позицию по данному вопросу, правовая оценка содеянного по ст. 174.1 УК РФ осложнена иными обстоятельствами. Поэтому нередко суды исключают из обвинения указанную статью уголовного закона как излишне вмененную. В обоснование такого решения указывают, что легализация (отмывание) денежных средств или иного имущества, добытого преступ-

---

[1] См. приговор Лысьвенского городского суда Пермского края от 21.03.2019; Апелляционное определение Пензенского областного суда от 06.02.2019 по делу № 22-113; приговор Ленинского районного суда г. Челябинска от 05.02.2019 по делу № № 1 – 129/2019; приговор Мотовилихинского районного суда г.Перми от 07.11.2018 по делу № 1-405-2018; приговор Ленинского районного суда г. Тюмени от 14.08.2018 по делу № № 1-753/2018; приговор Рамонского районного суда Воронежской области от 27.03.2018 по делу № 1-24/2018 // URL: https://bsr.sudrf.ru (дата обращения 23.04.2019).

[2] Постановление Пленума Верховного Суда РФ от 26.02.2019 № 1 «О внесении изменений в постановление Пленума Верховного Суда Российской Федерации от 7 июля 2015 года № 32 «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем» // Российская газета. 2019. 7 марта.

[3] Российская газета. 2015. 13 июля.

[4] Волеводз А.Г. Оценка криптовалюты как предмета преступления, предусмотренного ст. 174.1 УК РФ // Уголовное право: стратегия развития в XXI веке: материалы XV Международной научно-практической конференции. М.: РГ-Пресс, 2018. С. 597-603; Ляскало А.Н. Криптовалюта как предмет и средство преступления // Уголовное право: стратегия развития в XXI веке: материалы XVI Международной научно-практической конференции. - Москва: РГ-Пресс, 2019. С. 91.

ным путем, является преступлением в сфере экономической деятельности и предполагает совершение таких финансовых операций или иных сделок, в результате которых данные денежные средства или иное имущество вовлекается в легальный экономический оборот. Это обстоятельство отличает уголовно наказуемую легализацию от основного преступления, совершаемого с использованием финансовых институтов, целью которых является конспирация как способ получения дохода от незаконного оборота наркотиков для личных нужд, что охватывается диспозицией ст. 228.1 УК РФ, и на этом обстоятельстве акцентировано внимание в п. 11 Постановления Пленума Верховного Суда РФ от 07.07.2015 № 32 «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем». На основании изложенного делается вывод о недоказанности цели придания правомерного вида владению, пользованию или распоряжению денежными средствами, полученными в результате совершения финансовых операций с криптовалютой, полученной в качестве оплаты за незаконный сбыт наркотических средств[1].

Думается, что последняя точка зрения зачастую обоснована, поскольку воспользоваться криптовалютой, как правило, можно только путем ее перевода в фиатные деньги. Именно этим обусловлены операции, совершаемые заинтересованными лицами.

Неоднозначная практика свидетельствует о необходимости внесения изменений в ч. 1 ст. 174.1 УК РФ, так как нынешняя редакция затрудняет ее применение в условиях современных реалий.

Ввиду того, что основанием уголовной ответственности в соответствии со ст. 8 УК РФ является совершение деяния, содержащего все признаки состава преступления, предусмотренного статьей Особенной части уголовного закона, правовая оценка обналичивания криптовалюты в целях распоряжения полученными денежными средствами для собственных нужд видится проблематичной.

Литература

1. Бастрыкин А.И. Следственный комитет Российской Федерации в авангарде борьбы с коррупцией и финансовыми нарушениями // Расследование преступлений: проблемы и пути их решения. 2016. № 2. С. 9-12.
2. Быкова Е.Г., Казаков А.А. О правовой оценке противоправного безвозмездного изъятия криптовалюты // Уголовное право. 2018. №2. С. 16-19.

[1] См., например, Апелляционное постановление Ростовского областного суда от 09.04.2018 по делу № 22-1313/2018; приговор Приволжский районный суд города Казани от 20.04.2018 по делу № 1-96/18; приговор Верхнепышминского городского суда Свердловской области от 10.07.2018 по делу №1-146/18; Апелляционное определение Верховного Суда Республики Крым от 02.08.2018 по делу № 22-1819/2018; Постановление президиума Верховного Суда Республики Крым от 07.11.2018 по делу 4У-789/2018 // URL: https://bsr.sudrf.ru (дата обращения 23.04.2019).

3. Волеводз А.Г. Оценка криптовалюты как предмета преступления, предусмотренного ст. 174.1 УК РФ // Уголовное право: стратегия развития в XXI веке: материалы XV Международной научно-практической конференции. М.: РГ-Пресс, 2018. С. 597-603.
4. Ляскало А.Н. Криптовалюта как предмет и средство преступления // Уголовное право: стратегия развития в XXI веке: материалы XVI Международной научно-практической конференции. - Москва: РГ-Пресс, 2019. С. 87-91.
5. Маркунцов С.А. Квазифинансовые инструменты как новые объекты уголовно-правовой охраны: постановка проблемы // Уголовное право: стратегия развития в XXI веке: материалы XV Международной научно-практической конференции. М.: РГ-Пресс, 2018. С. 590-595.
6. Перов В.А. Уголовно-правовые аспекты использования криптовалюты в России // Вестник Московской академии Следственного комитета Российской Федерации. 2017. № 3. С. 78-81.
7. Уфимцева В.А. Уголовно-правовые риски использования криптовалюты // Уголовное право: стратегия развития в XXI веке: материалы XVI Международной научно-практической конференции. - Москва: РГ-Пресс, 2019. С. 140-146.

С.Б. Вепрев

Криптовалюта как прорыв в области финансовых технологий XXI века

Аннотация. В сообщении в общем виде рассмотрены основные особенности функционирования и реализации криптовалюты биткоин. Сделана попытка уточнить возможности и место использования криптовалюты в нашей современной действительности

Ключевые слова: криптовалюта, блокчейн, биткоин, майнинг, nonce.

Как субъект, хочу высказать свое субъективное мнение по вопросу внедрения криптовалюты в нашу современную российскую жизнь. На сегодняшний день имеется множество криптовалют, многие из которых имеют свои особенности и проанализировать их все – задача необозримая для данного выступления. Я попытаюсь сделать своё заключение на примере наиболее популярной криптовалюты биткоин, основываясь на цитатах из интернета, которые мне показались любопытными. К счастью, любой из вас легко может найти в интернете неисчислимое множество подобных же цитат по заданной тематике. По возможности, я хочу рассмотреть только основные рекламируемые плюсы криптовалюты биткоин, которые утверждаются, практически, в каждой публикации о ней:

Криптовалюта – это одно из решений математической головоломки. Покупатель криптовалюты — инвестор, оплачивающий труд математиков по получению одного из решений головоломки и добыть биткоин при помощи специально организованной деятельности (майнинга) может любой желающий.

Нет единого эмиссионного центра и органов, контролирующих процесс циркуляции криптовалюты. Децентрализованный выпуск криптовалюты обеспечивает отсутствие контроля за ее получением.

Поскольку при операциях с криптовалютой исключена деятельность банков, то при проведении таких операций практически нет комиссий. Платежи дешевле, чем при использовании обычных денежных средств.

Все операции с криптовалютой происходят абсолютно анонимно и все сведения о его владельце закрыты. Единственная открытая информация – это номер электронного кошелька.

Итак, по порядку.

Эта технология (криптовалюта), появившаяся из неоткуда, способна приносить огромный доход.[1] Криптовалюта — это одно из решений математической головоломки. Покупатель криптовалюты — инвестор, оплачивающий труд математиков по получению одного из решений головоломки.[2] Ух ты, огромный доход за разгадывание математической головоломки! В чем же она заключается и каким образом решается - очень интересно! Так вот, доказательством работы является хэш рассматриваемого сообщения, объединенного со специальным полем (nonce), и числовое значение этого хэша должно быть меньше заданного. Nonce не несет смысла — это поле перебирается(!) автором доказательства, пока не будет найдено подходящее значение. Например, если нужно, чтобы первые 16 бит хеша равнялись нулю, то в среднем нужно перебрать 65536 значений nonce.[3] Совершенно бессмысленная работа! Это просто затрата энергоресурсов на комбинаторную задачу. Более того, хотя большое количество узлов производят вычисления, в реальности только первый, кто произведет успешную работу, получит вознаграждение. И еще: после перебора всех этих nonce может оказаться, что работа вообще была бесполезной, ибо вы не смогли найти правильный хеш. Для нахождения нужного правильного хеша, оказывается, может быть важен не только nonce. Так, если диапазон nonce кончился, а хеш оказался больше желаемого, то корректируется задание, изменяются поля nbits и ntime и... [4] И начинай сказку сначала!

И еще один важный момент, связанный с самим принципом технологии блокчейна, он состоит в неизменности уже проведенных транзакций. А если транзакция реализует намеренно искажённую информацию? Тогда, с одной стороны, вся построенная на ней ветвь блокчейн становится нелегитимной с точки зрения закона, но легальной с точки зрения блокчейн-технологии. А сделать откат, как утверждается, практически невозможно.

Но все-таки, вот они – денежки, только руку протяни, поставь себе программу майнинга и зарабатывай себе втихаря. Исследователь Sergio Demian Lerner, используя анализ техники прироста поля ExtraNonce, определил и доказал, что в начале цепочки блокчейн, то есть с Genesis - блока до блока #36288 майнин-

[1] https://kinvestor.ru/kriptovaluta-kak-zarabotat/
[2] https://tutdenegki.com/crypta/kriptovalyuty.html
[3] https://habr.com/ru/
[4] https://miningbitcoinguide.com/mining/sposoby/chto-takoe-sut-vidy

гом занимался только один компьютер. Это расследование показывает, что именно этот компьютер добыл первые 1,148,800 монет BTC. В современном пересчете это примерно 612 264 448 000 рублей! Вот так и надо зарабатывать всем майнерам!

Однако, следует заметить, что со временем процесс добывания криптомонет все более и более усложняется и майнинг при помощи оборудования отдельных пользователей становится все менее рентабельным. Сейчас, занимаясь майнингом, вы наверняка только потеряете деньги. Но есть возможность влезть в долю. Поскольку очевидно, что майнинг, во-первых, энергозатратен и, во-вторых, положительный результат маловероятен, майнеры объединяются в колхозы, совхозы, артели и т. п., которые называются фермами. А полученная криптовалюта делится пропорционально. Хотя это тоже малоэффективно.

Но лично у меня вызывают уважение те люди, которые действительно глубоко, очень глубоко прониклись идеей майнинга криптовалют. И вот что они говорят: во-первых, заработать много вам уже никак не удастся, прошли те времена; во-вторых, требуются постоянные затраты по обновлению комплектующих, не реже, чем раз в квартал; в третьих, требуется проводить постоянный мониторинг криптовалют с целью выявления наиболее выгодной для текущего майнинга. То есть, майнинг для них – это постоянная дополнительная кропотливая вдумчивая работа. Такие продвинутые майнеры создают и свои индивидуальные фермы. А то, что добыть биткоин при помощи специально организованной деятельности (майнинга) может любой желающий – это давно уже иллюзия.

Главным преимуществом криптовалюты перед фиатными деньгами стала полная децентрализация.[1] В абсолютную децентрализацию лично мне поверить крайне сложно. Должны быть правила и алгоритмы проведения транзакций, их согласования и онлайн-распределения блокчейна по пользователям, хранения и идентификации паролей, проведения аудита и т.п. Получается, что все отдано на откуп некоторому всесильному всеведущему алгоритму и идет автоматически. Но так ли это на самом деле? В такой распределенной сети должна осуществляться синхронизация и единое управление. Хоть децентрализованное, хоть какое другое, но должен же существовать четкий механизм, который позволяет собирать воедино и решать текущие логические задачи по обеспечению функционирования всех пользователей, распределенных по всему земному шару! Ведь, если ждать подтверждения работы от всех майнеров всей сети, то и не дождешься. Сколько же нужно сообщений, кто их анализирует и где они аккумулируются для внесения в блокчейн и дальнейшей рассылки по сети? Как только пытаешься вникать в эти тонкости – все, стена и общие фразы об эффективности.

Утверждается, что блокчейн – это система алгоритмов консенсуса. Но как и у любой абстрактной системы, у блокчейна есть уровни. Узлы консенсуса (майнеры) – формируют блокчейн, группируют транзакции в блоки. Узлы аудита – распределяют нагрузку по сети, проверяют работу майнеров. Легкие узлы –

[1] https://tutdenegki.com/crypta/kriptovalyuty.html

клиенты – не имеют полной версии блокчейна (криптовалютные кошельки, программы).[1] Но и тут масса вопросов о том, как взаимодействуют майнеры и формируется блокчейн. Утверждается, что все майнеры равноправны, но если я, например, сейчас стану майнить крипт, на своем убогом ПК, то равноправен ли я, да и как я проверю не «обувают» ли меня? Как только пытаешься глубже разобраться с этим вопросом – снова стена. Все под честное слово. Так или нет?

И еще, декларируется, что для успешной атаки на блокчейн нужно иметь 51% мощности сети. То есть, если злоумышленник имеет 51% мощностей, он всегда в состоянии сделать откат транзакций. Также он может создать альтернативную цепочку блоков, которая гарантированно обгонит основную цепочку и сама станет основной. Но мы ведь все знаем и абсолютно уверены, что блокчейн надежно защищен. А все потому, как всеми утверждается, что в связи с огромным количеством майнеров блокчейн в безопасности. Но так ли это? Нет, не так. Майнинг все же подвержен проблеме централизации. Так, более 70% хешрейта биткойна на данный момент находится в одной стране — Китае.[2] Вот так: ждала сова галку, а выждала палку. Понимаю, китайцам совсем не нужно компрометировать блокчейн, они на нем зарабатывают, но они же, в любой момент, в случае надобности, вполне могут это сделать. Опять все под честное слово. Так или нет?

Утверждается, что главными преимуществами криптовалюты перед фиатными деньгами стало отсутствие высоких комиссий. Какая прелесть, неужели хоть здесь коммунизм? Однако, оказывается, что рекомендованная комиссия для транзакции — 100-120 сатоши за байт. А заплатив $2, вы обеспечите своей транзакции бóльшую вероятность попадания в следующий найденный блок. За счет комиссии время проведения транзакции уменьшится. И такую комиссию автоматически назначают большинство бирж, облачных майнингов и магазинов, принимающих биткоины.[3] А чем же это дешевле обычных банковских операций? Не дешевле. Но более того, транзакционные сборы влияют и на то, как транзакции распространяются по сети Bitcoin. Существует настраиваемый параметр minrelaytxfee биткоин-клиента по умолчанию (Bitcoin Core), который определяет минимально возможную сумму комиссии за килобайт размера транзакции. Транзакции с более низкой платой вообще считаются спамом и не распространяются биткоин-узлом! Они висят в так называемом облаке транзакций. Кстати, и достать их обратно является не такой уж простой задачей.

Есть еще одна «фишка» - это увеличение сложности процесса майнинга во времени. Необходимость роста сложности добычи биткоин обуславливается, прежде всего, развитием технологий майнинга, прежде всего, появлением более производительных специализированных технических устройств. Так, в начале процесса майнинга использовались видеокарты, а в 2014 году, майнеры получили в распоряжение ASIC — специальное оборудование, ориентированное на скоростное выполнение однотипных задач, направленных на перебор nonce и

[1] https://miningbitcoinguide.com/mining/sposoby/chto-takoe-sut-vidy
[2] https://habr.com/ru/company/bitfury/blog/327468/
[3] https://crypt-mining.net.

поиск интересующего хэша. Это привело к тому, что «добыча» одного блока стала меньше заложенного изначально норматива в 10 минут. На это криптовалютная сеть реагирует очередным ростом сложности. То есть, не имеет значения, сколько майнеров криптовалюты и какие у них мощности, главное – должен примерно соблюдаться установленный параметр— около 10 минут на блок. Система реагирует и усложняет задачу посредством задания некоторого рандомного (случайного) числа, которое постоянно меняется.[1] И тут снова для меня возникает вопрос о неуловимой системе, порядке ее управления и правилах ее функционирования.

Абсолютная надежность блокчейн от взлома тоже под вопросом. Все, что создано человеческими руками, человеческими руками может быть сломано и взломано. Криптовалютная биржа Binance объявила о взломе, в результате которого было потеряно более 7000 биткоинов. В компании подчеркнули, что хакерам удалось получить доступ только лишь к «горячему» кошельку, на котором хранилось около 2% средств. Генеральный директор биржи Чанпэн Чжао (он же «CZ») сказал, что после консультации с несколькими специалистами было принято решение не делать откат в сети биткоина, чтобы вернуть украденные средства.[2] То есть, во-первых, криптовалютная биржа Binance не смогла защитить именно ей доверенные «горячие кошельки» и, во-вторых, **главное,** биржа Binance имеет возможность делать откат в сети биткоин? Фантастика!

Анонимность. Все операции с криптовалютой происходят абсолютно анонимно и все сведения о его владельце закрыты. Единственная открытая информация – это номер электронного кошелька, если, конечно сам владелец не захочет быть опознанным. Но такое уж ли это достоинство? Если вы, например, расплачиваетесь в обычном магазине обычными российскими рублями, то, по-моему, анонимность купли-продажи сохраняется абсолютно. Кто узнает, купил ли я и именно я бутылку минералки или батон хлеба? Никто! Более того, люди сами по своей доброй воле лишают себя анонимности, используя электронные средства платежа типа пластиковых карт, смартфонов и др. Но все же этот вопрос об анонимности адресантов и транзакций беспокоит больше всего и он постоянно на слуху. Так зачем же эта скрытность? А все очень просто: в магазине анонимно вы не купите наркотики, не приобретете гранатомет или автомат и т. п. Нормальный законопослушный человек не будет постоянно ежедневно менять криптокошелек, создавать новые однодневные адреса электронной почты, использовать неучтенные сим-карты. Это нужно, прежде всего, именно для скрытного осуществления незаконных действий. С учетом использования анонимайзеров, таких как TOR, продажа и распространение порнографии, наркотиков, оружия, вербовка в террористические организации, распространение экстремальной литературы, заказ убийств и поддельных документов… - все это становится анонимным и, практически, ненаказуемым. Крайне сложно, а порой и невозможно отследить трафик передвижения криптовалюты. На взгляд очень многих именно это и является наиболее привлекательным в использовании

[1] https://tehnoobzor.com.
[2] https://forklog.com.

криптовалюты биткоин. Повторюсь: разве расплачиваясь в обычном магазине обычными нашими российскими рублями, монгольскими тугриками или зелеными долларами вы не остаетесь анонимным покупателем? Видимо, здесь иные задачи, цели и принципы. И они заключаются в обеспечении бесконтрольности.

И напоследок, дополнительно, об изюминке, которая связывается с блокчейн. Это смарт-контракты. Но, на самом деле, основной принцип умного контракта состоит в полной автоматизации и достоверности исполнения договорных отношений. Все условия контракта должны иметь математическое описание и ясную логику исполнения. Да, такая технология может быть реализована и на основе блокчейн, но совсем не обязательно. Универсальность в данной сфере может оказаться даже менее эффективной, чем прагматичность. Пока это еще глубоко не рассматривалось.

Вместо заключения.

Не хочу слишком перегружать свое сообщение. У меня есть еще много вопросов о целесообразности внедрения технологии криптовалют. Это и вопросы о создании, распределении и хранении открытых и приватных ключей, и вопросы о защищенности легких и тяжелых кошельков, эффективности реализации финансовых потоков, проблема использования корпоративных или чужих ИТ-ресурсов для скрытного майнинга криптовалют и т. п. Но это отдельный разговор.

Ну раз технология блокчейн такая эффективная, то давайте внедрим её в каждый магазин и будем расплачиваться как с пластиковой карты. А почему нельзя? Не сможем обеспечить трафик? Вот оно как. Но, значит, надо не петь панегирики, а четко определять возможности и место применения такой технологии. Итак, можно ли и нужно ли использовать криптовалюту в России? Почему бы и нет? Например, создать крипторубль, контролируемый центробанком. Получаем все прелести криптовалюты плюс анонимность пользователей такая, как и у простого рубля и, при этом, без энергозатрат на майнинг и ускорением создания блоков в блокчейн. Почему плохо?

Не хочется с грязной водой выплескивать ребеночка, но нужно четко и ясно представлять область возможного применения новой технологии и опасности и угрозы, связанные с ее внедрением в повседневную жизнь. Как учили нас демократы конца XX века – рынок сам самоорганизуется и станет оптимальным. Не стал. Кажется, все-таки надо быть немного поосторожней и сначала семь раз отмерить, а потом уж отрезать.

А.Г. Волеводз

Противодействие легализации (отмыванию) доходов от преступлений, совершенных с использованием криптовалюты: правовые основы международного сотрудничества в сфере уголовного судопроизводства

Аннотация. Автором приводятся аргументы необходимости организации международного сотрудничества при расследовании преступлений, совершенных с использованием криптовалюты, с учетом того, что в большинстве случае они носят трансна-

циональный характере по способу их совершения и другим обстоятельствам, подлежащим доказыванию.

Ключевые слова: криптовалюта; легализация (отмывание) доходов от преступлений; международное сотрудничество в сфере уголовного судопроизводства; транснациональные преступления.

В последние годы все чаще легализация (отмывание) доходов от преступлений осуществляется с использованием криптовалют[1], в частности, наиболее известной из них – Биткойн (Bitcoin)[2].

Правовая неурегулированность статуса криптовалют в праве большинства стран мира осложняет не только оценку ее использования при квалификации содеянного[3], но и существенно затрудняет раскрытие и расследование преступлений при совершении которых используется криптовалюта.

На внутригосударственном уровне постепенно накапливается следственно-судебная практика расследования и разрешения уголовных дел о преступлениях, совершенных с использованием криптовалюты. Например, она свидетельствует, что примерно с 2012 года на территории России действуют преступные сообщества (преступные организации) для совершения тяжких и особо тяжких преступлений в сфере незаконного оборота наркотических средств и психотропных веществ с использованием возможностей современных телекоммуникационных сетей, в том числе Интернета, и нового расчетного инструмента – криптовалюты. В основу функционирования таких преступных сообществ (преступных организаций) положен бесконтактный способ незаконного сбыта наркотических средств путём производства тайников (закладок), с активным использованием сети Интернет (Даркнет) для обмена информацией о совершаемых преступлениях между соучастниками, общения с покупателями наркотических средств, получения электронных платежей в форме криптовалюты за реализованные наркотики в качестве оплаты противоправных действий[4].

---

[1] *Криптовалюта* – подвид нефиатных (частных) электронных денег, эмиссия (зачастую сопряженная со значительными вычислительными затратами, определяющими внутреннюю стоимость денежных единиц) и учет которых базируются на криптографических методах, а функционирование самой платежной системы происходит децентрализовано в распределенной компьютерной сети.

[2] *Биткоин* или *Биткойн* (*Bitcoin*) – нефиатные электронные средства, представляющие собой криптографические (математические) хэш-коды. Одновременно *Bitcoin* – это децентрализованная P2P сеть, обслуживаемая ее пользователями, функционирующая без органов управления и посредников на фоне отсутствия централизованного контроля. В основе этой сети лежит публичный реестр (Blockchain, или «цепочка блоков»), в котором хранится информация обо всех произведенных транзакциях пользователей сети между собой и тем самым подтверждается или опровергается факт проведения той или иной транзакции.

[3] Сидоренко Э.Л. К вопросу о статусе криптовалюты в российском и зарубежном праве // Государственная служба. 2018. Том 20. № 1. С. 53-59; Сидоренко Э.Л. Криптовалюта и преступления: проблемы правовой оценки // Банковское дело. 2018. № 7. С. 80-85.

[4] Ализаде В.А., Волеводз А.Г. Судебная практика по делам о преступлениях преступных сообществ (преступных организаций) в сфере незаконного оборота наркотиков, совершенных с использованием информационно-телекоммуникационной сети Интернет и криптовалюты // Библиотека криминалиста. Научный журнал. 2017. № 6(35). С. 281-299; Ализаде В.А., Воле-

Для таких преступлений характерна организация и деятельность преступных сообществ (преступных организаций) не только на региональном уровне (в пределах конкретного субъекта РФ), но и межрегиональном, а также, что особенно важно, на международном, уровнях. Например, «согласно части проанализированных в ходе исследования приговоров, организаторы, руководители, а также отдельные члены преступных сообществ по ряду дел находились в Украине, США, Голландии, Германии, Чехии, Таиланде. Ряд осужденных лиц являются гражданами Украины, где они прошли предварительную подготовку к совершению преступлений и откуда организованно были направлены в конкретные регионы РФ для совершения преступлений. Согласно 19 приговорам (или 20% от всех исследованных) посылки с наркотическими средствами поступали к виновным почтовыми отправления из США, Голландии, государств СНГ и других стран. Несмотря на такую широкую географию ни в одном из приговоров нет упоминания о доказательствах, свидетельствовавших бы об исследовании этих обстоятельств, равно как и нет каких-либо данных о выделении в отдельное производство дел по этим фактам, а тем более о результатах их расследования или направления для осуществления уголовного преследования компетентным органам зарубежных стран. Игнорируя организующую роль «иностранного элемента» органы следствия, а за ними и суды, не учитывали ее при квалификации содеянного осужденными»[1].

Однако «международная составляющая» этих преступлений не повлекла за собой международное сотрудничество в сфере уголовного судопроизводства, прежде всего, в силу неурегулированности правового статуса криптовалюты, и отсутствия каких-либо специальных международно-правовых механизмов, допустимых к использованию в отношении криптовалюты.

Представляется, что отказ от международного сотрудничества в сфере уголовного судопроизводства по делам о преступлениях, совершенных с использованием криптовалюты, является ошибкой в условиях, когда другие государства активно используют возможности этого направления международного сотрудничества для обеспечения привлечения к ответственности лиц, совершивших подобные преступления. Начиная с получившего широкую известность расследования компетентными органами США деятельности организатора сайта Silk Road, через который в сети Даркнет за криптовалюту реализовывались наркотики и другие предметы, изъятые из свободного оборота, международное со-

---

водз А.Г. Судебная практика по делам о преступлениях в сфере незаконного оборота наркотиков, совершенных с использованием криптовалюты: от разных подходов к предложению единого понимания // Библиотека криминалиста. Научный журнал. 2018. № 1(36). С. 306-333; Ализаде В.А., Волеводз А.Г. Судебная практика применения ст. 174.1 УК РФ по делам о наркопреступлениях, совершенных с использованием криптовалюты // Наркоконтроль. 2017. № 4(22). С. 8-14; Ализаде В.А., Волеводз А.Г. Неприменение ст. 174.1 УК РФ по делам о наркопреступлениях, совершенных с использованием криптовалюты, как следствие непонимания сущности легализации (отмывания) нового вида преступных активов // Наркоконтроль. 2018. № 1(50). С. 5-13; Чистанов Т.О. Незаконный сбыт наркотических средств с использованием телекоммуникационных сетей и устройств // Международный научно-исследовательский журнал. 2016. № 11 (53). Часть 1. С. 86-88.

[1] Там же.

трудничество при расследовании преступлений с использованием криптовалюты постоянно расширяется:

- в 2014 году завершено совместное расследование деятельности виртуальной сети распространения наркотиков, в котором приняли участие компетентные органы 14 стран («Onimys»)[1];

- в 2016 году на территории государств Евросоюза завершено расследование совершенных международной ОПГ преступлений, связанных с реализацией крупных партий фальшивых Евро с использованием криптовалют (обеспечивалось сотрудничество 8 стран)[2];

- в июле 2017 года в результате проведенного ФБР США расследования («Байонет»), в ходе которого осуществлялось сотрудничество с правоохранительными органами Литвы, Канады, Великобритании, Франции, Голландии, Таиланда и Европолом, была пресечена преступная деятельность, осуществлявшаяся через даркнетовские сайты AlphaBay и Hansa, специализировавшиеся на наркоторговле[3].

Заглавным вопросом, который встает при организации международного сотрудничества по делам о преступлениях, связанных с использованием криптовалюты в качестве средства для легализации (отмывания) доходов от преступлений, является определение надлежащей правовой основы такого сотрудничества.

В этой связи, напомним, что согласно ч. 1 ст. 453 УПК РФ «при необходимости производства на территории иностранного государства допроса, осмотра, выемки, обыска, судебной экспертизы или иных процессуальных действий, предусмотренных настоящим Кодексом, суд, прокурор, следователь, руководитель следственного органа, дознаватель вносит запрос об их производстве компетентным органом или должностным лицом иностранного государства в соответствии с международным договором Российской Федерации, международным соглашением или на основе принципа взаимности».

Несмотря на отсутствие упоминания криптовалюты и преступлений с ее использованием в международных договорах, в которых участвует Россия, существующая международно-правовая база не препятствует международному сотрудничеству в сфере уголовного судопроизводства по рассматриваемой категории дел. На сегодняшний день специалистами признано, что одной из наиболее востребованных сфер криминального использования криптовалюты считается легализация преступных доходов от незаконного оборота наркотиков, деятельность преступных организаций и финансирование терроризма. Независимо от способов использования при совершении таких преступлений криптовалю-

---

[1] Internet Organised Crime Threat Assessment (iOCTA), 2014 [Electronic resource] // EUROPOL. – URL: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2014 (Дата обращения: 01.02.2019).

[2] Internet Organised Crime Threat Assessment (iOCTA), 2015 [Electronic resource] // EUROPOL. – URL: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2015 (Дата обращения: 01.02.2019).

[3] URL: https://en.wikipedia.org/wiki/Operation_Bayonet_(darknet) ; URL: http://www.bbc.co.uk/news/technology-40670010 (Дата обращения: 01.02.2019).

ты, международно-правовая основа для противодействия им уже создана и включает хорошо известные правоохранителям антинаркотические конвенции (Единая конвенция о наркотических средствах 1961 г. и другие), антитеррористические международные договоры (48 «антитеррористических» международных договоров - 19 универсальных (14 документов и 5 поправок к ним) и 29 региональных), Конвенцию ООН против транснациональной организованной преступности и многие другие, в том числе многосторонние и двусторонние договоры о выдаче и взаимной правовой помощи по уголовным делам.

О достаточности уже действующих международных договоров для направления и исполнения ходатайств о правовой помощи по таким делам свидетельствует в частности то, что на протяжении 2017-2018 годов в производстве компетентных органов ряда европейских стран имелись уголовные дела о вымогательствах криптовалюты, совершенных с применением компьютерных вирусов-вымогателей, блокирующих информацию на компьютерах потерпевших. По имеющимся в распоряжении автора данным, российские компетентные органы исполняли запросы о правовой помощи по этим делам, направленные в Россию на основании Европейской конвенции о взаимной правовой помощи по уголовным делам.

В некоторых странах исполнение ходатайств о взаимной правовой помощи по уголовным делам, связанным с использованием криптовалюты, в ближайшей перспективе будет опираться не только на международные договоры, но и внутригосударственное законодательство. В первую очередь это относится к странам-членам Европейского союза. В рамках этого интеграционного образования принята Директива (ЕС) 2018/843 Европейского парламента и Совета от 30 мая 2018 года об изменении Директивы ЕС 2015/849 о предотвращении использования финансовой системы в целях отмывания денег или финансирования терроризма и изменении Директив 2009/138/ЕС и 2013/36/ЕС1. Директива:

требуют от платформ, обеспечивающих трансфер криптовалют и провайдеров электронных кошельков, принимать исчерпывающие меры по идентификации своих клиентов;

обязывает государства-члены ЕС обеспечить, чтобы провайдеры ресурсов, осуществляющих обмен виртуальных валют на фиатные деньги и поставщики кошельков виртуальной валюты регистрировались, с тем чтобы должным образом обеспечивался контроль такого обмена валюты и проверки кассовых офисов таких поставщиков;

усиливает требования к прозрачности операций с криптовалютой, в значительной мере предопределяя их деанонимизацию;

открывают национальным правоохранительным службам широкий доступ к информации об операциях с криптовалютой, в том числе к регистрационным данным участвующих в этом физических и юридических лиц.

[1] 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. – Official Journal of the European Union. -19.6.2018 - L156/43-74.

Тем самым Директива создала правовую основу для поступательного развития сотрудничества как между государствами-членами Евросоюза, так и со странами, не являющимися членами ЕС, в борьбе отмыванием доходов от преступлений с использованием криптовалюты1.

Следует обратить внимание и на то, что ныне на органы предварительного расследования России возложен минимальный круг обязанностей по установлению обстоятельств, способствовавших совершению преступления, и их устранению путем внесения соответствующих представлений (ч. 2 ст. 158 УПК РФ). Однако этого недостаточно для устранения обстоятельств, способствующих совершению транснациональных преступлений. Это обусловлено тем, что в сфере транснациональной криминальной деятельности Россия выступает: 1) как территория, на которую направлена криминальная деятельность с территории иностранного государства, 2) как государство, с территории которого криминальная деятельность направлена на территорию под юрисдикцией другого государства, 3) как страна транзита для совершения транснациональных преступлений[2].

В силу этого, отказ от международного сотрудничества в сфере уголовного судопроизводства создает благоприятные условия для бесконтрольной транснационализации преступности с использованием криптовалюты.

Данная проблема в рамках действующего уголовно-процессуального законодательства и международных договоров должна разрешаться на досудебных стадиях процесса путем реализации институтов взаимной правовой помощи по уголовным делам, выдачи и направления уголовных дел для осуществления уголовного преследования компетентным органам иностранных государств (в случаях невыдачи лиц, подлежащих привлечению к уголовной ответственности) по всем уголовным делам при расследовании которых имеются основания – достаточные данные, свидетельствующие о транснациональном характере способа совершения преступлений и других обстоятельств, подлежащих доказыванию.

Для целенаправленного предупреждения транснационализации преступлений, совершенных с использованием криптовалюты, представляется необходимым обязательно информировать компетентные органы иностранных государств о таких преступлениях используя для этого возможности, предоставляемые широким кругом международных договоров. В частности, согласно п. 4 ст. 18 Конвенции ООН против транснациональной организованной преступности

---

[1] Ализаде В.А. Оборот криптовалюты в Европейском союзе: на пороге правового регулирования // Библиотека криминалиста. Научный журнал.2018. № 2(37). С. 316-327; Ализаде В.А. О формировании правового регулирования оборота криптовалюты в антикриминальных целях (на примере Европейского союза) // Международное уголовное право и международная юстиция. 2018. № 3. С. 19-22.

[2] Хижняк Д.С. Борьба с транснациональными преступлениями и их расследование: стратегические аспекты: монография / под науч. ред. докт. юрид. наук А.Г Волеводза. – М: Юрлитинформ, 2015; Хижняк Д.С. Информационные модели транснациональной криминальной деятельности: монография / под науч. ред. докт. юрид. наук А.Г Волеводза. – М: Юрлитинформ, 2018.

«без ущерба для внутреннего законодательства компетентные органы Государства–участника могут без предварительной просьбы передавать информацию, касающуюся уголовно-правовых вопросов, компетентному органу в другом Государстве–участнике в тех случаях, когда они считают, что такая информация может оказать помощь этому органу в осуществлении или успешном завершении расследования и уголовного преследования или может привести к просьбе, составленной этим Государством–участником в соответствии с настоящей Конвенцией»[1].

Принимая решение о дальнейшем направлении расследования в случаях выявления «иностранного элемента» в делах о преступлениях, связанных с использованием криптовалюты для легализации (отмыванию) доходов от преступлений, наряду с иными факторами следует исходить из того, отказ от принятия мер по организации и участию в международном сотрудничестве при расследовании уголовных дел о таких преступлениях, противоречит интересам полного раскрытия и расследования таких преступлений, выявления всего круга лиц, виновных в их совершении, предупреждения таких преступлений как на внутригосударственном, так и международном уровнях.

Литература

1. Ализаде В.А. Оборот криптовалюты в Европейском союзе: на пороге правового регулирования // Библиотека криминалиста. Научный журнал. 2018. № 2(37). С. 316-327.
2. Ализаде В.А. О формировании правового регулирования оборота криптовалюты в антикриминальных целях (на примере Европейского союза) // Международное уголовное право и международная юстиция. 2018. № 3. С. 19-22.
3. Ализаде В.А., Волеводз А.Г. Судебная практика по делам о преступлениях преступных сообществ (преступных организаций) в сфере незаконного оборота наркотиков, совершенных с использованием информационно-телекоммуникационной сети Интернет и криптовалюты // Библиотека криминалиста. Научный журнал. 2017. № 6(35). С. 281-299.
4. Ализаде В.А., Волеводз А.Г. Судебная практика по делам о преступлениях в сфере незаконного оборота наркотиков, совершенных с использованием криптовалюты: от разных подходов к предложению единого понимания // Библиотека криминалиста. Научный журнал. 2018. № 1(36). С. 306-333.
5. Ализаде В.А., Волеводз А.Г. Судебная практика применения ст. 174.1 УК РФ по делам о наркопреступлениях, совершенных с использованием криптовалюты // Наркоконтроль. 2017. № 4(22). С. 8-14.
6. Ализаде В.А., Волеводз А.Г. Неприменение ст. 174.1 УК РФ по делам о наркопреступлениях, совершенных с использованием криптовалюты, как следствие непонимания сущности легализации (отмывания) нового вида

[1] Конвенция ООН против транснациональной организованной преступности // Собрание законодательства РФ. 2000. № 50. Ст. 4894.

преступных активов // Наркоконтроль. 2018. № 1(50). С. 5-13.
7. Сидоренко Э.Л. К вопросу о статусе криптовалюты в российском и зарубежном праве // Государственная служба. 2018. Том 20. № 1. С. 53-59.
8. Сидоренко Э.Л. Криптовалюта и преступления: проблемы правовой оценки // Банковское дело. 2018. № 7. С. 80-85.
9. Хижняк Д.С. Борьба с транснациональными преступлениями и их расследование: стратегические аспекты: монография / под науч. ред. докт. юрид. наук А.Г Волеводза. – М: Юрлитинформ, 2015. 184 с.
10. Хижняк Д.С. Информационные модели транснациональной криминальной деятельности: монография / под науч. ред. докт. юрид. наук А.Г Волеводза. – М: Юрлитинформ, 2018. 248 с.
11. Чистанов Т.О. Незаконный сбыт наркотических средств с использованием телекоммуникационных сетей и устройств // Международный научно-исследовательский журнал. 2016. № 11 (53). Часть 1. С. 86-88.
12. Internet Organised Crime Threat Assessment (iOCTA), 2014 [Electronic resource] // EUROPOL. – URL: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2014 (Дата обращения: 01.02.2019).
13. Internet Organised Crime Threat Assessment (iOCTA), 2015 [Electronic resource] // EUROPOL. – URL: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2015 (Дата обращения: 01.02.2019).

Л.В. Голоскоков

Философско-юридическое осмысление феномена криптовалют

Аннотация. Рассматривается ситуация с криптовалютами в России с позиций философского подхода, когда от конкретной частной проблемы предлагается переход к более общей проблеме и определяются подходы к её решению – частные и общие. Предлагается частично уйти от навязываемых извне проблем путём создания своего глобального поля действий, на котором правила игры будет задавать Россия, в том числе, возможно, путём создания более обеспеченной российской валюты или криптовалюты для укрепления финансового и экономического положения России.

Ключевые слова: философия, право, государство, валюта, криптовалюта, стратегия.

В настоящем обзоре мы оденем философские очки и посмотрим на проблему с общих философских позиций, чтобы увидеть, как данное явление включено в контекст других событий, какую роль играет феномен криптовалют в современной ситуации, в которой находится Россия. При этом мы не будем касаться никаких технических и узкоспециальных юридических аспектов.

Если посмотреть на процесс обсуждения проблем криптовалют с большой высоты, мы увидим картину такого плана: множество маленьких клеточек залов, где сидят специалисты и обсуждают критовалюты. Вот они все внизу, в

виде клеток шахматной доски, сведённые мысленным приёмом во времени на одну площадку. Одновременно идут дискуссии по близким темам: валюта, вывоз капитала, отмывание денег, нехватка инвестиций, инфляция, таргетирование, проблемы, связанные с ВТО, Всемирным банком, МВФ и многие другие. Поле проблем расширилось, и мы видим нашу проблему криптовалют в контексте массы иных схожих, близких, не очень близких и совершенно разных и очень сложных проблем. Все они располагаются на огромном поле клеток, связаны между собой, но многие связи нам не видны вообще, и мы пытаемся найти решения массы изолированных для нас проблем силами специалистов и разных государственных институтов.

Мы действуем разрозненно, не видя всего поля проблем и того, откуда они все берутся, не видим связи многих проблем во времени, а они идут одна за другой, и мы часто думаем, что вот, появилась новая тема, нужно её обсуждать, решать новые задачи, отвечать на новые вызовы. А есть ли у нас ресурсы для решения возрастающего потока задач, сложность которых также растёт? Ресурсов не хватает, и это подтверждает, в частности, реакция ЦБ РФ, который с 2014 года отреагировал на появление биткоинов разъяснением в своих письмах лишь того, что это рискованно и опасно. Нулевая реакция на динамичное событие мирового масштаба, что и доказывает отсутствие и уменьшение интеллектуальных и всех прочих ресурсов.

Жизнь не остановилась на биткоине и преподнесла серию криптовалют. Криптовалюта в нашем обзоре – это метафора, лишь один из источников множества информационных проблем, и ни на одной из них, ни на одной криптовалюте не написано, что она создавалась против России или её граждан. Обобщаем их все. Что видно с высоты философских обобщений? Видно, что мы играем на большом поле, которое построено кем-то, мы видим только свою клетку, в которой обсуждаем узкую проблему, мы в этой игре ведомые, не знаем, что будет следующим вызовом, потому что планировщик нам об этом не сказал. Мы не знаем его планов по вбрасыванию проблем на других полях, не понимаем, как всё это связано и каков стратегический замысел противника. Возможно, что силы, которые планируют эти проблемы, приготовили их для нас целую серию, и они будут последовательно возникать, а пока мы будем их решать, время истощит наши ресурсы, и мы не решим другие действительно важные задачи.

Обратим внимание на ключевое слово в названии нашего «круглого стола». Юристы сочтут, что это криптовалюта. Да, от её проблем теперь не уйдёшь, но с философских позиций ключевое слово другое – «противодействие»! Есть известные русские слова: вечереет, громыхает. Громыхать может очень сильно, но за грозным явлением нет субъекта. Мы же в названии сами указали, что есть действие, кто-то наносит удар, и этот кто-то – субъект, а если он начал действовать, значит, имел некий план. От реализации этого плана у нас проблемы, поэтому мы и собрались на «круглом столе». Кому мы предъявим претензии по проблемам криптовалюты: мифическому Накамото, Пентагону, всем мировым сетям? Каким силам мы собрались противодействовать?

Оказалось, что сила и субъект – где-то вне зоны досягаемости наших сил и средств, а проблема уже здесь и сейчас, и мы собрались её решать.

Вообще говоря, не суть важно, существует ли такой единый планировщик или так получается в реальности ещё и от действия факторов развития техники, прогресса, но картина именно такова, как будто действует субъект. То, что в США продолжают работать против России целые институты, давно известно: Минфин, Пентагон, АНБ и др. Разумеется, там точно так же работают и против других стран, но это беды других стран. Война в сетях – это информационная война, она ведётся круглосуточно и безжалостно, то есть, нам не дадут в этой войне скидку на нашу неопытность или убогость и не будут ждать, пока мы поумнеем и обретём силу для ответного удара.

Д.Б. Изюмов и Е.Л. Кондратюк пишут: «Примером организации сетей «гражданских сетецентрических войн» могут служить создаваемые в настоящее время в Пентагоне межфункциональные группы («Cross-functional teams» – CFTs). Данные группы создаются с целью оптимизации системы принятия решений, выработки эффективного и молниеносного решения возникшей проблемы, в интересах создания временного запаса и обеспечения доминирующих позиций в любом возникающем кризисе. Данная концепция уже широко применяется бизнесом и гражданскими органами управления США»[1]. Обратим внимание, что Пентагон перебросил войну в сферу гражданских отношений. Юристы этого ещё не поняли, а когда ощутят эти действия, начнут готовиться к противодействию и искать виновных. А.В. Федоров пишет, что «за рубежом чаще законодательно устанавливается корпоративная ответственность (ответственность организаций) и её субъектами являются не только юридические лица, но и другие образования. При этом не во всех странах имеется одинаковое определение того, что есть юридическое лицо как таковое»[2].

Когда юристы разберутся с определениями, введут новые законы или нормы в Уголовный кодекс, включая, возможно, и в отношении наших юридических лиц, или поймут, как с помощью имеющихся норм применить наказание к тем, кто будет использовать криптовалюты в противоправных целях, противник тотчас же будет нами идентифицирован, и это будет только российский гражданин или юридическое лицо. Может нам привлечь к ответственности американский Минфин, Пентагон и других лиц по списку – от АНБ до ЦРУ? Да, есть вероятность, что будет наказан иностранный гражданин, который совершит правонарушение или преступление на территории России, но об этом не стоит говорить – маловероятно, а иностранное юридическое лицо мы не достанем. Так где же тогда наш противник, которому мы собрались противодействовать? Мы видим, что план действующего лица оказался гениальным: субъекта вредоносного действия нам не достать, ибо мы не знаем, кто он и где он, а противодействующая сила (это мы) нанесёт в конечном итоге удар по своему юридическому лицу или человеку, пусть и преступнику, правонарушителю. Своими руками накажем своих лиц и людей. Вывод – противником стали мы сами! Вот

[1] Изюмов Д.Б., Кондратюк Е.Л. Гражданские сетецентрические войны // Инноватика и экспертиза. Научные труды. 2016. Выпуск 3 (18). С. 84

[2] Федоров А.В. Уголовная ответственность юридических лиц как составляющая правового администрирования // Вестник Московской академии Следственного комитета Российской Федерации. 2018. № 3. С. 23.

это и есть настоящий инструмент гибридной информационной войны. Юристам нужно учиться играть на глобальном мировом поле, не запираться в ракушку своих частных проблем: из слегка приоткрытой юридической раковины не видно всего многообразия мира.

В деле обсуждения криптовалют, так же как и в попытках решить иные подобные проблемы, мы идём вдогонку, поэтому не видим предложенный нам путь, но он ясен противнику, который ведёт нас к поражению не спеша, чтобы мы не поняли, куда и зачем мы идём. Далее нас ждёт следующая заготовка планировщика под каким-то иным мудрёным названием, в новой технологической оболочке, долгий путь противодействия и последующего запрограммированного поражения. Поражение состоит ещё и в том, что мы будем поражать своих лиц, а не иностранных, которые создали нам проблемы.

Вот доказательства. Вспомним уже состоявшийся путь подобного рода. Россия 16 лет пыталась вступить в ВТО. Против вступления России была Грузия, вступившая туда намного раньше, но мы очень хотели попасть туда, куда все шли толпой. Мы не хотели видеть, что все вступившие в ВТО намного раньше России небольшие страны (Киргизия, Латвия, Эстония – вступили в 1999 году), к 2012 году, то есть, к моменту вступления России в ВТО, не встали на путь процветания. Спустя всего 2 года, даже Президент Российской Федерации В.В. Путин выразил сомнение: «Введённые против нашей страны ограничения – это не что иное, как отказ от базовых принципов ВТО некоторыми нашими партнёрами. Нарушается принцип равенства условий доступа всех стран – участников экономической деятельности к рынкам товаров и услуг, игнорируется режим наибольшего благоприятствования в торговле и принцип справедливой и свободной конкуренции. Делается это всё политизированно, без всякого соблюдения общепризнанных норм той самой Всемирной торговой организации, о которой я только что говорил. Фактически группа стран в одностороннем порядке позволила себе зачеркнуть эти и ряд других принципов и правил ВТО для России»[1]. А мы ждали там нарисованный рай, погнались за ним в ВТО, которая, оказывается, была создана вовсе не для того, чтобы облагодетельствовать Киргизию или Россию.

Причина такого положения дел. Мы позволили себя втянуть на чужое поле в игру по чужим правилам, которые созданы так, что выигрыш обеспечен только создателю. Это касается и криптовалюты, и ВТО и прочего. Мы вторичны, без идеи, без собственного плана, принимаем то, что нам навязывают. Мы не имеем глобального взгляда, потому что у нас местечковое сознание, которое и не позволяет подняться над ворохом частных (узкоспециальных) проблем и увидеть, что нас используют в своих целях. Плоскостное мышление не позволяет понять, что игра идёт даже не на поле, а в многомерном пространстве и во времени, где нужно быстро думать, искать новые подходы, действовать нестандартно и опережающим образом. Так действуют сетевые структуры в киберпространстве, в котором наша вертикаль власти и государства (иерархическая система)

[1] Путин В.В. Заседание Государственного совета. 18 сентября 2014 года 16:30. Официальный сайт Президента Российской Федерации, http://www.kremlin.ru/events/president/news/46636.

не может находить решения, ибо это совершенно новая и необычная для неё среда. Для этого нужны новые сетевые инструменты и методы и другой тип мышления, организации науки, производства, культуры.

Для решения частных проблем, порождаемых криптовалютами, а также иных информационных проблем, нам нужно научиться мыслить глобально, стать глобальным игроком с сознанием победителя. Для этого нужна сильная идея государства, которая будет привлекательна как для своих граждан и для граждан других стран. На основе идеи нужно разработать свою доктрину и стратегию. Только после обретения глобального видения, формирования образа будущего и образа победы мы сможем перейти от ответов на вызовы, которые кто-то генерирует, к собственным амбициозным планам и перестать отвечать на всякий окрик со стороны. Без образа будущего решение частных проблем не имеет смысла. Сначала нужно сменить последовательность действий: общее, а потом частное. Разумеется, часть вызовов и проблем порождена обстоятельствами, прогрессом и его оборотной стороной, другими факторами, а не сознательно действующим против нас субъектом. Известно и то, что максимальное количество проблем мы порождаем для себя сами.

Имея стратегию, можно и нужно выстраивать собственные поля игры со своими правилами, в рамках которых, не исключено, мы создадим собственные криптовалюты для нужных нам целей и в нужном количестве. Точно так же мы можем создавать и другие инструменты для достижения наших целей, а эти инструменты, должны будут использовать все новейшие технологии: электронные, сетевые, цифровые и прочие современные и будущие.

Например. Криптовалюта – это слово имеет главный корень и содержание – валюта, а «крипто» имеет второстепенный характер. Сегодня она «крипто», а завтра будет какая-нибудь «нано» или «кванто». Мы не знаем. Нам нужно работать на опережение, а не плестись в хвосте чужих идей и интересов. В данном случае, с криптовалютой с нами обошлись именно так: мы увидели (или нам создали) проблему, а мы ищем ответы вместо нападения, опережения, творчества и захвата рынков или интеллектуального пространства, мы похожи на лиц, которых используют втёмную, которых хотят измотать в бесплодной борьбе с виртуальным монстром, и где гарантия, что завтра нам не подкинут «суперкриптовалюту», с которой мы будем иметь ещё больше проблем?

Почему бы нам не создать свою более привлекательную валюту в ответ и не только в ответ, а для опережения. Для этого нужно сделать наполнение российской валюты такое, чтобы оно было более солидным, чем ранее давало золото, которым обеспечивался рубль или доллар до Бреттон-Вудской конференции 1944 г., когда считалось, что эти валюты были обеспечены золотом (мы не вступаем в дискуссию о том, в какой степени валюты действительно были обеспечены золотом). Нам надо уйти от состояния, когда «наличие ядерного оружия – единственное на сегодня материальное свидетельство того, что Рос-

сия является великой державой»[1] и добавить к списку признаков великой державы обеспеченную валюту, экономику и др.

Для этого мы предлагаем составить математическое уравнение, в котором будут сложены разнородные сущности – финансы и ценности. В нём можно будет представить в отвлечённых цифрах – индексах (вариант – в натуральных показателях), какие ресурсы и в каких количествах имеет Россия. Уравнение и предшествующая ему его табличная форма собранных данных также должны показать, чего не имеют другие страны и народы, и как это можно использовать. Нужно составить перечень всех таких ресурсов и ценностей и произвести с ними вычисления, позволяющие объединить их все в одной формуле и отразить далее в рейтинге подобных же вычислений, сделанных для других стран. Понятно, что все рейтинги условны в силу различия их методик и в силу ангажированности рейтинговых агентств, но данный рейтинг мы будем составлять для пользы России, поэтому если мы в этом рейтинге где-то будем надувать щёки от важности, то надо понимать, где мы это можем делать: запросто и не оглядываясь ни на кого – в сфере нефтяной и газовой, поскольку у России крупнейшие запасы в мире, в пространственной, земле-почвенной, лесной, пресноводной и других сферах, где у нас неоспоримые преимущества перед всеми странами мира. Уравнение покажет и основу обеспечения рубля.

Приводимая нами формула заведомо упрощена, она показывает метод и обозначает вектор развития науки, в частности, экономики, финансов, права, поскольку наши предложения в конечном итоге могут быть в какой-то части закреплены в виде норм права, регулирующие финансы и экономику.

Россия имеет ресурсы: газ, нефть, уголь, иные полезные ископаемые, лес, энергетические ресурсы, объекты животного мира и объекты водных биологических ресурсов. Особо ценным ресурсом скоро станет питьевая вода. Ресурс, который обычно не продаётся – это территория государства (исключение из правила – продажа Аляски), иначе говоря, пространство.

Особый ресурс, который Россия тратила не по-хозяйски, – это научный потенциал: по данным МВД России за период 1992-2001 годы эмигрировали 45544 работников науки[2]. Сложно формализуемый и вычисляемый ресурс – это образовательный уровень страны, который складывается из количества учёных, инженеров и других специалистов, качества их знаний. Наконец, нужно использовать суммарные ресурсы и ценности прошлого – достижения России в литературе, культуре, искусстве, науке, живописи, архитектуре, спорте и т.д., поскольку эти ранее созданные ценности позволяют и сегодня извлекать их них значительные доходы (спорт, туризм и др.).

Наша задача – рассчитать некий суммарный потенциал России, стоимостную оценку её материальных и нематериальных ресурсов и получить в итоге выигрышную картину, которая показала бы, что в России итоговая сумма её ценно-

---

[1] Макаренко В.П. Современный российский милитаризм (статья вторая) // Политическая концептология. 2013. № 4. С. 10.

[2] Агамова Н.С., Аллахвердян А.Г. Утечка умов из России: причины и масштабы // Наука России. От настоящего к будущему / Под. ред. В.С. Арутюнова, Г.В. Лисичкина, Г.Г. Малинецкого. Изд. 2-е. М.: Книжный дом «ЛИБРОКОМ», 2009. С. 355.

стей, рассчитанная по этому уравнению, существенно выше, чем во многих других странах. Эту гипотезу нужно облечь в математически форму, исходя из понимания, что Россия по многим показателям занимает в разных мировых рейтингах весьма посредственные места, плохо коррелирующие с её потенциалом, и составление рейтинга, в котором Россия объективно займёт более приличное место, будет важной политической, пропагандистской, психологической задачей, решение которой покажет пути преодоления социального пессимизма, который несут с собой многие нынешние рейтинги России. Пора заменить точку невозврата точкой валютного оптимизма.

Такой формой может стать уравнение ценностей, включающее в себя все значимые виды ресурсов России, взвешивающее ценности этих ресурсов с помощью весовых коэффициентов (методику определения коэффициентов мы не рассматриваем, ибо это отдельная задача, в большей степени экономическая, политическая, чем правовая). Данное уравнение нужно будет использовать для расчёта такой же системы ценностей для других государств, которые есть смысл сравнивать с Россией.

Итоговый вид уравнения ценностей для России и любого конкретного государства:

$V = k_1G + k_2O + k_3Md + k_4W + k_5Nr + k_6S + k_7Pl + k_8Sc + k_9E + k_{10}I$

Здесь использованы следующие обозначения:

V – численное выражение суммы ценности всех существующих ресурсов государства (в т.ч. интеллектуального, научного, культурного и других); вообще говоря, может иметь два выражения – отдельно денежное, а отдельно – числовое, когда абстрактное число (индекс) будет характеризовать сумму ценностей;

k_1 – коэффициент, указывающий вес (значение) параметра G;

G – стоимостной (или натуральный) объём запасов газа государства;

k_2 – коэффициент, указывающий вес (значение) параметра O;

O – стоимостной (или натуральный) объём запасов нефти государства;

k_3 – коэффициент, указывающий вес (значение) параметра Md;

Md – стоимостной (или натуральный) объём месторождений полезных ископаемых государства, включая наличное золото, серебро, платину, палладий, уран и их разведанные запасы;

k_4 – коэффициент, указывающий вес (значение) параметра W;

W – стоимостной (или натуральный) объём запасов пресной воды государства;

k_5 – коэффициент, указывающий вес (значение) параметра Nr;

Nr – стоимостной (или натуральный) объём всех остальных природных богатств государства;

k_6 – коэффициент, указывающий вес (значение) параметра S;

S – площадь всей территории государства;

k_7 – коэффициент, указывающий вес (значение) параметра Pl;

Pl – площадь пахотных земель на территории государства;

k_8 – коэффициент, указывающий вес (значение) параметра Sc;

Sc – суммарный показатель, характеризующий уровень развития науки в государстве;

k9 – коэффициент, указывающий вес (значение) параметра E;

E – суммарный показатель, характеризующий уровень образования всех граждан данного государства;

k10 – коэффициент, указывающий вес (значение) параметра I;

I – суммарный показатель, характеризующий уровень интеллекта всех граждан данного государства.

Коэффициенты k1–k10 должны иметь соответствующую размерность, позволяющую получить итоговую сумму в виде показателя (индекса), не имеющего размерности, или денежного показателя.

Определение каждого из слагаемых представляет собой сложную задачу. По этому поводу В.Л. Иноземцев справедливо отмечает, что «все отмеченные методики и многие активно разрабатываемые в наши дни подходы к определению стоимости интеллектуального и, в частности, человеческого капитала не совершенны, ибо ориентированы на суждение о субъективных предпочтениях по динамике денежных показателей»[1]. Однако это означает, что экономистам нужно активнее совершенствовать методики расчётов.

Десяти приведённых нами параметров достаточно, чтобы обозначить цель и принцип построения данной формулы и понять, что нужно иметь в уравнении гораздо больше параметров, чтобы учесть все особенности России, и все основные виды ценных ресурсов. После составления полной формулы можно сделать расчёты по этой формуле для других стран и сравнить их итоговый потенциал. Сформулировав эту задачу в общем виде, мы оставляем её детальное решение экономистам, математикам, статистикам, финансистам, историкам, географам и другим специалистам.

Показатель V – численное выражение суммы ценности всех существующих ресурсов России, в состав которых входит и золото, которое мы не выделяли специально, поскольку в качестве обеспечения валюты могут использоваться и иные металлы платиновой группы, и не только они, и на фоне суммы всех остальных ценностей все они вместе взятые не будут доминирующими. Поэтому брать для обеспечения валюты только одно золото представляется весьма архаичным подходом, в то время как сегодня можно неплохо подсчитать и использовать для этих целей всю совокупность ценностей – V, что и позволит сделать валюту более обеспеченной и надёжной. В то же время V – это также показатель для рейтинга.

Большинство войн в мире были затеяны за обладание ресурсами. В связи с особой важностью ресурсов следует в уравнении придать им соответствующий вес. Во время войны современной и масштабной золото не обязательно будет цениться так, как во время Второй мировой войне, когда за него покупали оружие и продовольствие. Для таких покупок нужно долго транспортировать золото в одну сторону, а товар – в другую, и будет ли это возможно на театрах военных действий на морях и океанах, представляется сомнительным. А нату-

[1] Иноземцев В.Л. За пределами экономического общества: Научное издание. М., 1998. С. 33.

ральный продукт, имеющийся в наличии, позволяющий удовлетворять первичные жизненные потребности здесь и сейчас (зерно, вода, уголь, нефть и др.) будет иметь непреходящую ценность, и в рейтингах и в их комментариях нужно эту мысль постоянно озвучивать с разных сторон, доказывая тем самым надёжность и обеспеченность валюты при любых событиях, тем более, форсмажорных, чего не будет у большинства стран мира.

Можно предположить, что расчёт по формуле покажет, что потенциал России выше, чем её положение, рассчитанное, например, по известным экономическим показателям типа ВВП на душу населения, и это будет служить важным ориентиром для развития страны, поднятия внутренней убеждённости власти и граждан в имеющихся перспективах России. Так нужно и сделать. А делать это может ЦБ РФ совместно с Минфином, с НИИ и кафедрами ведущих экономических, технических и иных вузов страны, которые могут постоянно или периодически участвовать в работе по составлению, поддержанию, обновлению рейтинга страны, расчёту стоимости обеспечения валюты России на текущий момент, распространению этой информации в мире в сетях и СМИ.

Постоянное определение и обновление стоимости всех ресурсов (показатель V) на текущий момент времени будет важным для того, чтобы всё время держать в курсе (и привлекать повышенное внимание) всех инвесторов, граждан и стран, желающих иметь резервы в надёжной валюте, чтобы постоянный интерес заставлял помнить о России как глобальной державе, имеющей совокупные ресурсы, которые, безусловно, ставят её в состав лидеров мира, несмотря на 2% мирового ВВП, которые она занимает сегодня в мире. Наше предложение хорошо также тем, что не потребует для реализации бюджетных денег, а простое переформатирование взгляда на самих себя даст хороший повод для излучения конструктивного оптимизма.

Да, если России начнёт осуществлять такой проект, вал критики будет обеспечен. Но пусть попробуют вставить в аналогичные клеточки нашей формулы свои значения запасов нефти и прочего, что мы им и предложим сделать. Получится у совсем немногих стран – США и Саудовской Аравии. Венесуэла, хотя и поставит что-то по нефти, но по всем остальным позициям будет смотреться хуже. Китай и ряд стран покажут превосходящие наличные запасы золота. Пусть покажут, а в остальном Россия будет опережать всех. Страны и лица, вложившиеся в валюту России, обеспеченную новыми ценностями, понимающие, почему они вложились, будут так или иначе заботиться и беречь чужие для них ценности (российские), потому что они станут их ценностями. Новый валютный мир, который уже начал активно создаваться в процессе переформатирования ценности и круга обращения ныне главных мировых валют, нужно встречать подготовленными заранее и предложить миру свою, укреплённую нашими ценностями, валюту.

Так, начиная со своей валюты, если нужно, своих криптовалют, привязанным или непривязанным ко всем ценностям или ресурсам России, мы сможем начать формировать свои поля игры, создавая на них выгодные для нас правила и головную боль решения возникающих от этого проблем у других стран-конкурентов в финансах, инвестициях, торговле, бизнесе и прочих делах.

Тогда мы не будем ломать голову над проблемами, создаваемыми нам чужими криптовалютами (например, так называемые атаки Финни, атаки Сибиллы[1] и многие другие) и прочими элементами информационного оружия, и думать, что с ними делать – пусть они думают, что делать с нашими, собирают своих учёных и проводят «круглые столы» по российской валюте и криптовалюте. Мы приедем и всё им разъясним. Снимаем философские очки…

Литература

1. Перов В.А. Выявление, квалификация и организация расследования преступлений, совершаемых с использование криптовалюты: учеб.-методич. пособие. М.: Юрлитинформ, 2017. 200 с.
2. Федоров А.В. Уголовная ответственность юридических лиц как составляющая правового администрирования // Вестник Московской академии Следственного комитета Российской Федерации. 2018. № 3. С. 18-27.

К.К. Грошиков

О требованиях Группы разработки финансовых мер борьбы с отмыванием денег относительно регламентации оборота виртуальных активов в государстве

Группа разработки финансовых мер борьбы с отмыванием денег (ФАТФ) первая обратила внимание международного сообщества на новую угрозу, связанную с появлением по существу новых объектов экономических отношений – криптовалюты и иных виртуальных активов.

В 2014 году ФАТФ опубликовала отчет «Виртуальные валюты», где содержались ключевые термины и определения нового явления, в том числе определение виртуальных валют, которые согласно документу представляет собой средство выражения стоимости, которым можно торговать в цифровой форме и которое функционирует в качестве средства обмена, расчетной денежной единицы или средства хранения стоимости, но не обладает статусом законного платежного средства (т.е. не является официально действующим и законным средством платежа при расчётах с кредиторами) ни в одной юрисдикции.

ФАТФ в 2015 году выпустила Руководство по применению риск-ориентированного подхода «Виртуальные валюты», где отмечается, что платежные продукты и услуги на основе виртуальной валюты представляют риски отмывания денег и финансирования терроризма, а также риски совершения других преступлений, которые необходимо выявлять и снижать.

В числе прочего была отмечена необходимость оценивать риски от платежных продуктов на основе криптовалюты. По итогам оценки рисков государ-

[1] Перов В.А. Выявление, квалификация и организация расследования преступлений, совершаемых с использование криптовалюты: учеб.-методич. пособие. М.: Юрлитинформ, 2017. С. 92-94.

ствам следует принять решение об объеме регулирования оборота криптовалюты.

В октябре текущего года Группой ФАТФ было сделано заявление по виртуальным активам, а также изменен текст Рекомендаций ФАТФ (данный термин включает в себя как криптовалюту, так и токены, выпускаемые в рамках их привязки к традиционным финансовым инструментам, например, ICO).

Суть изменений, внесенных в стандарты ФАТФ, состоит в дополнении Рекомендации 15 ФАТФ положением, согласно которому провайдеры услуг в сфере виртуальных активов должны быть охвачены регулированием сферы противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, подлежать лицензированию или регистрации, а также подлежать эффективным системам мониторинга и обеспечения соблюдения соответствующих мер, к которым призывают Рекомендации ФАТФ.

Также, глоссарий к Рекомендациям ФАТФ дополнен определениями виртуальных активов и провайдеров услуг в сфере виртуальных активов.

Согласно определениям виртуальный актив – это цифровое выражение ценности, которое может торговаться или переводится в цифровом виде и может быть использовано для целей платежа или инвестиций. Виртуальные активы не включают в себя цифровое выражение фиатных валют, ценных бумаг и других финансовых активов, которые уже как-либо охвачены Рекомендациями ФАТФ; провайдер услуг виртуальных активов означает любое юридическое или физическое лицо, неохваченное каким-либо образом Рекомендациями ФАТФ и которое осуществляет в качестве предпринимательской деятельности один или более следующих видов деятельности или операций в отношении другого физического или юридического лица:

- обмен между виртуальными активами и фиатными валютами;
- обмен между одной и более видами виртуальных активов;
- перевод (осуществление операции от имени другого физического или юридического лица, которое перемещает виртуальный актив с одного адреса или счета виртуальных активов на другой) виртуальных активов;
- хранение и (или) администрирование виртуальных активов или инструментов, позволяющих осуществлять контроль над виртуальными активами;
- предоставление финансовых услуг, связанных с предложением выпускающего лица и (или) продажей виртуального актива или участие в такой деятельности.

В своем заявлении ФАТФ отметило срочную необходимость для всех стран принять скоординированные меры и предотвратить использование виртуальных активов в преступных целях.

Заявление ФАТФ акцентирует необходимость проведения оценки рисков отмывания денег и финансирования терроризма в отношении виртуальных активов.

В настоящее время подготовлен проект изменений в Пояснительную записку к Рекомендации 15 ФАТФ. Их суть в предписании государствам рассматривать виртуальные активы как имущество, а также в определении требований к провайдерам услуг виртуальных активов.

Работа по правовой регламентации оборота виртуальных активов в Российской Федерации осуществляется согласно перечню поручений Президента Российской Федерации по итогам совещания по вопросу использования цифровых технологий в финансовой сфере, состоявшегося 21 октября 2017 года.

В рамках указанного поручения принят Федеральный закон от 18.03.2019 № 34-ФЗ «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации», которым предусмотрено введение в гражданский оборот нового вида имущества – цифровых прав.

Согласно части 1 статьи 141.1 Гражданского кодекса Российской Федерации цифровыми правами признаются названные в таком качестве в законе обязательственные и иные права, содержание и условия осуществления которых определяются в соответствии с правилами информационной системы, отвечающей установленным законом признакам. Осуществление, распоряжение, в том числе передача, залог, обременение цифрового права другими способами или ограничение распоряжения цифровым правом возможны только в информационной системе без обращения к третьему лицу.

Исходя из смысла приведенной нормы, требуется принятие федеральных законов в целях признания виртуальных активов, предполагаемых к обороту на территории государства, цифровыми правами.

Такой законопроект в настоящее время внесен в Государственную Думу и принят в первом чтении - проект федерального закона № 419059-7 «О цифровых финансовых активах». Указанный законопроект вводит новую категорию цифровых прав – цифровые финансовые активы, а также определяет субъектов, посредством которых предполагается осуществление сделок с цифровыми финансовыми активами.

Учитывая, что законопроект находится в стадии доработки, прогноз состояния соответствия стандартам ФАТФ российского законодательства в части урегулирования надлежащим образом оборота виртуальных активов преждевременен.

В рамках текущей оценки системы противодействия отыманию доходов, полученных преступным путем, и финансированию терроризма указанные аспекты не оцениваются, что дает фору нашей стране в выстраивании системы мониторинга оборота виртуальных активов.

А.В. Иванов
И.В. Кондратьев

Противодействие финансированию терроризма через криптовалюты

Аннотация. Авторы исследуют проблемные вопросы финансированию терроризма через цифровые валюты — криптовалюту, создание и контроль за которой базируются на криптографических методах. Отмечается, что современный банковский сектор остается самым надежным местом для глобальных транзакций, и сама система остается уязвимой для финансирования терроризма. Делается вывод о сложности и неоднозначности рассматриваемой категории вопросов и проблем.

Ключевые слова: *к*риптовалюта, консенсусный реестр (ledger), биткойн «Crypto currency» (криптографическая валюта), форжинг или ICO, блокчейн, ZeroCash, Financial Action Task Force (ФАТФ).

Криптовалюта – разновидность цифровой валюты, создание и контроль за которой базируются на криптографических методах. Как правило, учёт криптовалют децентрализирован. Функционирование данных систем основано на таких технологиях, как блокчейн, направленный ациклический граф, консенсусный реестр (ledger) и др. Информация о транзакциях обычно не шифруется и доступна в открытом виде. Для обеспечения неизменности базы цепочки блоков транзакций используются элементы криптографии (цифровая подпись на основе системы с открытым ключом, последовательное хеширование) [1]. Термин закрепился после публикации статьи о системе Биткойн «Crypto currency» (Криптографическая валюта), опубликованной в 2011 году в журнале Forbes. Сам же автор и создатель биткойна, чья личность неизвестна, как и многие другие, использовал термин «электронная наличность» (англ. electronic cash).

Иногда новая криптовалюта появляется как ответвление (форк) от другой криптовалюты за счёт изменения параметров, что делает их несовместимыми. При этом обе криптовалюты могут иметь общую историю транзакций до момента их разделения.

Эмиссия разных криптовалют может происходить через майнинг, форжинг или ICO.

Об экономической сути и юридическом статусе криптовалют ведутся дискуссии. В разных странах криптовалюты рассматриваются как платёжное средство, специфичный товар, они могут иметь ограничения в обороте (например, запрет операций с ними для банковских учреждений). Ключевой особенностью криптовалют является отсутствие какого-либо внутреннего или внешнего администратора. Поэтому банки, налоговые, судебные и иные государственные или частные органы не могут воздействовать на транзакции каких-либо участников платёжной системы. Передача криптовалют необратима — никто не может отменить, заблокировать, оспорить или принудительно (без приватного ключа) совершить транзакцию. Однако участники сделки могут добровольно временно взаимно блокировать свои криптовалюты в качестве залога или установить, что для завершения/отмены сделки требуется согласие всех (или произвольных дополнительных) сторон [2].

Технология криптовалют исходит из того, что в сети нет доверенного узла – того, чьи действия гарантированно истинны и кто может подтвердить корректность чужих операций (задача византийских генералов). Впервые эта проблема была решена в системе «Биткойн» за счёт искусственного усложнения внесения изменений в реестр истории операций. Для хранения данных транзакции объединяются в блоки, из которых формируется непрерывная цепочка (блокчейн). Непрерывность обеспечивается не столько нумерацией, сколько включением в текущий блок хеш-суммы предыдущего блока, что не позволяет изменить информацию в блоке без изменения хешей во всех последующих блоках. Все хеши отвечают определённым требованиям, сгенерировать хеши, которые удо-

влетворяют этим требованиям, занимает много времени либо очень дорого. Истинной считается только самая длинная цепочка. В разных криптовалютах право сформировать очередной блок получает выполнивший определённую работу (Proof-of-work), имеющий некоторую сумму на счету (Proof-of-stake), предоставивший некоторые ресурсы (Proof-of-space) либо за основу берётся иная процедура, которую легко проверить, но сложно выполнить или подделать.

Как правило, в криптовалютах разработчики изначально оговаривают верхний предел общего объёма эмиссии. Однако у некоторых криптовалют, таких как PPCoin[en], Novacoin, Sifcoin и других, отсутствует фиксированный верхний предел общего объёма эмиссии и возможна как эмиссия, так и демиссия (путём обязательного уничтожения фиксированной суммы в каждой транзакции).

Большинство криптовалют обеспечивают псевдонимность – все транзакции между всеми адресами общедоступны, но нет данных о владельцах адресов. Однако личность владельца может быть установлена, если становится известна дополнительная информация. В ZeroCash изложена возможность заменить псевдонимность на анонимность.

После террористических атак в Париже в ноябре 2015 года правительства «удвоили усилия» в борьбе с терроризмом. Продолжается и борьба с финансированием терроризма, и возникает вопрос, может ли эта борьба затронуть криптовалюты? [3].

Фактически, регуляторы понимают, что криптовалюты не представляют интереса для террористов. Если вытеснить из мира цифровых валют законных игроков, то мы увидим только «маскировку» от правительств, которая скроет и законное, и незаконное использование криптовалюты. Среди политиков много «перестраховщиков». Но в то же время, среди политиков много таких людей, которые понимают – запретительные меры только вредят, вне зависимости от того, насколько громкими являются заголовки газет.

Роль криптовалют в финансировании терроризма может быть сильно преувеличена. Является ли биткоин в действительности валютой террористов? Такое мнение однозначно может сложиться после чтения некоторых крупных СМИ. Но недавнее исследование межправительственной организации ФАТФ по вопросам основных источников финансирования терроризма показывает совсем другую картину.

Financial Action Task Force (ФАТФ) – межправительственный орган, который разрабатывает новую системную политику, чтобы защитить глобальную финансовую систему от преступного отмывания денег, финансирования терроризма и создания оружия массового уничтожения. Недавно был опубликован их доклад "Новые террористические риски".

В докладе имеется небольшой раздел о цифровых валютах в качестве инструмента для возможного финансирования террористов. Однако в отчете говорится и о том, что иностранные террористические группы, в первую очередь, используют традиционные методы. Это частные пожертвования, самофинансирование и преступная деятельность по сбору средств. Статистика свидетельствует, что новые технологии оплаты представляют собой определенную уяз-

вимость, которая может увеличиваться с течением времени, но распространенность этих технологий среди террористических групп в настоящее время крайне мала [4].

Целью доклада является анализ недавно появившихся методов финансирования терроризма. В докладе утверждается, что понимание того, как террористы управляют активами, является ключом к ограничению их доступа к деньгам и разрушительно влияет их деятельность. Эксперты из глобальной сети ФАТФ, а также из правоохранительных органов, спецслужб и подразделений финансовой разведки принимали активное участие в подготовке этого доклада.

Террористические группы собирают деньги, как правило, для боевых операций, пропаганды, обучения и вербовки. Борьба с отмыванием денег и усилия по борьбе с финансированием терроризма подорвали способность этих организаций использовать некоторые традиционные методы сбора средств. Тем не менее, эти организации могут адаптироваться к определенным методам давления, поэтому власти должны продолжать контролировать использование террористами традиционных методов финансирования.

Виртуальные и цифровые валюты не упоминаются до последней части доклада.

Цифровые валюты привлекли террористов и преступников, потому что они предлагают анонимность транзакций и пользователей, скорость сделок, низкую волатильность и надежность, отмечается в докладе.

Правоохранительные органы заметили, что некоторые террористические вебсайты используют биткоины для приема пожертвований. Власти также обнаружили в онлайн-дискуссиях среди террористов, что те использовали виртуальную валюту для покупки оружия. Одно из подразделений ИГИЛ (ISIL) ранее предложило использовать Bitcoin для поддержки терроризма.

В докладе приводится недавний случай, когда подросток из Вирджинии Али Шукри Амина, который был арестован за использование Twitter для продвижения терроризма, инструктировал людей, как использовать Биткоин. У Амина в Twitter было более 4000 последователей [4].

При всей привлекательности криптовалют, другие технологии оплаты по рейтингу стоят гораздо выше в списке опасений ФАТФ. Одним из основных являются социальные сети. Доноры социальных сетей и площадок краудфандинга зачастую не знают конечного использования привлеченных средств. Такие кампании могут привлечь тысячи доноров. Террористические группы также используют другие платежные сети в качестве площадок для связи, в том числе мобильные приложения, чаты и форумы.

Растущее использование террористами онлайновых платежных систем также требует значительного внимания. Чтобы избежать обнаружения при использовании этих систем, террористам необходимо исказить регистрационную информацию [5].

Эксплуатация природных ресурсов для финансирования терроризма получает все большую популярность. Другие виды преступной деятельности, которые террористы используют для сбора средств, – контрабанда, незаконная добыча

полезных ископаемых, вымогательство и похищение с целью получения выкупа.

Террористические группы также проникают в некоммерческие организации, чтобы получить доступ к благотворительным средствам. Доклад ФАТФ от 2014 года о некоммерческих организациях исследовал нарушения в области глобального некоммерческого сектора. Благотворительные и некоммерческие организации, которые работают в зонах конфликтов, находятся в повышенной зоне риска проникновения террористических групп. Они также могут быть частью цепочки по переводу средств от законных коммерческих предприятий в террористические организации.

Другие незаконные действия по сбору средств включают мошенничество с кредитными картами, мошенничество с кредитами, страховое мошенничество, контрабанду, банковские ограбления, незаконный оборот наркотиков, налоговое мошенничество, вымогательство, похищение и выкуп.

В одном из разделов доклада рассматривается, как террористические группы переводят свои активы. Отмечается, что банковский сектор остается самым надежным местом для глобальных транзакций, и сама система остается уязвимой для финансирования терроризма. Меры по борьбе с отмыванием средств осложняют для террористов использование банковского сектора, тем не менее традиционные финансовые продукты по-прежнему могут быть использованы для финансирования террористической деятельности. Террористическая группа может открыть счет в банке и получить кредитные карты, чтобы позволить членам своей организации получить доступ к наличным через сеть банкоматов.

Таким образом, традиционные методы финансирования по-прежнему являются основными для террористических организаций, но необходимо контролировать социальные сети, а также отслеживать криптовалюты, предоставляющие анонимность при осуществлении своих транзакций.

Литература

1. Мащенко П. Л., Пилипенко М. О. Технология Блокчейн и ее практическое применение // Наука, техника, образование. — 2017. — № 32. — С. 61-64.
2. Хажиахметова Е. Ш. Криптовалюта — деньги XXI века // Новая наука: от идеи к результату. —2016. — № 11—2. — С. 177-179.
3. http://finglobal.ru/5840-Nekotorye-fakty-o-kriptovalyutah-i-finansirovanii-terrorizma.html
4. https://bits.media/rol-kriptovalyut-v-finansirovanii-terrorizma-silno-preuvelichena/
5. https://bitcointalk.org/index.php?topic=1221966.0

В.А. Кинсбурская

Правовые вопросы идентификации держателей криптовалюты в целях ПОД/ФТ и предотвращения уклонения от уплаты налогов[1]

Аннотация: Исследование направлено на изучение рисков использования криптовалюты в целях ПОД/ФТ и уклонения от уплаты налогов, а также определение допустимых методов противодействия указанным противоправным деяниям. Рассмотрены документы ФАТФ, касающиеся сферы виртуальных валют, зарубежный и отечественный опыт правового регулирования оборота криптовалют, в том числе российская правоприменительная практика по уголовным делам, связанным с использованием криптовалюты. В результате проведенного анализа сделан ряд предложений по внесению изменений в национальное законодательство, связанных с осуществлением финансового мониторинга и налогового контроля за операциями по с криптовалютой в России. Автор отстаивает мнение о необходимости лицензирования деятельности провайдеров услуг по обмену, переводу и хранению криптовалют, введении обязанности данных организаций по проведению проверки личности держателей криптовалют и отслеживанию совершаемых ими операций, а также указывает на допустимые способы сбора и подтверждения идентификационных данных держателей криптовалют и лиц, создающих криптовалюту (майнеров).

Ключевые слова: криптовалюта, отмывание доходов, финансирование терроризма, ФАТФ, «Знай своего клиента», лицензирование, идентификация, налогообложение криптовалюты, майнинг.

Обзор зарубежной и отечественной практики показывает, что частные (децентрализованные) криптовалюты активно используются при торговле наркотическими средствами, психотропными веществами, оружием, порнографическими материалами, иными запрещенными товарами, контентом и услугами, а также для отмывания доходов, полученных преступным путем, и финансирования терроризма[2]. Популярность криптовалют в преступной среде обусловлена тем, что до настоящего времени не определены юридические параметры криптовалюты и не установлены границы ее безопасного оборота. Кроме того, криминогенные свойства присущи главным техническим характеристикам частных криптовалют, таким как: относительно высокая степень анонимности для держателей криптовалют и совершаемых транзакций; низкие комиссионные; доступ из любой точки мира через Интернет; отсутствие ограничений по сумме денежных переводов; транснациональность криптовалюты (невозможность установления государственных и таможенных границ при проведении транзакций); необратимость транзакций; отсутствие единого руководящего лица, который может выступать в качестве «центральной точки контроля» в процессе вы-

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16145 мк «Механизм правового регулирования отношений с использованием технологии распределенных реестров».

[2] См., например: *Иванцов С. В., Сидоренко Э. Л., Спасенников Б. А., Берёзкин Ю. М., Суходолов Я. А.* Преступления, связанные с использованием криптовалюты: основные криминологические тенденции // Всероссийский криминологический журнал. 2019. Т. 13, № 1. С. 86–87.

пуска и обращения частных криптовалют и который может проинформировать уполномоченные государственные органы о совершении подозрительных операций, и др.[1]

В связи с этим ФАТФ в течение ряда лет проводит исследования, направленные на изучение реальных и потенциальных рисков совершения финансовых операций с использованием виртуальных валют (в том числе криптовалют) и определение способов предотвращения неправомерного использования виртуальных валют в целях ПОД/ФТ.

Одной из последних инициатив ФАТФ в данной сфере являются изменения, внесенные в октябре 2018 г. в Рекомендацию 15 и Глоссарий, разъясняющие, каким образом эти документы применяются в случае финансовой деятельности с использованием виртуальных активов[2].

22 февраля 2019 г. ФАТФ опубликовала предварительную версию требований для представителей криптовалютной отрасли, которые рекомендуется внедрить в своих юрисдикциях странам-участницам[3]. ФАТФ планирует выпуск Пояснительной записки к новой редакции Рекомендации 15, конкретизирующей исполнение стандартов ПОД/ФТ при осуществлении финансовой деятельности с использованием виртуальных активов. Предполагается, что провайдеры услуг в сфере виртуальных активов должны пройти регистрацию или получить лицензию в юрисдикциях, резидентом которой они являются; в целях осуществления финансового мониторинга собирать и хранить данные об отправителях и получателях криптовалютных платеже, а также направлять эти данные в уполномоченные государственные органы по их требованию (если транзакция будет признана подозрительной, регулятор должен принять меры для ограничения возможностей ее осуществления). Надзор за провайдерами услуг в криптовалютной отрасли должны осуществлять государственные органы, а не саморегулируемые организации (которые часто неспособны эффективно противостоять рискам ОД/ФТ), при этом надзорные органы должны иметь полномочия налагать санкции, включая право отзыва, ограничения или приостановления действия лицензии или регистрации провайдера услуг в криптовалютной отрасли.

Указанные требования ФАТФ в основных чертах отражают сложившиеся к настоящему моменту модели правового регулирования криптовалютной отрасли, принятые в целях финансового мониторинга в ряде зарубежных стран (Германия, Швейцария, Франция, США, Канада, Южная Корея и др.).

В России, несмотря на отсутствие законодательного регулирования, при совершении преступлений с использованием криптовалют правоохранительные

---

[1] См.: *Бондаренко Д. Д.* Виртуальные валюты: сущность и борьба с их использованием в преступных целях (на примере США) // Международное уголовное право и международная юстиция. 2015. № 6. С. 24.

[2] См.: Внесение изменений в стандарты ФАТФ и заявление ФАТФ по виртуальным активам (2018 г.). URL: http://fedsfm.ru/documents/international-fatf (дата обращения: 20.05.2019).

[3] Public Statement – Mitigating Risks from Virtual Assets. Paris, France, 22 February 2019. URL: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets-interpretive-note.html (дата обращения: 20.05.2019).

органы, по сути, приравнивают криптовалюты к имуществу и идентифицируют их в денежном эквиваленте. При этом действия, связанные с использованием криптовалюты для отмывания преступных доходов, должны подпадать под регулирование статей 174 и 174.1 Уголовного кодекса Российской Федерации[1] (далее – УК РФ). 26 февраля 2019 г. Верховный Суд РФ признал криптовалюту одним из средств отмывания денег. Согласно новой редакции Постановления Пленума Верховного Суда РФ от 07.07.2015 № 32 «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем»[2], предметом преступлений, предусмотренных статьями 174 и 174.1 УК РФ, могут выступать, в том числе, денежные средства, преобразованные из виртуальных активов (криптовалюты), приобретенных в результате совершения преступления. Позиция Пленума Верховного Суда РФ, безусловно, будет способствовать формированию единообразной практики по соответствующим уголовным делам с использованием криптовалюты, но не повлияет на регулирование криптовалюты вне уголовно-правового поля.

Для минимизации случаев криминального использования криптовалют необходимы разрешительный порядок деятельности провайдеров услуг в криптовалютной отрасли, учет лиц, осуществляющих операции по созданию и использованию криптовалют, в органах финансового мониторинга и налогового контроля, и работающий механизм отслеживания операций с криптовалютой.

На основании требований ФАТФ, а также с учетом принципиальной позиции Росфинмониторинга и ФСБ России о необходимости разработки процедур идентификации держателей криптовалюты в целях выявления лиц, занимающихся отмыванием денег, финансированием терроризма и финансированием распространения оружия массового уничтожения[3], в проект федерального закона № 419059-7 «О цифровых финансовых активах»[4] (далее – законопроект «О цифровых финансовых активах») ко второму чтению должны быть внесены поправки, предусматривающие обязательность прохождения идентификации для получения права осуществления операций с цифровыми финансовыми активами. Предполагается, что без идентификации клиенты не смогут переводить деньги со своих счетов в российских банках в цифровые финансовые активы,

[1] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (в ред. от 23.04.2019) // СЗ РФ. 1996. № 25. Ст. 2954.

[2] Постановление Пленума Верховного Суда РФ от 07.07.2015 № 32 «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем» (в ред. Постановления Пленума Верховного Суда РФ от 26.02.2019 № 1) // Российская газета. 2015, 13 июля.

[3] ФСБ представила Госдуме замечания к законопроекту о цифровых финансовых активах // ТАСС, 18.03.2019. URL: https://tass.ru/ekonomika/6229429 (дата обращения: 20.05.2019).

[4] Проект федерального закона № 419059-7 «О цифровых финансовых активах» (17.05.2018 принят в первом чтении). URL: https://sozd.duma.gov.ru/bill/419059-7 (дата обращения: 20.05.2019).

частности, в криптовалюты (суммовой порог, с которого начнется обязательный контроль, будет установлен дополнительно)[1].

Принимая во внимание изложенное, целесообразным видится внесение следующих изменений в действующее законодательство.

1. Организации, осуществляющие услуги по обмену, переводу и хранению криптовалют, должны подлежать лицензированию (получать специальное разрешение от Банка России), и сведения о таких организациях должны быть включены в государственный реестр, ведение которого может осуществлять Банк России. Организации, уже имеющие лицензии на осуществление иных видов финансовой деятельности, также должны получать специальную лицензию на осуществление операций с криптовалютой.

2. В Федеральном законе от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»[2] (далее – Закон № 115-ФЗ) следует установить обязанность организаций, осуществляющих услуги по обмену, переводу и хранению криптовалют, проводить комплексную проверку личности клиентов, осуществляющих операции с криптовалютами. До начала работы на криптобирже (при регистрации аккаунта и открытии криптокошелька) личность клиента должна быть идентифицирована путем использования сведений из разных источников. Так, необходимо выявлять IP-адрес клиента; запрашивать у него данные документа, удостоверяющего личность, и проводить перепроверку полученных идентификационных данных путем использования общедоступных электронных государственных сервисов (например, сервиса проверки паспортов на сайте Главного управления по вопросам миграции МВД России); осуществлять в сети «Интернет» поиск дополнительной информации, подтверждающей, что деятельность клиента и его деловая репутация соответствуют характеру проводимых им операций с криптовалютами (с учетом соблюдения требований законодательства о персональных данных[3]).

3. В Законе № 115-ФЗ следует установить суммовой порог, с которого будет начинаться обязательный контроль криптовалютных операций в целях ПОД/ФТ. Все криптовалютные операции, превышающие указанный суммовой порог, должны быть «прослеживаемыми»: информация о личности плательщика и получателя, сумме операции, дате и времени ее совершения должна храниться в архивной базе данных организации, осуществляющей операции с криптовалютой, не менее пяти лет и быть доступной органам финансового мониторинга и налогового контроля (по их требованию). В случае наличия у организации, осуществляющей операции с криптовалютой, обоснованных подозре-

---

[1] Предъявите ваш токен: владельцев криптовалют будут идентифицировать // Известия, 07.03.2019. URL: https://iz.ru/853019/dmitrii-grinkevich/prediavite-vash-token-vladeltcev-kriptovaliut-budut-identifitcirovat (дата обращения: 20.05.2019)

[2] Федеральный закон от 07.08.2001 № 115-ФЗ (ред. от 18.03.2019) «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» // Российская газета. 2001. 9 авг.

[3] Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 31.12.2017) «О персональных данных» // Российская газета. 2006, 29 июля.

ний в том, что конкретная операция совершается в целях ОД/ФТ, информация об этом должна быть направлена в Росфинмониторинг.

В мировом масштабе существуют примеры регулирования, при котором используется многоуровневая система проверки в зависимости от услуги, необходимой клиенту. Так, правила компании «Kraken» (одной из старейших и самых популярных в мире криптовалютных обменных платформ, основанной в 2011 г. в Сан-Франциско), предусматривают пять различных по «глубине» уровней проверки, от которых зависят торговые лимиты клиента. Для предоставления возможности сдачи на хранение и снятия криптовалюты, а также торговли криптовалютами и фиатными валютами клиент должен указать свое полное имя, дату рождения, электронную почту, страну проживания и номер телефона; кроме того, клиент должен указать реквизиты своего банковского счета, с которого будут осуществляться переводы денежных средств (поскольку банковские и электронные переводы являются единственными доступными способами для внесения средств на платформе «Kraken»). Для получения услуг валютного финансирования клиент должен загрузить официальные формы идентификации и доказательства проживания в стране; для резидентов США дополнительно требуется представить номер социального страхования, для резидентов Германии или Японии – удостоверение личности с фотографией. Максимальный уровень проверки предполагает предоставление подписанной формы заявки и документов, оформленных в соответствии с требованиями KYC («Знай своего клиента»)[1].

По нашему мнению, многоуровневая система проверки представляет собой достаточно эффективный механизм осуществления контроля за лицами, осуществляющими операции с криптовалютами, который (в той или иной мере) может быть реализован и в национальном правовом поле. Тем не менее очевидно, что основные риски неправомерного использования криптовалют возникают на этапе обмена криптовалюты на фиатные деньги. Именно в этот момент деятельность, связанная с криптовалютами, выходит из виртуального пространства и пересекается с регулируемой финансовой системой, где используются обычные денежные средства. С точки зрения ПОД/ФТ в момент обмена криптовалют на фиатные деньги (и последующего зачисления соответствующей суммы на счет злоумышленника в безналичной форме либо снятия этой суммы наличными) можно признать оконченными преступления, предусмотренные статьями 174 и 174.1 УК РФ. Поэтому представляется, что именно в процессе обмена криптовалют на фиатные деньги должен осуществляться наиболее жесткий контроль как со стороны организаций, осуществляющих операции по обмену, переводу и хранению криптовалют, так и со стороны уполномоченных государственных органов.

4. При определении налоговых последствий операций, совершаемых с криптовалютой, момент обмена криптовалют на фиатные деньги также имеет особое значение. С точки зрения экономической сущности налогообложения лишь в

[1] См.: Обзор биржи «Kraken». URL: https://minings.ru/obzor-birzhi-kraken/ (дата обращения: 20.05.2019).

этот момент у криптомонеты возникает та реальная стоимость, которую можно подсчитать и обложить соответствующим налогом. В связи с этим, по нашему мнению, для целей прямого налогообложения доход следует признавать только в момент обмена криптовалюты на фиатные деньги.

Кроме того, при рассмотрении налоговых последствий криптообменных операций следует учитывать, что введение в национальное противолегализационное законодательство требований об идентификации держателей криптовалюты и «прослеживаемости» криптовалютных операций неминуемо повлечет «перетекание» значительной части криптотрейдеров в зарубежные юрисдикции, в которых пока действует более льготное правовое регулирование. В таких условиях более «жизнеспособным» (во всяком случае, на начальном этапе функционирования криптовалютной отрасли в России) видится вариант, при котором операции, совершаемые в блокчейне, в том числе операции по обмену одной криптовалюты на другую, будут освобождены от налогообложения (либо установлено льготное налогообложение).

5. При рассмотрении налоговых последствий операций по созданию криптомонет надо исходить из того, что в текущей редакции законопроекта «О цифровых финансовых активах» вопросы майнинга не отражены и, по всей видимости, специальным образом они регулироваться не будут. В отсутствие законодательного регулирования доход, полученный от майнинга, допустимо на общих основаниях облагать НДФЛ или налогом на прибыль организаций (в зависимости от надлежащего субъекта налогообложения). Однако возникают два серьезных вопроса, связанных с налоговым администрированием: механизм выявления налогообязанных лиц и порядок расчета налоговой базы.

При решении первого из указанных вопросов следует учитывать, что с технической точки зрения факт установки майнерского оборудования в конкретном помещении можно выявить по объемам потребляемой электроэнергии и структуре электропотоков, приходящихся на данное помещение. Обязанность по осуществлению такого мониторинга и предоставлению в налоговые органы сведений о предполагаемых майнерах теоретически можно было бы возложить на компании, являющиеся поставщиками электроэнергии на территории соответствующих субъектов Российской Федерации. Тем не менее сначала необходимо просчитать процент эффективности деятельности, связанной с выявлением потенциальных майнеров, принимая во внимание, в частности, возможные материальные, трудовые и временные затраты энергосбытовых компаний по осуществлению предварительного и текущего мониторинга и налоговых органов – по осуществлению последующего контроля за потенциальными майнерами. Возможно, с экономической и правовой точек зрения более оправданным вариантом является официальное признание майнинга предпринимательской деятельностью, в частности, введение обязанности физических лиц – майнеров регистрироваться в качестве индивидуальных предпринимателей.

При решении второго вопроса следует учитывать, что в отличие от обычных денег (национальных валют), курс которых в принципе без особых проблем устанавливается заранее на день вперед, курсы криптовалют могут многократно (причем резко) меняться в течение дня. В связи с этим относительно целесо-

образной видится идея об установлении налога на вмененный доход от майнинговой деятельности (по аналогии со специальным налоговым режимом, предусмотренным главой 26.3 Налогового кодекса Российской Федерации[1]). Субъектами этого налога могут быть физические и юридические лица, осуществляющие создание криптомонет (майнинг). В качестве объекта налога можно рассматривать вмененный доход лица, полученный от создания криптомонет, рассчитываемый, в частности, с учетом таких параметров, как: награда за создание блока; период времени майнинга, выраженный в секундах; вычислительная мощность техники, выражаемая в хэшах в секунду (hash/s); сложность майнинга. Безусловно, такой налоговый режим в состоянии частично нивелировать проблему расчета налоговой базы в условиях волатильности курсов частных криптовалют. Но, с другой стороны, именно по причине волатильности курсов криптовалют размер вмененного дохода может весьма сильно отличаться от реального дохода лица (что, очевидно, не отвечает принципу справедливости налогообложения). В связи с этим, как и в случае определения механизма выявления майнеров, при установлении налога на вмененный доход от майнинговой деятельности необходимо просчитать процент эффективности.

Литература

1. Отчет ФАТФ «Виртуальные валюты – ключевые определения и потенциальные риски в сфере ПОД/ФТ» (2014 г.). URL: http://www.fedsfm.ru/content/files/documents/fatf/virtualnye_valyuty_fatf_2014.pdf (дата обращения: 20.05.2019).
2. Руководство ФАТФ по применению риск-ориентированного подхода для провайдеров услуг по обмену конвертируемой виртуальной валюты (2015 г.). URL: http://www.fedsfm.ru/content/files/documents/fatf/rop_virtualnye_valyuty.pdf (дата обращения: 20.05.2019).
3. Внесение изменений в стандарты ФАТФ и заявление ФАТФ по виртуальным активам (2018 г.). URL: http://fedsfm.ru/documents/international-fatf (дата обращения: 20.05.2019).
4. Public Statement – Mitigating Risks from Virtual Assets. Paris, France, 22 February 2019. URL: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets-interpretive-note.html (дата обращения: 20.05.2019).
5. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (в ред. от 23.04.2019) // СЗ РФ. 1996. № 25. Ст. 2954.
6. Налоговый кодекс Российской Федерации (часть вторая) от 05.08.2000 № 117-ФЗ (ред. от 01.05.2019) // СЗ РФ. 2000. № 32. Ст. 3340.
7. Федеральный закон от 07.08.2001 № 115-ФЗ (ред. от 18.03.2019) «О противодействии легализации (отмыванию) доходов, полученных пре-

[1] Налоговый кодекс Российской Федерации (часть вторая) от 05.08.2000 № 117-ФЗ (ред. от 01.05.2019) // СЗ РФ. 2000. № 32. Ст. 3340.

ступным путем, и финансированию терроризма» // Российская газета. 2001. 9 авг.
8. Постановление Пленума Верховного Суда РФ от 07.07.2015 № 32 «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем» (в ред. Постановления Пленума Верховного Суда РФ от 26.02.2019 № 1) // Российская газета. 2015, 13 июля.
9. Проект федерального закона № 419059-7 «О цифровых финансовых активах» (17.05.2018 принят в первом чтении). URL: https://sozd.duma.gov.ru/bill/419059-7 (дата обращения: 20.05.2019).
10. *Батоев В. Б., Семенчук В. В.* Использование криптовалюты в преступной деятельности: проблемы противодействия // Труды Академии управления МВД России. 2012. № 2 (42). С. 9–15.
11. *Бондаренко Д. Д.* Виртуальные валюты: сущность и борьба с их использованием в преступных целях (на примере США) // Международное уголовное право и международная юстиция. 2015. № 6. С. 23–25.
12. Евразийская экономическая комиссия. Регулирование криптовалют: исследование опыта разных стран. Декабрь 2017 г. URL: http://www.eurasiancommission.org/ru/act/dmi/workgroup/Documents/digest/Регулирование%20криптовалют%20в%20странах%20мира.pdf (дата обращения: 20.05.2019).
13. *Иванцов С. В., Сидоренко Э. Л., Спасенников Б. А., Берёзкин Ю. М., Суходолов Я. А.* Преступления, связанные с использованием криптовалюты: основные криминологические тенденции // Всероссийский криминологический журнал. 2019. Т. 13, № 1. С. 85–93.
14. Предъявите ваш токен: владельцев криптовалют будут идентифицировать // Известия, 07.03.2019. URL: https://iz.ru/853019/dmitrii-grinkevich/prediavite-vash-token-vladeltcev-kriptovaliut-budut-identifitcirovat (дата обращения: 20.05.2019).
15. ФСБ представила Госдуме замечания к законопроекту о цифровых финансовых активах // ТАСС, 18.03.2019. URL: https://tass.ru/ekonomika/6229429 (дата обращения: 20.05.2019).

А.Н. Кирков
Научный руководитель:
Денчев Стоян Георгиев, проф. д.э.н.

Проблемы перед экспертизой электронных денежных средств и криптовалюты

Аннотация. В статье рассматриваются препятствия при подготовке технической экспертизы по криптовалютам в досудебных и судебных делах в Болгарии.

Ключевые слова: экспертиза, криптовалют, электронных денежных средств.

Введение

На практике электронные денежные средства появляются в начале 90-х годов XX века. На данный момент это реально третье поколение. Законодательство об электронных денежных средствах существует в большинстве стран мира, и они все равно до сих пор незнакомы.

В 1997 году была выпущена первая успешная международная цифровая валюта – e-Gold. В 1999 году она уже имеет огромный успех и через нее прошли миллиарды долларов.

В 2004 году из-за отсутствия регулирования e-Gold использована при множестве преступлений и против нее велись множество дел, и на практике она действовала до 2006 года, когда руководство компании потребовало, чтобы государственный регулятор в США эту цифровую валюту больше не рассматривал как валюту.

Фактически, в период с 2001 по 2004 годов команда e-Gold установила основные правила работы с электронными валютами, которые действуют и сегодня.

Приблизительно 10 лет назад, когда мои коллеги рассказали мне о новом цифровом чуде – биткойне (Bitcoin), я все еще помнил урок e-Gold и был настроен скептически. Тогда были в моде преступления с банковскими карточками, которые наносили ущерб в миллиарды, и тогда я сосредоточил свое внимание именно на эти преступления.

В настоящее время в мире насчитывается 2119 видов криптовалют, которые распространены более чем в одной стране.

Мы уже в XXI веке, и с криминалистической точки зрения мы не можем проигнорировать цифровую криптовалюту, так как мы будем все чаще сталкиваться с ними.

За последние два года в Болгарии было несколько случаев, когда преступники использовали криптовалюту для укрытия сумм или совершения преступлений, как «кражи криптовалюты».

За неделю до моего приезда в Москву я закончил экспертизу другого международного дела о незаконном приобретении криптовалюты.

Поэтому я хотел бы поделиться своим опытом с проблемой исследование криптовалюты.

Для начала нам нужно знать, что у нас есть два разных типа цифровых денежных средств, а именно:

- Электронные деньги, это электронные платежные инструменты, выпущенные уполномоченный или государственный органами. Такими являются: Крипторубль – вероятно вам известно, что Россия была одной из первых стран, создавших электронную валюту, Ekrona - электронная валюта, выпущенная под контролем шведского государства, и так далее.

- Виртуальные валюты — это термин, который Европейская комиссия официально ввела в 2018 году, чтобы заполнить пробел в европейском законодательстве о криптовалютах, который не выданных уполномоченной организацией.

Виртуальные валюты в действующем законодательстве

Пока с электронными деньгами все ясно и независимо от принципа их работы они юридически приведены в соответствие с обычными валютами, то на практике во многих странах не существует правовых норм по отношению к криптовалютам, то есть, согласно законодательству, они не могут быть платежным инструментом и на них не действует материальный закон, но они все еще существуют и с ими проводятся реальные действия.

С этой целью Европейское банковское управление (EBA) дало определение, согласно которому: виртуальная валюта является видом нерегулируемых цифровых денег, которые не выпускаются и не гарантируются центральным банком, но которые могут выступать в качестве платежного средства. Виртуальные валюты могут иметь различные формы.

Это слишком общее определение все еще предназначено для того, чтобы дать юридическое определение, оно использовалось в Директиве ЕС 2018/843, которая открывает двери, но пока не существует применимого законодательства.

По понятным причинам из государственных органов в Болгарии и некоторые страны в Европейском союзе, самыми быстрыми новаторами в этой области стала Налоговая администрация, которые сразу же дали толкование, независимо что виртуальные валюты являются легально или нелегальном средством расплатитья, они облагаются налогом.

На самом деле, технологии виртуальных валют стремительно развиваются, и уже ясно, что они являются частью нашего настоящего и будущего. Они все чаще присутствуют в делах, и поэтому мы не можем их игнорировать, тем более что во многих случаях отслеживание денежных потоков обеспечивает ясность расследовании, в то время как при виртуальных валютах это не всегда возможно.

Сходства и различия с обычными валютами

Поскольку электронные деньги подробно описаны в законах или в других актах, я хотел бы обратить внимание на виртуальные валюты, о которых мы все еще мало знаем.

На самом деле, виртуальные валюты в значительной степени соответствуют принципам обычных валют и банковских операций, а именно:

1. Виртуальные валюты имеют фиксированное количество денежных знаков, то у них есть конечное количество, которое не меняется.
2. Каждый денежный знак имеет цифровую идентификацию, будь то порядковый номер или сложный код.
3. Виртуальные валюты содержат цифровые счета, похожие на банковские счета, которые называются адресами.
4. Виртуальные валюты отслеживаются, и любой платеж или перевод денежных средств, можно отслеживать из какого счета и на какой счет он отправлен.
5. Виртуальные валюты используются через электронные портфели, которые по своей природе аналогичны программам Интернет-банкинга.

Конечно, счета часто являются анонимными, но по количеству транзакций можно легко определить, является ли владелец счета обменником (обменным бюро) или обычным пользователем.

Многие полицейские и специальные агентства по всему миру уже пытаются идентифицировать владельцев счетов виртуальной валюты и, в меньшей степени, создают базы данных со своими уже известными владельцами, такие программы уже продаются, и через них общая картина заполняется и уточняется.

Виртуальных валют не имеет материальное обеспечение, поэтому их курсы обмена с другими валютами определяются только рыночным спросом.

Самой популярной и распространенной виртуальной валютой является биткойн, а самым популярным алгоритмом распространения является блокчейн (blockchain).

Биткойн запущен в 1998 году и использует онлайн-систему учета для поддержки отдельных учетных записей. Он работает по принципу полностью децентрализованной сети и не находится под контролем учреждения.

Биткойн можно получить двумя способами: путем добывания, т.е. когда компьютер подключен к их сети, он работает как сервер и поддерживает так называемую систему учета биткойна. Единицы платежа биткойн создаются в качестве вознаграждения за проделанную вычислительную работу, или второй способ является его покупка.

Стоимость биткойнов зависит от их рейтинга по отношению к другим валютам и меняется очень динамично.

По состоянию на 2014 год насчитывается более 12 миллионов биткойнов, причем их общее количество постоянно растет, но их максимальное количество не может превышать 21 миллион. Это их технологический предел.

Публичный регистр транзакций (так называемый «публичный реестр» на английском: public ledger), представляет собой публичный список всех выполненных транзакций и реализован в виде цепочки блоков (blockchain). Данные баланса для каждой учетной записи записываются в файл на всех компьютерах, участвующих в Биткойн сети. Это позволяет каждому пользователю проверять достоверность каждой транзакции и просматривать всю историю с самого начала сети. Криптографические методы используются для функционирования и защиты платежной системы, а подлинность всех транзакций защищена цифровыми сертификатами. Реестр хранит учет в партнерской сети каждые 10 минут. Транзакция обычно считается подтвержденной после шести подтвержденных регистраций (требуя около часа).

Все транзакции с биткоинов являются открытыми и регистрируются. Это означает, что каждый член сети может видеть баланс и транзакции, выполняемые каждым адресом (счет) биткойна.

Возможности об доказательства

Что мы можем узнать при расследовании сделки с биткойнами или разработке судебно-технической экспертизы:

Поиск программного обеспечения для управления криптовалюты: Лица, использующие криптовалюту, в основном устанавливают программное обеспече-

ние электронного кошелька на свои компьютеры или телефоны. Это помогает легко управлять биткойнами, без технических знаний о протоколе биткойна.

Через кошельки пользователи могут отправлять и получать биткойны в электронном виде на своем персональном компьютере, мобильном устройстве или веб-приложении.

Кошелек хранит ссылки на криптографические пароли или «закрытые ключи», которые обеспечивают доступ к балансам и трансфер биткойнов, и могут содержать несколько учетных записей. Каждый кошелек получает индивидуальный код, представляющий собой длинную последовательность цифр и букв (обычно около 33 символов), которая при биткоин всегда начинается с 1 или 3.

Отслеживание транзакций: личность пользователя, который использует биткойн адрес или кошелек, остается неизвестной для сети Биткойн, пока пользователь не связывает свое имя с его / ее адресом публично в Интернете.

Однако возможно при «подслушвании» соединения устройства, на котором установлено программное обеспечение биткойна, в Интернете, чтобы отследить, по какому IP-адресу инициируется транзакция, и прочитать всю информацию о транзакции. Также IP адреса могут быть получены от Интернет-провайдера, и можно сравнить с найденными в экс-чейнджер адресов. Экс-чейнджеры хранят личные данные своих пользователей, а также IP адресов, которые они используют, и так по этим адресам можно идентифицировать пользователей валюты.

Другой метод: поиск пароля к кошельку: Пароли для электронные портфели часто сохраняют на бумаге, потому что они длинные и трудны для запоминания или используют знакомые и распространенные пароли. При тщательном рассмотрении вещественных доказательств часто можно найти записные книжки или специальные файлы, содержащие список паролей. Взломать пароль с помощью специального программного обеспечения возможно, но это занимает много времени и зачастую экономически невыгодно.

Другой метод - анализ информации с нескольких экс-чейнджеров, с которым подозреваемый имел сделки для криптовалют. Может быть запрошена информация с экс-чейнджеров для определения того, кто совершает сделки с криптовалютами. экс-ченджеры помогают следственным органам, потому что их деятельность связана с обменом валют, а не с укрытием сумм.

Хардуерные кошельки: также при получении вещественных доказательств важно знать, что уже существуют устройства подобные флэш-накопителям, которые хранят криптовалюту. Они называются хардуер или колд леджер (холодный кошелек) и предназначены для защиты криптовалюты, находящейся в кошельке.

Заключение

Видимо криптовалюта будет развиваться и в будущем. Вероятно, их число будет уменьшено, но они будут продолжать присутствовать в нашей повседневной жизни, и их все чаще придется исследовать.

Без регулирования очень трудно установить важную информацию для расследования, так как большинство криптовалют являются анонимными и хоро-

шо защищены. На данном этапе способы изучения криптовалют предоставляют в основном косвенные доказательства действий обвиняемых. Пока не будет введено обязательство, предоставлять информацию, потребуется много усилий, чтобы понять используемые технологии и найти способы их изучения. Это одно из главных препятствия не только для экспертов, но и для государственные учреждения в современном мире.

Литература

1. A Forensic Look at Bitcoin Cryptocurrency, SANS, USA, 2015;
2. Относно правния режим на виртуалните валути и борбата с прането на пари в Република България, Ю. Матеева, Г. Ковачева, ВСУ „Черноризец Храбър”, България.
3. 10-те криптовалути с най-голяма пазарна капитализация, forexnews.bg, 2017, България
4. Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto, USA

М.А. Моисеенко

Правовое регулирование налогообложений операций с криптовалютой в зарубежных странах

Аннотация. В статье рассматриваются проблемы правового регулирования налогообложения операций с криптовалютой на основе зарубежного опыта.

Анализируется объекты налога на операции с криптовалютами, виды деятельности в данной сфере, доходы от которых подлежат налогообложению.

Ключевые слова: биткойн, блокчейн, криптовалюта, налогообложение, зарубежные страны, фьючерсы, транзакции.

Развитие современных цифровых технологий оказывает во всем мире непосредственное влияние как на специфику современной предпринимательской деятельности, так и на налогообложение. Появление новой технологии децентрализованного хранения данных о транзакциях – блокчейн, созданной для обеспечения операций с криптовалютой Биткойн привела к появлению новых видов деятельности и активов, характеризующимися потенциальной возможностью являться объектами налогообложения.

Несмотря на то, что создатели Биткойна строили такую альтернативную платформу, которую было бы трудно монетизировать, зарубежные страны задумываются над тем какие преимущества для экономики даст блокчейн технология, как это отразится на экономике и насколько серьезной проблемой это является сейчас. Очевидно, что сочетание технологии и экономики несомненно создает проблемы правовой определенности блокчейна, включая вопросы налогообложения.

Потенциал использования блокчейна значительно шире возможностей, которые мировые финансовые системы могут обеспечивать сегодня. С одной сторо-

ны, очевидно, что в корпоративном мире по существу отсутствует доверие (что и привело к созданию криптовалют и блокчейна), и второе – технология развивается стремительно, и вероятно блокчейн скоро перейдет из частного в общественное достояние. Способ блокчейна заключается в том, что после того, как транзакция размещена в интернете, майнеры могут проверить перевод средств, создавая «цепочку», которая затем делает каждый «блок цепочки» безопасным. Таким образом, использование блокчейна может обеспечить больше прозрачности сторонам сделки, которые концептуально не доверяют друг другу. Поскольку криптовалюты находятся в цифровом формате, который использует методы шифрования данные трансакции остаются закрытыми[1].

В использовании новой технологии блокчейна заинтересованы финансовые институты, банки. Например сделка между S7 Airlines и Альфа-банком стала первым смарт-контрактом в Российской Федерации, связанным с блокчейном.

Принципы работы смарт-контрактов предлагается применять и к трудовой деятельности, т.к. эта автоматическая система позволит упростить контроль работодателя за работником и осуществлять оплату труда работников криптовалютой[2].

Более того блокчейн может революционизировать процесс исчисления налога на операции с трансакциями к которым каждый, включая органы налогового администрирования, налогоплательщиков может иметь прямой доступ.

Право любого государства установления и введения налогов, включая налоги на операции с криптовалютой и финансовые результаты деятельности является юридически не ограниченным, однако его реализация должна соответствовать принципам международного сотрудничества в сфере налогообложения и налоговой политике государства.

Существенное значение имеет применение соответствующих средств юридической техники при определении юридической конструкции налога, элементы которой необходимо законодательно определить. Речь идет в данном случае о применении норм п.1 ст.17 НК Российской Федерации, в соответствии с которыми, налог считается установленным лишь в том случае, когда определены налогоплательщики (конкретные лиц, которые с правовой точки зрения могут рассматриваться, например, как эмитенты криптовалют) и обязательные элементы налогообложения. Поскольку выпуск цифровых денег происходит различными способами - ICO (первичное размещение монет, система инвестирования), майнинг (поддержание специальной платформы для создания новых криптоденег), forging (образование новых блоков в уже имеющихся криптовалютах)[3], прежде всего, необходимо выбрать объект (объекты) налогообложения, который возникает в результате действий субъекта налогового права. Законодателю необходимо определить юридический факт, который в соответ-

[1] Bridging the digital gap: How tax fits into cryptocurrencies and blockchain development. https://blog.nationalarchives.gov.uk/bridging-digital-gap/

[2] См.: Лескина Э.И. Применение блокчейн-технологий в сфере труда Лескина Э.И. // Юрист №11 2018. С. 29.

[3] См.: Александр Бычков, Транзакции с криптоактивами и их правовая защита // Новая бухгалтерия №04, 2018.

ствии с налоговым законом обуславливает обязанность по уплате соответствующего налога с учетом идентичности операции и местоположения проведенной операции. Кроме того, в законе о налоге определяется налоговая база, налоговый период, налоговая ставка, порядок исчисления и сроки уплаты налога.

В данном случае юридическая конструкция налога законодательно формализует пространственно-временные, физические, стоимостные, фактические и иные характеристики обстоятельств и предметов материального мира, а также порядок исчисления, документальной фиксации и внесения лицом конкретной суммы налога[1].

И второй важный вопрос, вытекающий из установления налога, связан осуществлением налогового контроля. Ведь для определения налогооблагаемой базы информацию и данные, записанные на частном блокчейне, будет необходимо учитывать в налоговые регистры в соответствии с требованиями налогового законодательства.

В разных странах мира, несмотря на достаточно широкое использование Биткойна и иных криптовалют правовое регулирование, включая вопросы налогообложения регулирование различно (см. Таблица).

Зарубежное законодательство в сфере налогообложения криптовалютных сделок[2].

Таблица

Страна	**Законодательство**	**Налогообложение**
Австралия	Специального нормативного регулировании криптовалют нет. Криптовалюта рассматривается как один из возможных способов для осуществления расчетов	К операциям с криптовалютой применяются стандартные правила налогообложения (налог на прибыль предприятий и подоходный налог), за вычетом налога на добавленную стоимость
Аргентина	В соответствии с законодательством криптовалюта не является национальной валютой, но может рассматриваться как деньги	Операции с криптовалютой облагаются существующими налогами в зависимости от вида операции с ней
Беларусь	Декрет «О развитии цифровой экономики»	Налогообложение операций с криптовалютами, майнинга
Болгария	Криптовалюты приравнены к «гибридным валютным средствам»	Облагаются налогами в соответствии общим принципам налогообложения, если они используются как валюта и при обменных операциях с/на фиатные деньги
Великобритания	Криптовалюты рассматриваются как «частные деньги». HMRC, с точки зрения налогообложения, не расценивает	Налог на крипто-капитал: любой доход, вырученный с криптовалюты, подлежит

[1] См. подроб.: *О. Ногина* К вопросу об элементном составе налога // Финансовое право. 2005. №7.

[2] https://lawstrust.com/ico/pravovoj-status-kriptovalyut/crypto-friendly, https://bits.media/pozitsiya-stran-mira-po-regulirovaniyu-kriptovalyut-na-fevral-2018-goda/

	крипто-активы как валюту, и разделяет их на три категории «токенов»: разменные (exchange tokens), продуктовые (utility tokens) и токены со статусом ценных бумаг (security tokens). Обложение налогами «разменных токенов» – термин охватывает такие активы, как Bitcoin, в целом, подход очень похож на подход IRS. HMRC рассматривает крипто-активы как часть личных инвестиций	налогообложению по налогу на капитал (CGT) в размере 20% от общего размера вырученного дохода. Учет виртуальных активов: при использовании remittance basis в качестве вида налоогобложения, обязанность по уплате налога на капитал (CGT) определяется исходя из места нахождения актива
Германия	С декабря 2013 года Федеральное управление финансового надзора рассматривает Биткоин в частности (и некоторые другие криптовалюты в целом) как единицу расчётов, легальными остаются только операции между физическими лицами	Применение правил налогообложения для «частных денег»
ЕС	Суд ЕС отнес криптовалюту к «контрактным» средствам платежа (contractual means of payment), используемым только при соглашении сторон сделки.	Согласно директиве «Об общей системе налога на добавленную стоимость» не подлежат обложению операции с законными средствами платежа
Израиль	Криптовалюта рассматривается как актив для целей бухгалтерского учета	Уплачиваются налоги на прирост капитала и НДС
Испания	Добытчики криптовалюты (майнеров) проходят особую процедуру регистрации. С 2014 г. криптовалюта относится к электронным средствам платежа	К операциям с криптовалютой применяются стандартные правила налогообложения
Китай	Операции связанные с обменом Биткоинами и др. криптовалютами незаконные. Отсутствует прямой запрет на криптовалютные операции	-
США	Лицензируемый вид деятельности	С 01.01. 2018 г. все операции с криптовалютами облагаются налогом
Япония	Биткойн приравнен к ценности подобной активами[1], законное средство обмена	Отменен налог с продаж Биткойна и другой криптовалюты

Как видно из данных, приведенных в Таблице, в зарубежных странах в основном применяется налогообложение к доходам, полученным в результате операций с криптовалютой, если она используются как валюта и при обменных операциях с/на фиатные деньги. Например, в США в зависимости от юрисдик-

[1] По определению ФАТФ: виртуальные активы – это цифровое выражение ценности, которое может цифровым образом обращаться или переводится и может быть использовано для целей платежа или инвестиций

ции трансакции с криптовалютой могли считаться биржевым товаром[1], валютой[2] или токеном вознаграждения. Однако с 1 января 2018 г. в США все сделки с криптовалютами облагаются налогом в момент из совершения. Служба внутренних доходов Великобритании IRS опубликовала руководство, в котором определила криптовалюту как собственность (property), операции с которой, в том числе майнинг, должны облагаться налогами. Таким образом, законодательство Великобритании регламентировало новый объект налогообложения - заработные платы, выплачиваемые работникам в криптовалюте, в таких налогах как федеральный подоходный налог (Federal Income Tax Withholding) и налог на заработную плату (Payroll Taxes). Кроме того, платежи за услуги контрагента по гражданско-правовому договору в криптовалюте также облагаются налогами. Информация о платежах в криптовалюте должна подаваться в соответствующие органы, а доходы, полученные физическим лицом в криптовалюте, и другие объекты налогообложения должны быть задекларированы.

Несмотря на различный правовой подход к определению правовой сущности криповалюты многие зарубежные страны относят деятельность, связанную с майнингом в число лицензируемых и включают операции с криптовалютой в объекты налогообложения.

Литература

1. А. Бычков. Транзакции с криптоактивами и их правовая защита // Новая бухгалтерия №04, 2018
2. О. Ногина. К вопросу об элементном составе налога // Финансовое право. 2005. №7.
3. https://lawstrust.com/ico/pravovoj-status-kriptovalyut/crypto-friendly, https://bits.media/pozitsiya-stran-mira-po-regulirovaniyu-kriptovalyut-na-fevral-2018-goda/

С.А. Нестерович

О некоторых уязвимостях технологии блокчен

Большинство протоколов блокчейна разработаны как децентрализованные одноранговые сети, которые позволяют членам совместно хранить и запускать вычислительные операции с данными без ущерба для безопасности и конфиденциальности. В последние годы технология блокчейн является одной из самой обсуждаемой темой в области информационных технологий. Это связанно с тем, что данная технология стала использоваться во многих отраслях: финан-

[1] В сентябре 2015 года Американская государственная комиссия, заведующая биржевыми фьючерсами) впер (Commodity Futures Trading Commissionвые приравняла биткоин к биржевым товарам

[2] В 2013 году судья Окружного суда Восточного округа Техаса принял решение (Memorandum Opinion), в котором признал биткоин валютой и применил к операциям с криптовалютами финансовое законодательство

сы, торговля, страхование, госуслуги, медицина, логистика и многие другие. Привлекательность технологии блокчейн особенно проявила себя в финансовом секторе. В её основе находятся ряд преимуществ: сокращается время обработки операций, снижаются различные издержки, выросла прозрачность проводимых расчетов, появилась возможность создания новых финансовых инструментов. Однако привлекательная технология блокчейн не так безопасна, и имеет свои уязвимости.

Блокчейн — распределенная база данных, которая хранит информацию обо всех транзакциях участников системы в виде «цепочки блоков» (именно так с англ. переводится Blockchain). Доступ к реестру есть у всех пользователей блокчейна, выступающих в качестве коллективного нотариуса, который подтверждает истинность информации в базе данных[1].

Как только появился финансовый или идеологический смысл в получении информации, сразу появляются технологии, по добычи и обработки этой информации сторонними лицами. Поэтому, компаниям, которые применяют технологии блокчейн нужно помнить это.

Уже известны случаю уязвимостей блокчейна на разных стадиях отработки технологии. По данным WinterGreen, рынок программного обеспечения, услуг и аппаратных решений для защиты блокчейнов может вырасти в десятки раз по сравнению с предыдущим годом. Для сравнения: в 2018 году он составлял $355 млн.

Остаются уязвимыми блокчейн-платформы и смарт-контракты[2]. Это программное обеспечение, которое быстро развивается, а значит, обладает уязвимостями, особенностью для постоянно развивающейся системы: нет времени на всестороннее тестирование, в том числе на тесты по безопасности. Уязвимости платформы уже приводили к ответвлениям в экосистеме криптовалют. Здесь можно прогнозировать увеличение подобных действий в других смарт-контрактах. Взлом криптобирж может быть выгоднее, чем взлом других интернет-площадок.

Так, в августе 2016 года с гонконгской биржи Bitfinex – одной из четырех крупнейших в мире площадок для криптовалютных торгов – похитили 119 756 биткоинов (около $65 млн). Злоумышленникам удалось обойти защиту Bitgo, в том числе двухфакторную аутентификацию и механизм мультиподписи, и совершить массовую кражу с индивидуальных кошельков пользователей[3]. Поэтому, злоумышленники могут заставить программное обеспечение выполнять не те функции, что были в нем предусмотрены изначально. Осуществлять подмену имен кошельков при переводе криптовалюты. Внедрять зловредные программы для использования компьютерных мощностей в своих целях.

---

[1] http://www.tadviser.ru/index.php/Статья:Блокчейн_(Blockchain)

[2] Смарт-контракт (англ. *Smart contract* – умный контракт) – компьютерный алгоритм, предназначенный для формирования, контроля и предоставления информации о владении чем-либо. Чаще всего речь идёт о применении технологии блокчейна. В более узком смысле под смарт-контрактом понимается набор функций и данных (текущее состояние), находящихся по определённому адресу в блокчейне.

[3] https://rb.ru/opinion/ugrozy-blokchejna/.

Еще одним важным моментом, является то, что сам принцип технологии блокчейна, состоит в неизменности проведенных транзакций, и при неправильной – ошибочной или намеренно искажённой – подтвержденной транзакции вся построенная на ней ветвь становится нелегитимной с точки зрения закона, но легальной с точки зрения блокчейн-технологии. Отменить транзакцию физически невозможно, даже если она ошибочна. Поэтому единственный выход, который может сегодня предложить данная технология – ответвленный проект**.** Злоумышленники могут сделать откат транзакций, т.е. напечатать альтернативные блоки и гарантированно опровергнуть то, что происходит в обычном блокчейне («атака 51%»).

«Атака 51%» происходит, когда у атакующей стороны, в роли которой может выступать сравнительно небольшое количество майнеров, находится «контрольный пакет» хэшрейта, т.е. вычислительных мощностей. В результате атаки майнеры получают контроль над всей сетью и могут создавать блоки по своему усмотрению[1]**.** Так, в среду, 4 апреля 2018 года, сеть анонимной криптовалюты Verge подверглась так называемой «Атаке 51%». В результате в течение трех часов мошенники полностью контролировали сеть и проходящие в ней транзакции.

Владение 51% мощностей означает, что этот майнер может подтвердить блок или не подтвердить, и то что он примет будет верным, не зависимо от того является это "истинным" или "ложным".

Например, допустим, мошенник хочет отправить транзакцию одного токена два раза, в то время в его кошельке находится один токен. В случае если никто не владеет 51%, первая транзакция пройдет, а вторая не пройдет, т.к. мощности распределены, и подтверждение блока является истинным. В случае владения 51%, майнер может намеренно подтвердить оба блока, и тогда дублированная транзакция будет истинной, а следовательно будет выполнен перевод одного и того же токена на два разных кошелька. таким образом, владеющий 51%, может "фальсифицировать" транзакции.

Лет через десять, компьютеры, поострённые на квантовых принципах, могут стать угрозой для криптовалют, в основе которых лежит технология блокчейн. К этому выводу пришел международный коллектив исследователей в своей научной статье, которая опубликована на сайте arXiv.org[2]**.**

По их мнению, криптографические протоколы, обеспечивают безопасность интернет-транзакций и финансовых операций, и они потенциально уязвимы для достаточно мощного квантового компьютера.

Пока майнинг биткоинов находится в относительной безопасности, так как в ближайшем времени технология по добычи криптовалют будет мощнее квантовых компьютеров. Но могут быть уязвимы алгоритмы цифровой подписи криптовалют, которые построены на основе эллиптических кривых. В целом, по

[1] https://decenter.org/ru/chto-takoe-ugroza-ataki-51
[2] https://arxiv.org/abs/1710.10377

мнению авторов статьи, квантовые компьютеры создадут угрозу биткоину к 2027 году[1].

Специалисты полагают, что такая атака может быть эффективной, так как при совершении операций с биткоинами между трансляцией и ее обработкой с сохранением данных в блокчейне проходит некоторое время. Поэтому, лет через десять, квантовые компьютеры смогут вычислить приватный ключ на основе публичного, что позволит, перенаправить передаваемые средства на другой кошелек.

В исследованиях специалисты по информационной безопасности изучили различные варианты постквантового шифрования, которые устойчивы для взлома квантовым компьютером, и другие способы противодействия такому виду атак.

В апреле анонимная группа «Большой биткоин-коллайдер» заявила, что может взламывать биткоин-кошельки, используя так называемую атаку методом грубой силы, направляя огромные количества вычислительных мощностей на подбор приватных ключей к индивидуальным кошелькам[2].

Технология блокчейна, при определенных условиях может быть весьма уязвимой. Иногда можно обвинить некачественное выполнение или непреднамеренные ошибки в написанном коде. В других случаях речь идет, скорее, о «серой зоне» – сложном результате взаимодействия кода, экономики блокчейна и человеческой жадности».

Конечно, наличие недостатков в безопасности блокчейна не делают технологию абсолютно неприменимой. Наоборот, по сравнению с централизованными системами обработки информации блокчейн выглядит как революционная модель с большими перспективами на отдельных типах задач. Однако необходимо знать и помнить о рисках и угрозах, которые могут существовать, и не относиться к блокчейну как к решению всех проблем информационной безопасности.

А.М. Новиков

Криптовалюты – это только начало

Аннотация. В статье рассмотрены перспективы развития блокчейн технологии. Отмечены достоинства новых систем. Даны прогнозы относительно перспектив применения технологии, лежащей в основе криптовалют, в экономике в целом.

Ключевые слова: криптовалюты, экономическая безопасность, государственное регулирование экономики, умные контракты, децентрализованные автономные организации.

Криптовалюты, несмотря на свое недавнее появление, уже перестали быть экзотикой и привлекают все большее внимание. В последнее время многие крупные компании выразили свое отношение криптовалюте. Особое внимание при этом уделяется технологии, которая лежит в основе криптовалют, а имен-

[1] https://mining-cryptocurrency.ru/kvantovyj-kompyuter-vzlomaet-koshelki-bitcoin/
[2] http://monetarystar.ru/kvantovyj-kompjuter-smozhet-vzlomat-koshelki/

но, цепочке блоков – блокчейну. Это технология, возможно, поменяет даже базовые принципы, которые лежат в основе повседневных деловых отношения, и уж тем более в сфере финансовых взаимоотношений. Из всех криптовалют доминирующее положение занимает биткоин, поэтому говорить будем прежде всего о нем.

Биткоин является цифровым документом на предъявителя, который можно передавать через надежную распределенную сеть. Передача не требует централизованного посредника, такого как банк. Только владелец актива может отправить сообщение о передаче актива, и получить его может только указанный получатель.

Биткоин появился прежде всего как платежное средство. Он претендует на роль альтернативы существующим системам фиатных денег. И хотя биткоин, и тем более любую другую криптовалюту, пока нельзя назвать деньгами, он, вероятно, является предвестником чего-то большего, чем просто вариант принципиально новой денежной системы. Уже сейчас можно сказать, что ведется последовательная работа по созданию *криптоэкономики*.

Важнейшими составляющими криптоэкономики, которые сейчас можно выделить, ни в коем случае не претендуя на полноту, являются:

криптовалюта (блокчейн);

регистрация прав собственности;

умные контракты;

децентрализованные автономные организации.

Прежде всего, биткоин предлагает альтернативу существующей денежной системе. Современные деньги представляют собой совокупность записей на счетах в коммерческих банках. Хотя считается, что учет этих записей централизованный, эта централизация не является полной, поскольку деньги — это записи в коммерческом банке, которые делают сами банки.

Биткоин обеспечивает как хранение учетных единиц, так и перевод от одного владельца к другому. Причем безопасность таких переводов сравнима с безопасностью перевода внутри банковской системы, а себестоимость переводов принципиально ниже. Но биткоин, по крайней мере пока, не является деньгами, он даже не является и всеобщим эквивалентом. Для того, чтобы стать деньгами, биткоину необходимо превратиться не только во всеобщий эквивалент, но и в постоянный, и устойчивый эквивалент. Однако, даже не став ни постоянным, ни устойчивым, ни всеобщим эквивалентом, биткоин имеет просто захватывающую динамику развития по всем этим направлениям.

Наиболее радикальные адепты криптовалют считают, что биткоин предлагает альтернативу существующей банковской системе: огромной централизованной махине, состоящей из коммерческих банков, внебанковских кредитных учреждений, центральных банков. Теоретически все это может быть заменено никем не контролируемой распределенной сетью.

Новые технологии потенциально могут затронуть не только финансовую сферу. Это, прежде всего, регистрация прав собственности. Так, централизованный регистратор авторских прав может быть заменён публичной учетной системой биткоина, которая может как зарегистрировать право, так и сделать

временную метку. Над созданием платформы для регистрации авторских прав уже работает ряд стартапов. Блокчейн потенциально может быть использован и для регистрации владения любым имуществом: недвижимости, автомобилей, ценных бумаг и так далее. И обществу нужно рассчитать, что выгодней: оставлять старую систему регистрации прав собственности или перейти на новую платформу. Такую работу может организовать только государство как выразитель общенародных интересов. И уж тем более решение вопроса нельзя отдавать «на откуп» заинтересованному ведомству.

Важнейшим свойством биткоина, которое нужно особенно подчеркнуть, является то, что это самоподдерживающаяся система, созданная на основе выбранных правил. Это система, работающая не зависимо от человеческих предпочтений и интересов, и устойчивая к внешнему воздействию. Данный подход позволяет участникам быть уверенными в том, что их права не будут нарушены, поскольку никто не сможет изменить правила. Важно также отметить, что система исходит из того, что человеческая природа не идеальна.

Следующий пункт касается контрактов. Традиционные контракты не только сложны в составлении, но и требуют привлечения третьих лиц для обеспечения их соблюдения. В случае разночтений стороны вынуждены обращаться в суды, что отнимает еще больше времени и денег.

В 1994 году Ник Собо предложил концепцию умных контрактов, определив такой документ как электронный протокол передачи информации, обеспечивающий исполнение сторонами условий контракта. Смарт-контракты позволяют обеспечивать автоматическое выполнение условий сделок без необходимости привлечения третьих лиц для обеспечения доверия.

Появление технологии блокчейн создало условия для создания систем, позволяющих заключать и автоматически исполнять сделки по достижении заданных условий, минуя централизованных посредников. В отличие от юридического языка, код не подвержен двойным толкованиям. Поскольку смарт-контракты являются программами, стороны сделки могут быть уверены, что условия, прописанные в коде контракта, будут соблюдены неукоснительно и не могут быть изменены задним числом.

Четвертой составляющей криптоэкономики, которую мы здесь отметим, являются децентрализованные автономные организации – ДАО. ДАО, которые являются попыткой реализации новой парадигмы экономического сотрудничества.

Децентрализованные автономные организации можно представить как комплекс из умных контрактов, который вписывает уставы, правила работы и метод управления организации в программный цифровой код.

Децентрализованность предполагает горизонтальное строение компании. У ДАО каждый участник организации – полноправный совладелец и обладает равными полномочиями и неограниченным доступом к информации. Для обеспечения деятельности подобной структуры необходим блокчейн. Блокчейн является электронным реестром компании, который поддерживается всеми участниками сети.

Автономность означает независимостью от традиционных финансовых и политических институтов, и важную роль в этом играет замена фиатных денег криптовалютой.

Система ДАО делает ненужной корпоративную юриспруденцию, поскольку все взаимодействия осуществляются с помощью умных контрактов. В идеале ДАО не только автономна, но и максимально или полностью автоматизирована.

За последние годы проделана большая работа по созданию элементов системы, которую можно охарактеризовать как «криптоэкономика». Но пока возможность ее появления только теоретическая. Хотя на практике существуют и криптовалюты (так, по капитализации биткоин сейчас – десятая валюта в мире), и умные контракты, и ДАО, но их влияние на реальную экономику крайне незначительно. И сейчас невозможно сделать прогноз о будущем развитии рассмотренных новых экономических структур.

Литература

1. Буликов С.Н. Криптовалюта и технология блокчейн//Теоретическая экономика. 2019. № 1 (49). С. 89-104.
2. Закон РФ "О денежной системе Российской Федерации" от 25.09.1992 N 3537-1.
3. Запорожан А.Я. Криптовалюта сегодня и завтра//Научные труды Северо-Западного института управления. 2018. Т. 9. № 4 (36). С. 147-153.
4. Новиков А.М. Криптовалюты: вызов современной денежно-кредитной системе или мыльный пузырь?//Российское государство и социально-экономические вызовы современности: сборник научных статей. Том 2. – М., Проспект, 2015. С. 157-163.
5. Положенцева Ю.С., Клевцов С.М., Тевяшова А.С. Менеджмент использования криптовалюты в дифференцированном интернет-пространстве//Бизнес. Образование. Право. 2018. № 1 (42). С. 103-110.

М.В. Пальчикова

Возможность законодательного регулирования технологии блокчейн и обращения криптовалют как способ противодействия террористическим угрозам

Аннотация. Статья посвящена анализу законопроекта «О цифровых финансовых активах» с точки зрения необходимости и достаточности предложенного правового регулирования. В статье рассматриваются различные подходы к понятиям блокчейн и криптовалюта и их имплементация в действующее законодательство, возможность противодействия финансированию террористических угроз путем легализации технологии блокчейн.

Ключевые слова: блокчейн, криптовалюта, майнинг, смарт-контракт, цифровой кошелек, терроризм.

Стремительное развитие технологии блокчейн является не угрозой национальной безопасности, а скорее вызовом регуляторам для принятия соответствующих решений. Главнейшим целью становится не запрет, а необходимость своевременного и достаточного регулирования дальнейшего развития технологии. Сейчас важно не опоздать, разрешить и установить необходимые правовые рамки, в том числе и для того, чтобы вовремя реализовать положения государственной программы «Цифровая экономика Российской Федерации»[1]. Россия в настоящий период времени находится в наиболее выгодном положении для привлечения инвестиций в развитие технологии блокчейн и рынок криптовалют. По словам Элины Сидоренко – руководителя межведомственной группы Государственной Думы Российской Федерации по оценкам оборота криптовалют – уникальное геополитическое положение РФ создает уникальную среду для развития криптооборота при условии удобного законодательства; основой этого является относительно дешевая электроэнергия, позволяющая использовать выделяемое тепло. Последние исследования подтверждают высказанные прогнозы. Россия заняла третье место в мире по объему привлеченных в ходе ICO средств. Аналитики аудиторской компании Ernst & Young подсчитали, что лидером по проведению ICO (первичное размещение криптовалюты) в мире стали США, где с помощью данного инструмента бизнес смог привлечь более $1 млрд инвестиций, на втором и третьем местах разместились Россия и Китай – $452 и $310 млн соответственно[2].

Вследствие вышесказанного становится понятно, что сейчас Россия находится в переломной точке, в которой главное «не упустить момент» и не только подвести под криптооборот грамотное законодательное регулирование, но и не сделать его жестким и не перспективным. Поэтому вполне обоснованным является представление Министерством финансов законопроекта «О цифровых финансовых активах», который находится в настоящее время находится на рассмотрении в Государственной Думе (Законопроект № 419059-7)[3].

Основные риски криптооборота, про которые наиболее часто упоминается в средствах массовой информации и в околонаучном сообществе, связаны с боязнью легализации денежных средств и направлении их на финансирование преступных групп и мероприятий, а возможностями защиты персональных данных при операциях с криптовалютой. Например, Японское правительство, министры финансов и главы центральных банков Франции и Германии предлагают сделать регулирование криптовалют международным с целью предотвращения отмывания денег посредством виртуальных валют. МВФ также придерживается точки зрения о необходимости регулирования рынка цифровых валют. Отсутствие внешнего и внутреннего контроля за оборотом криптовалют и анонимность расчетов создают потенциальные предпосылки для их использования с целью легализации денежных средств, полученных преступным путем,

[1] Распоряжение Правительства РФ от 28.07.2017 № 1632-р «Об утверждении программы «Цифровая экономика Российской Федерации» // Официальный интернет-портал правовой информации http://www.pravo.gov.ru. 03.08.2017.

[2] Проект федерального закона «О цифровых финансовых активах» // https://www.minfin.ru.

[3] АЗОД Государственной Думы РФ http://asozd.duma.gov.ru.

оплаты запрещенных к свободному обращению товаров, в частности, наркотиков и оружия, дает возможность финансирования терроризма.

Данные вопросы по мере возможностей современного законодательства были решены в представленном законопроекте. Остановимся на данном регулировании подробнее.

Самым слабым в цепочке обращения криптовалют является звено, в котором криптовалюты обмениваются на традиционные деньги. Так как это происходит на вновь созданных нерегулируемых биржах, то они часто становятся объектом хакерских атак. Ярким примером проблемы безопасности криптовалют является история биржи Coincheck в Японии, которая была взломана мошенниками, в результате чего были похищены 520 млн токенов NEM с потерями для биржи на сумму около $440 млн. Хакеры воспользовались уязвимостью IT-систем и с помощью вируса украли ключи шифрования кошельков пользователей. Эти ключи были выложены на различных сайтах в «даркнете» (DarkNet)[1].

Противодействие легализации в проекте Закона «О цифровых финансовых активах» осуществлено путем введения понятия «цифровой кошелек», который может быть открыт только путем прохождения процедуры идентификации его владельца в соответствии Федеральным законом от 07.08.2001 № 115-ФЗ (ред. от 29.07.2017) «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»[2] [3]. Если под «транзакцией» понимать процесс передачи биткоинов, или другой криптовалюты в блокчейне, подтвержденных цифровой подписью, а не просто перемещением, то после занесения «хеша» в новый блок и его проверки майнерами, транзакция фиксируется в блокчейне и считается успешной. И, только после этого считается совершенной транзакцией путем консенсуса. Особенностью является то, что практически в любом блокчейне каждый имеет возможность просмотреть историю всех транзакций, которые произошли раньше, однако личные данные владельца кошелька не отображаются. Цифровой кошелек согласно российскому законопроекту служит для хранения токенов и открывается брокерами и дилерами. Остальные пользователи имеют возможность приобрести токен только путем открытия счета в цифровом кошельке, порядок этой операции должен установить Центральный Банк РФ.

Установленный порядок сводит на нет дискуссию о возможности легализации преступных доходов, поскольку привязывает оборот криптовалют к уже апробированному законодательному регулированию и дополнительным правилам ЦБ РФ.

Проблема законопроекта заключается в том, что авторы восприняли концепцию отождествления блокчейна и криптовалюты, хотя криптовалюта является по сути одним из конечных результатов применения технологии блокчейн. Например Bitcoin foundation и ряд других ведущих мировых пропагандистов

[1] Доклад Международного дискуссионного клуба «Валдай» «Блокчейн и криптовалюты: обзор трендов и перспектив» // http://ru.valdaiclub.com/files/21191/

[2] Федеральный закон от 07.08.2001 № 115-ФЗ (ред. от 29.07.2017) "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" (с изм. и доп., вступ. в силу с 28.01.2018) // Российская газета. № 151-152, 09.08.2001

блокчейна дают следующие определения, которые на наш взгляд более полные по смыслу и значению. Это, прежде всего децентрализованный способ хранения данных или цифровой реестр информации, транзакций, сделок, контрактов, основанных на криптографии. Всего что нуждается в отдельной независимой записи которая может быть проверена и которая основана на консенсусе всех кто ее подтвердил.

В блокчейне можно хранить данные о выданных кредитах, правах на собственность, нарушении правил дорожного движения, актах бракосочетаний и т д. То есть практически обо всем, а не только использовать в криптовалютных транзакциях. Главным его отличием и неоспоримым преимуществом является то, что этот реестр не хранится в каком-то одном месте или на одном сервере. И, в этом ключевое различие блокчейн-технологии и серверной. Он распределен среди нескольких сотен и даже тысяч компьютеров во всем мире[1]. Являясь абсолютно новым и никак не описанным в юридической практике явлением, технология блокчейн включает в себя помимо криптовалюты, платежную систему, бизнес-процесс (смарт-контракт как форма), и возможность программирования и включения в криптокод необходимой информации. Последнее, по прогнозам экспертов, снимет все вопросы по аутентификации авторства и изменит целую отрасль права- авторское право.

Например, законопроект положил конец спорам и отождествил криптовалюту как имущество. На наш взгляд, это противоречит и самой концепции имущества и имущественных прав и ставит блок для дальнейшего регулирования, в случае, когда криповалюта будет реализовывать право требования.

В мае 2019 года Девятый Арбитражный апелляционный суд в споре о банкротстве признал криптовалюту имуществом.

Уже после рассмотрения этого дела в первой инстанции в Госдуму внесли законопроект, который предлагает закрепить в ГК несколько базовых положений для регулирования новых объектов экономических отношений – «токены», «криптовалюты» и другие. Так что довод апелляции о том, что для квалификации криптовалюты в качестве объекта для включения в конкурсную массу необходим специальный закон, не выглядел бы достаточно убедительно, еще до заседания в 9-м ААС говорила Людмила Меркулова, правовой эксперт.

Эксперты сходятся во мнении, что данное решение суда дает российским должникам этакую лазейку для вывода активов, причем фактически бесконтрольного[2]. Такая неоднозначная позиция судов и правоприменителей ставит законодателю дополнительные вопросы – как использовать новые виды имущества, дабы избежать размывания финансовых активов должников, которые могут быть выведены и использованы на совсем не благие цели.

Также смарт-контракт по проекту закона оказался видом договора, а не его формой. С учетом заложенных условий он может применяться только в целях оборота и регулирования криптовалют, хотя смарт-контракты имеют гораздо более обширную сферу и направления применения.

---

[1] Официальный новостной интернет–портал https://www.obozrevatel.com.

[2] Официальный интернет-портал правовой информации. URL: https://pravo.ru.

Вторым недостатком законопроекта на наш взгляд является слишком однозначная дефиниция «майнинга» как деятельности по созданию криптовалют, хотя именно этим майнинг не ограничивается. Гораздо более прогрессивным и точным было бы его определение через суть – выделение мощностей для целей поддержки распределенного реестра и создания новых блоков с возможностью получения условного вознаграждения. Майнинг не должен представляться как эмиссия, а скорее как товаропроизводство.

Защите персональных данных в законопроекте внимание не уделяется, что представляется вполне оправданным, но потребует уточнения в дальнейшем. Все же следует помнить, что технология блокчейн имеет ряд преимуществ:

- высокая степень достоверности произведенных операций
- практически абсолютная прозрачность
- невозможность изменения данных задним числом
- высокая степень безопасности
- отсутствие человеческого фактора
- оперативность.

В заключении следует отметить, что законопроект «О цифровых финансовых активах» важный шаг на пути регулирования процесса блокчейна, который в перспективе позволит расширить возможность борьбы с нелегальным оборотом денежных средств, увеличит прозрачность финансовых операций, а также иных действий, способствующих идентификации пользователей по самым различным направлениям.

В.А. Перов

Криминалистическая методика выявления лиц, совершающих преступления с использованием криптовалюты

Аннотация. В статье рассматривается основа криминалистической методики по выявлению преступлений, совершаемых с использованием криптовалюты и последующему расследованию такого рода уголовных дел.

Анализируя функциональные принципы функционирования криптовалют и систему сложившихся в указанной области закономерностей автором предлагается основа соответствующей криминалистической методики.

Ключевые слова: криминалистическая методика, криптовалюта, криптокошельки, криптовалютные транзакции, «Silk Road», товары запрещенные или ограниченные в гражданском обороте, онион (onion) зона, даркнет, майнинг, выявление преступлений, расследование уголовных дел.

Совершение преступлений с использованием криптовалюты требует создание продуманной криминалистической методики противодействия таким преступлениям и выявлению лиц их совершающих. На сегодняшний день мы не может сказать о том, что существует эффективная методика выявления лиц стоящих за анонимно открытыми криптокошельками и использующих их при совершении преступлений в указанной сфере.

К сожалению, сегодня преступления с использованием криптовалюты продолжают совершаться, и к сожалению, в большинстве случаев безнаказанно. Кроме того, можно сказать, что в условиях к сожалению сложившейся правовой неопределенности, криптовалюты как объекта гражданских прав, подобного рода деятельность приобретает характер промысла. То есть лица совершающие подобного рода противоправные деяния ставят их совершение на поток, имея своей целью наличие постоянного дохода, сопряженного с криминальной деятельностью.

Приходиться констатировать, что на сегодняшний день большинство товаров, реализуемых за криптовалюту запрещены или ограничены в гражданском обороте. Это наркотические или сильнодействующие вещества, оружие, поддельные документы или деньги.

Так например, если, с помощью популярного сегодня «TOR»-браузера зайти в онион (onion) зону, то можно обнаружить большое количество такого рода интернет-магазинов (интернет-площадок) торгующих товарами подобного рода или принимающих заказы на сомнительные услуги, типа: «продаем удостоверения МВД, ФСБ, СК, Прокуратуры Российской Федерации, Росгвардии, судьи, адвоката». И это не самое криминальное, но, пожалуй, наиболее часто встречаемое объявление.

Более того у подобного рода интернет-магазинов существует свой рейтинг и свои интернет-форумы, где покупатели в сети «Даркнет» обмениваются друг с другом информацией о надежности того или иного продавца и качестве приобретенного ими товара или оказанной услуги.

При этом местоположение и IP-адрес onion-сервиса скрыты, вследствие чего гораздо труднее его блокировать или идентифицировать владельца.

Весь осуществляемый между пользователями «Tor» и onion-сервисами трафик защищен сквозным шифрованием, а адреса onion-сервиса генерируется автоматически.

Соответственно оплата приобретаемого товара в интернет-магазинах подобного рода осуществляется путем криптовалютных перечислений с крипто-кошелька покупателя на крипто-кошелек продавца. В свою очередь доставка покупателю оплаченного подобным образом товара осуществляется либо путем «закладок», то есть оставления приобретенного товара в определенном месте, предварительно согласованного с покупателем, либо путем почтовых отправлений на абонентский ящик покупателя.

При это если, доступ к сети «Tor» будет заблокирован интернет-провайдером, то «Tor»-браузером предусмотрены определенные инструменты (подключаемые транспорты) для обхода таких блокировок, которые свободно можно найти на сайте Tor Browser.

Также нередки случаи хищения крипто-монет из крипто-кошельков, совершаемых как путем банального фишинга (разновидности интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей, то есть определенным логинам и паролям с помощью которых можно получить доступ к чужому счету и произвести перечисление денежных средств, применительно к данному случаю криптовалюты), так

и путем автоматического подбора соответствующего ключа, осуществляемого ботом (роботом). При этом в каждом конкретном случае от метода, которым было совершено то или иное преступление зависит его юридическая квалификация.

К сожалению, в настоящий момент мы можем говорить о том, что выявляются, пресекаются и расследуются преступления, в которых криптовалюта фактически является средством платежа, но не преступления в которых криптовалюта выступает в качестве предмета преступного посягательства.

Как правило такие преступления выявляются и пресекаются на стадии, когда покупатель уже получил доставленное ему почтой специальное отправление (посылку, бандероль) или попытался в заранее оговоренном месте взять оставленную для него «закладку». При этом незаконное приобретение товара фиксируется, а покупатель незаконно приобретший указанный товар как правило задерживается и в отношении него возбуждается уголовное дело. Также имеют место случаи задержания и привлечения к уголовной ответственности так называемых «закладчиков», то есть лиц, непосредственно осуществляющих в специально оговоренном с покупателем месте закладку ограниченного или запрещенного в гражданском обороте товара.

При всем этом к ответственности чаще всего привлекаются лишь исполнители преступления, а организаторы продолжают руководство преступным сообществом, осуществляющим незаконный сбыт товаров, запрещенных или ограниченных в гражданском обороте в том числе наркотических средств и сильнодействующих средств, оружия, боеприпасов, поддельных документов

И такое положение дел существует по двух причинам:

Во-первых не определен правовой статус криптовалюты на территории Российской Федерации, хотя в Государственной Думе находится на рассмотрении соответствующий законопроект.

И во-вторых отсутствует эффективная криминалистическая методика, позволяющая выявлять соответствующие преступления, дающая возможность добычи доказательств по расследуемому уголовному делу.

Таким образом на сегодняшний день складывается достаточно парадоксальная ситуация, при которой преступления с использованием криптовалюты продолжают совершаться, но какого-либо доступного и эффективного способа их выявления и пресечения не существует. Уже само по себе отсутствие адекватного противодействия совершаемым преступлениям приводит к увеличению количества таких преступлений, и порождает иллюзию безнаказанности и вседозволенности у лиц их совершающих.

На сегодняшний день как уже было сказано выше не существует единого мнения относительно наиболее эффективных способов выявления преступлений, совершаемых с использованием криптовалюты и последующего расследования такого рода уголовных дел.

Мнения о необходимости создания такой методики разняться. От мнения о необходимости ее создания до ее ненужности, так как якобы существуют некие программы-руткиты, позволяющие каким-то образом отслеживать владельцев крипто-кошельков, совершающий незаконные криптовалютные сделки. Можно

также встретить мнения относительно того, что феномен криптовалют до конца не изучен, вследствие чего можно ограничиться накоплением эмпирического материала по данной тематике.

Что можно на это возразить? Нельзя конечно исключать возможности создания соответствующих руткитов собирающих информацию о владельцах крипто-кошельков, однако сведения о наличии и функционировании таких программ на текущий период времени отсутствуют, вследствие чего строить криминалистическую методику на возможности их использования не представляется возможным если конечно мы не рассматриваем некую возможную отдаленную перспективу.

Подобного рода криминалистическая методика должна быть основана только на основополагающих функциональных принципах криптовалют.

К таковым относятся:

-децентрализация их выпуска;

-отсутствие по крайней мере на сегодняшний день возможности в том числе и технической за их контролем и регулированием обращения;

-анонимность лиц, использующих криптовалюту при полной открытости обращения криптомонет и возможностью отслеживания криптовалютных транзакций;

-отсутствие административно-территориальных барьеров для создания и использования криптовалюты;

-наличие анонимной возможности совершения любого вида сделок вне зависимости от требований национального законодательства определенного государства.

Таким образом принимая во внимание определенный уровень анонимности использования криптовалют необходимо определить те границы, где указанная анонимность заканчивается и начинаются так называемые «точки доступа» к персональным данным определенного лица, совершающего криптовалютные операции, нарушающие требования национального законодательства.

Учитывая, что крипто-кошельки как правило являются анонимными одной из таких «точек доступа» может являться операция по обмену (купле-продаже) той или иной криптовалюты на фиатные деньги. Именно при совершении данной операции, осуществляемой путем зачисления фиатных денежных средств на банковский счет (списания со счета) лица продавшего (приобретшего) криптомонеты появляется возможность установить участника такой сделки или по крайней мере лицо, действующее в его интересах или с ним связанное определенными отношениями.

Второй «точкой доступа» хотя и не всегда позволяющей точно персонифицировать лицо, совершающего противозаконные сделки с криптовалютой, но при этом все-же позволяющей сделать относительно-определенные предположения относительно такого лица является комплексный анализ информации о связях анонимного лица с уже ранее реально установленными лицами, а также анализ информации анонимных и реальных лиц в том числе в телекоммуникационной сети интернет.

Именно таким образом по информации ФБР США был установлен и в последующем привлечен к ответственности владелец торговой интернет-площадки Silk Road («Шелковый путь») Росс Уильям Ульбрихт (Ross William Ulbricht).

Для этой цели могут быть успешно использованы как компьютерные программы для построения диаграммы связей, так и схемы, построенные экспертом-аналитиком. Конечно наиболее эффективным будет являться комплексный подход с использованием аналитических знаний человека и возможностей вычислительной машины.

Комплексное использование двух указанных способов на сегодняшний день является наиболее эффективным средством выявления преступлений, совершаемых с использованием криптовалюты и источником доказательств при расследования соответствующих уголовных дел. Именно они должны быть положены в основу криминалистической методики по выявлению преступлений, совершаемых с использованием криптовалюты и расследованию такого рода уголовных дел.

Таким образом данная методика основывается на практике выявления лиц, совершаемых с использованием криптовалюты, опробированной ФБР США и как это кому-то не покажется странным системы криминалистических учетов, используемых в СССР. Именно такая автоматизированная информационная учетная программная система (АИС) должна быть использована для упорядочения по определенным признакам сведений, иметь общие принципы описания, хранения и манипулирования такими данными.

Второй вид АИС представляет собой системы, осуществляемые поиск определенной информации (об определенном лице) в телекоммуникационной сети Интернет и установления его возможных связей.

Комплексное применение указанных АИС с системой геопозиционирования и предусмотренных Федеральным законом «Об оперативно-розыскной деятельности» от 12.08.1995 № 144-ФЗ оперативно-розыскных мероприятий позволяет раскрыть анонимность лиц, использующих крипто-кошельки в противоправных целях.

Литература

1. В.А. Ализаде, А.Г. Волеводз. Судебная практика по делам о преступлениях в сфере незаконного оборота наркотиков, совершенных с использованием криптовалюты: от разных подходов к предложению единого понимания. Журнал «Библиотека криминалиста» № 1 (36) 2018
2. Э.Л. Сидоренко Особенности квалификации преступлений, связанных с хищением криптовалют. Журнал «Библиотека уголовного права и криминологии» 2018. № 3 (27)
3. П.В. Галушин, А.Л. Карлов. Сведения об операциях с криптовалютами (на примере Биткойна) как доказательство по уголовному делу. Электронный научно-теоретический журнал «Ученые записки Казанского юридического института МВД России» 2017 Том 2 (4)

Интернет-ресурсы

1. Официальный сайт ФБР США (https://www.fbi.gov/)
2. Официальный сайт Следственного комитета Российской Федерации (http://sledcom.ru/)
3. Официальный сайт МВД Российской Федерации (https://xn--b1aew.xn--p1ai/)
4. http://privatfinance.com
5. https://blockchain.info/ru
6. https://cryptocurrency.tech

Д.А. Печегин

Проблемные аспекты квалификации криптопреступлений в Германии[1]

Аннотация. В настоящее время не существует универсального правового определения криптовалюты. На основании доклада Европейского Центрального Банка **(**ЕЦБ**)** 2012 г**.** Европейский Суд по делу Skatteverket v. David Hedqvist (Case C-264/14) пришел к выводу о том**,** что представляют собой виртуальные валюты. Однако уже в 2015 г. ЕЦБ предложил новое определение. Самостоятельную дефиницию криптовалюты предложил и FATF, а равно ряд иных организаций, в том числе на международном уровне. Вместе с тем, отсутствие четкого законодательного определения криптовалюты отнюдь не означает невозможность уголовного преследования за противоправные деяния в криптосфере. Правоприменители в Германии стремятся квалифицировать криптопреступления с помощью имеющегося законодательства, не дожидаясь нового регулирования, осуществляя тем самым превентивную функцию.

Ключевые слова: криптовалюта, валютное регулирование, денежный суррогат, уголовное законодательство, криптосфера, ФРГ.

В апреле 2018 г. именно Германия при поддержке Франции внесла в повестку дня стран G20 тему определения правовой природы и порядка законодательного регулирования криптотокенов и других современных электронных сущностей совместно с такими организациями, как CPMI, IOSCO, FATF. При этом экономика Германии является крупнейшей среди европейских государств, а те или иные изменения немецкого законодательства в связи с новыми технологиями неизбежно оказывают влияние на законодательство стран романо-германской правовой традиции ввиду установившегося тренда лояльности по отношению к новым сущностям. С учетом этого и поставленной перед отечественным законодателем задачи активного развития законодательства в области криптоиндустрии, анализ немецкого подхода к вопросу о квалификации криптопреступлений является актуальным.

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16062 "Концепция правового обеспечения цифровизации сферы публичных финансов".

Современные исследователи, изучая уголовно-правовой статус криптовалют, выделяют разные подходы. Отмечается, что криптовалюта не создаст каких-либо проблем для правоприменителя в случае с квалификацией оборота наркотических средств, психотропных веществ, их аналогов и прекурсоров. Связано это с тем, что в отечественном законодательстве именно такого рода действия образуют объективную сторону преступления (ст. 228-229.1 УК РФ). В связи с этим криптовалютная транзакция может рассматриваться как доказательство перехода предмета преступления от одного лица к другому. Хищение криптовалюты уже представляет определенную сложность, хотя бы потому, что конкретный правоприменитель сегодня не видит в ней предмета посягательства, в связи с чем вправе отказать в возбуждении уголовного дела (неясно, как оценить содеянное в денежном эквиваленте, т.к. у криптовалюты пока еще нет гражданско-правового статуса)[1].

Однако, поскольку современные технологии и криптовалюты так или иначе связаны с использованием информационных технологий, постольку особо значимыми сегодня становятся преступления, совершаемые с помощью компьютерных данных либо против таких данных, хранящихся где-либо. Между тем криптовалюты сегодня вряд ли можно отнести к самостоятельным объектам таких преступлений, за исключением лишь, пожалуй, хищения. Скорее, новые технологии выступают в качестве особого способа совершения того или иного преступления.

Если так называемые традиционные преступления (mala in se), совершенные посредством новых технологий, еще более или менее можно подвести под действующее регулирование в сфере уголовного законодательства, то сегодня весьма распространенными становятся новые «крипто»-преступления. Полиция ФРГ все чаще сталкивается с преступниками и целыми группировками, которые совершают преступления в сети Интернет с использованием высокотехнологичного оборудования. Центральной задачей правоохранительных органов ФРГ в данной сфере является превенция совершения противоправных действий. Реакция на развитие преступности так называемой экономики 2.0, 3.0 и т.д. должна быть адекватной. Криминалистические техника и методики также должны соответствовать уровням 2.0, 3.0 и проч. Этим занимаются отделы по противодействию киберпреступности и цифровым расследованиям уголовного розыска той или иной земли ФРГ. Например, это относится к явлению скрытого майнинга, т.е. несанкционированного тайного использования ресурсов компьютера пользователя с целью извлечения выгоды в форме потенциально возможного получения вознаграждения за майнинг.

Федеральная служба уголовной полиции ФРГ (Bundeskriminalamt) представила ежегодный отчет о состоянии киберпреступности в стране за 2017 год.[2] В данном отчете были отражены сведения и о преступлениях, связанных с крип-

[1] Сидоренко Э.Л. Правовой статус криптовалют в Российской Федерации // Экономика. Налоги. Право. 2018. № 2. С. 133-134.

[2] URL: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2017 (дата обращения: 12.12.2018).

товалютой. Причем многие вредоносные программы сегодня акцентируются на том, чтобы нелегально и незаметно использовать ИТ-ресурсы той или иной компании либо отдельного пользователя для того, чтобы осуществлять скрытый криптомайнинг, в том числе известной цифровой валюты *Bitcoin*. Причем для этого сегодня не обязательно заражать компьютер конкретного пользователя, соответствующие скрипты, которые будут «высасывать» энергоресурс вашего компьютера теперь можно встраивать в сайты и видео (музыку). Зайдя на тот или иной ресурс и нажав кнопку «Play» пользователь автоматически разрешает такому ресурсу использовать вычислительную мощность его компьютера до тех пор, пока он данным ресурсом пользуется. Сложность квалификации такого деяния заключается в том, что такие программы зачастую не нарушают целостность самой системы, а просто нагружают ее гораздо сильнее, пока пользователь обращается к интернет-ресурсу. Иными словами, как только пользователь закроет сайт или браузер, то соответствующий скрипт прекратит свое выполнение и не будет наносить вреда системе пользователя. УК ФРГ содержит самостоятельный состав преступления, предусмотренный § 303a, который устанавливает ответственность за неправомерное удаление, преобразование, приведение в непригодное состояние и изменение данных пользователя.

Однако для того, чтобы квалифицировать описанный выше случай по § 303a УК ФРГ, соответствующий скрипт должен проникнуть в уязвленную систему и образовать в этой системе условия для постоянной связи с соответствующим сервером. В последнем случае, такое деяние подпадает под признаки преступления, предусмотренного § 303a УК ФРГ, поскольку тут, скорее всего, произойдет тайное и несанкционированное изменение данных пользователя. Вместе с тем для такого вывода программное обеспечение соответствующего компьютера, по идее, должно стать единым, по подобию блокчейн-технологии, когда любое изменение требует создание нового блока, что позволит легко выявить несанкционированные изменения системы. Но даже и без такой структуры программного обеспечения конкретного пользователя данный случай, в целом, подпадает под § 303a УК ФРГ.

Земельный суд г. Кемптена (Бавария) в своем решении[1] от 27 июля 2017 года указал, что изменение данных по смыслу абзаца 1 § 303a УК ФРГ имеет место в результате нарушения функций данных, которые приводят к изменению их информационного содержания или показателя. Под это подпадает любая форма преобразования содержимого сохраненных данных, причем не имеет значения, является ли это объективным улучшением. Решающее значение имеет, скорее, то, что состояние системы отличается от предыдущего. При этом сам пользователь обязан предпринять меры по защите своей информации, например, воспользоваться брандмауэром, который не позволит обычном пользователю без специальной подготовки получить доступ к информационной системе.

Однако это не означает, что преступник в последнем случае избежит ответственности. В рассмотренном деле только на 75 % зараженных компьютеров

[1] BGH 1 StR 412/16 - Beschluss vom 27. Juli 2017 (LG Kempten). URL: https://www.hrr-strafrecht.de/hrr/1/16/1-412-16.php (дата обращения: 12.04.2019).

брандмауэр был включен автоматически, тогда как в 25 % случаев такая программа была деактивирована. Вместе с тем, вредоносное программное обеспечение скрытно устанавливалось на компьютеры пользователей и обладало возможностью обходить защиту брандмауэра. Поэтому все установленные судом случаи были верно квалифицированы по § 303a УК ФРГ.

С другой стороны современные технологии позволяют, как мы выяснили выше, обходиться и без изменения соответствующих данных либо заражения компьютера, что требует самостоятельного осмысления с точки зрения описания преступного деяния в доктрине уголовного права и далее, соответственно, в уголовном законодательстве. В частности, отдельного осмысления требует та граница, за пределами которой будет установлена уголовная ответственность при несанкционированном использовании ресурсов компьютера пользователя, посетившего тот или иной интернет-ресурс. Ведь данные скрипты весьма успешно могут использоваться рекламодателями взамен обращения к баннерам, которые иногда слишком навязчиво предлагают какой-либо товар пользователю и в большей степени нагружают операционную систему компьютера пользователя. Однако данная проблема в науке уголовного права ФРГ не решена.

Сегодня нередки и такие случаи, когда компьютеры, особенно ИТ-системы компаний и их серверы, намеренно заражаются вирусной программой в целях скрытого криптомайнинга. Так, в июне 2017 года во всем мире произошло массовое разрушительное воздействие вредоносного программного обеспечения на ИТ-системы предприятий. Эти события коснулись и ФРГ. Вредоносная программа «NotPetya»[1] изначально заразила несколько компаний, преимущественно в Украине, для выявления уязвимости в бухгалтерском программном обеспечении. Вредоносные программы затем распространялись самостоятельно и на многие другие компании, которые также использовали упомянутое программное обеспечение. Наряду с предприятиями в Украине предприятия во многих других государствах были заражены этим вирусом. В результате заражения указанные системы перестали функционировать и в целом вышли из строя. После первоначального акта заражения вредоносная программа распространилась самостоятельно на другие уязвимые системы, даже за пределами уже зараженных компаний. Это свидетельствует о растущем техническом развитии вредоносных программ.

В итоге отдельные компании не смогли полностью восстановить свои ИТ-инфраструктуры в течение нескольких недель после атаки. Датская судоходная компания MAERSK и компания фрахтовых услуг TNT Express полагают, что понесенные ими убытки составили более 300 млн. долларов США. В целом ущерб, нанесенный вредоносным вирусом только в Европе, оценивается более чем в 1 миллиард евро.

Распространение описанного вредоносного программного обеспечения было направлено на уничтожение данных и блокирование/саботирование бизнес-процессов. Данный случай, таким образом, является актом киберсаботажа, что

[1] URL: https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-executive-summary-en.pdf (дата обращения: 12.04.2019).

подпадает под действие § 303b УК ФРГ. Однако на практике такие случаи фиксируются очень редко. Связано это с тем, что злоумышленники стараются разработать такую программу, которая длительное время не позволяла бы себя обнаружить. Кроме того, сами компании могут обращаться с тем или иным заявлением в правоохранительные органы спустя большое количество времени, а в расследовании цифровых преступлений именно время становится ключевым фактором. Все это осложняет деятельность органов полиции ФРГ по противодействию преступлениям в сфере цифровых инноваций. Тем не менее, такой подход немецкого правоприменителя позволяет приобрести тот ценный опыт, который позволит в будущем, при наличии законодательного регулирования криптосферы, с большей эффективность противодействовать криптопреступлениям.

Литература

1. Сидоренко Э.Л. Правовой статус криптовалют в Российской Федерации // Экономика. Налоги. Право. 2018. № 2. С. 129-137.
2. BGH 1 StR 412/16 - Beschluss vom 27. Juli 2017 (LG Kempten). URL: https://www.hrr-strafrecht.de/hrr/1/16/1-412-16.php.
3. Зигмунт О.А. Кибер- и Интернет-преступность в Германии и России: возможности сравнительного исследования // Юридическая наука и правоохранительная практика. № 4 (34). 2015. С. 180-188.
4. Кучеров И.И. Криптовалюта (идеи правовой идентификации и легитимации альтернативных платежных средств): монография. М., 2018. 204 с.
5. Печегин Д.А. Крипториски // Российский журнал правовых исследований. 2017. № 3. С. 151-157.
6. Талапина Э.В. Право и цифровизация: новые вызовы и перспективы // Журнал российского права. № 2. 2018. С. 5-17.
7. Хабриева Т.Я. Право перед вызовами цифровой реальности // Журнал российского права. № 9. 2018. С. 5-16.
8. Хабриева Т.Я., Черногор Н.Н. Право в условиях цифровой реальности // Журнал российского права. № 1. 2018. С. 85-102.
9. Brenig C., Accorsi R., Müller G. Economic Analysis of Cryptocurrency Backed Money Laundering // ECIS Completed Research Papers. 2015. Paper 20. URL: https://aisel.aisnet.org/ecis2015_cr/20/.
10. Bryans D. Bitcoin and Money Laundering: Mining for an Effective Solution // 89 Ind. L.J. 441. 2014. URL: https://ssrn.com/abstract=2317990.
11. Grzywotz J., Köhler O., Rückert C. Cybercrime mit Bitcoins – Straftaten mit virtuellen Währungen, deren Verfolgung und Prävention // StV. 2016. № 11. P. 753-759.

В.А. Прорвич

Особенности алгоритмов комплексного применения специальных знаний для выявления и расследования криминальных сделок с криптовалютой

Повышение эффективности борьбы с новыми криминальными проявлениями, характерными для информационного общества, требует выявления и пресечения источников их финансирования. При этом важно обратить внимание на то, что многие из этих источников финансирования также могут носить криминальный характер. То есть, речь может идти о своеобразных «цепных реакциях» преступлений различного вида, характерных для деятельности организованных групп и преступных сообществ. Более того, нередко выясняется международный характер источников финансирования таких преступных сообществ, а также явные признаки направляющей и организующей роли в деятельность таких сообществ иностранных центров.

Особую роль в быстром росте новых видов преступлений играют современные сетевые технологии формирования денежных потоков между экономическими субъектами различного вида и уровня. При этом у соответствующих субъектов возникают новые возможности для маскировки своей преступной деятельности и сокрытия источников ее финансирования с помощью современных информационных технологий, включая алгоритмы распределенного хранения и доступа к зашифрованной информации типа «блокчейн». Соответственно, новые задачи встают и перед правоохранительными органами, призванными выявлять признаки таких преступлений и осуществлять надлежащее расследование соответствующих уголовных дел.

Для осуществления эффективного контроля за применением технологии «блокчейн», а также более совершенных способов кодирования информации, ее распределенного хранения и авторизованного доступа, необходимы не только соответствующие технические и программные средства, но и правовое обеспечение соответствующей деятельности правоохранительных органов. В этой связи необходимо обратить внимание на постановление Пленума Верховного Суда Российской Федерации от 26 февраля 2019 г. № 1 «О внесении изменений в постановление пленума Верховного Суда РФ от 7 июля 2015 г. № 32 «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступных путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем»».

В опубликованных комментариях по поводу содержания данного Постановления отмечается, что его положения подводят под уголовное преследование покупку криптовалюты на «грязные», то есть, незаконно полученные деньги. Особая важность данного Постановления определяется тем, что в настоящее время правовой статус подобных «виртуальных» денег не определен. Не секрет, что реально различные виды криптовалюты уже не только существуют несколько лет, котируются на специализированных биржах и обмениваются на «реальные» денежные суммы на банковских счетах, а затем «обналичиваются», но и нередко используются преступниками, причем не только при совершении

финансовых или экономических преступлений. Все больше сведений приводится о применении криптовалют при организации незаконного оборота наркотических средств и психотропных веществ, финансировании экстремистских и террористических организаций.

Как экономисты, так и правоведы пока еще не определились в своем отношении к таким «цифровым» деньгам, поскольку соответствующего понятия нет ни в законодательстве о Центральном Банке, банках и банковской деятельности, ценных бумагах и других нормативных правовых актах, формирующих правовой фундамент российской денежной системы. А для введения понятия цифровых денег или криптовалюты необходимо не только осмыслить их содержательные особенности, но и внести многочисленные изменения и дополнения в действующее законодательство.

Пока что законодатель сделал лишь первую попытку в данном направлении, введя Федеральным законом от 23 апреля 2018 г. № 111-ФЗ новую редакцию ч. 3 ст. 159^6 УК РФ, предусматривающей уголовную ответственность за хищение с чужого банковского счета, а равно в отношении электронных денежных средств путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации.

При этом во многих странах мира такое законодательство не только активно создается, но и активно нарабатывается опыт его правоприменения. Более того, определенные виды из более, чем 2000 криптовалют, создаются не только некоторыми коммерческими банками, но и государственными. Подобные планы неоднократно озвучивали и многие руководители крупных российских банков, в том числе с государственным участием, а представители законотворческих органов в ближайшее время обещают представить на обсуждение соответствующие законопроекты.

Не дожидаясь внесения столь кардинальных изменений действующего законодательства, Пленум Верховного Суда РФ дал разъяснения о том, что «предметом преступлений, предусмотренных ст. 174 и 174.1 Уголовного кодекса РФ, могут выступать в том числе и денежные средства, преобразованные из виртуальных активов (криптовалюты), приобретенных в результате совершения преступления». При этом Пленум Верховного Суда не ставил цель дать определение понятия виртуальных активов, которого нет в российском законодательстве. Кроме того, данное постановление не приравнивает к преступлению операции по «обналичиванию» криптовалюты. Речь идет о том, что следствие обязано доказать, что с помощью таких операций производится легализация денег или имущества, полученных преступным путем.

Для получения необходимых доказательств следует учитывать, что для «обналичивания» криптовалюты (например, биткоинов) обычно используются биржи криптовалюты и посредники, имеющие как аккаунты в криптовалютных системах, так и обычные банковские счета с безналичными денежными средствами. Через таких посредников следствие может выйти на тех лиц, которые обратились к ним за помощью в обналичивании своей криптовалюты и выяснить у них, насколько легальными являются источники ее получения.

При обосновании сделанных разъяснений в данном Постановлении дается ряд ссылок на то, что международное сообщество, стремясь выработать эффективные меры по предупреждению транснациональной легализации (отмывания) денежных средств или иного имущества, добытых преступным путем, приняло ряд документов, к которым относятся конвенции Организации Объединенных Наций о борьбе против незаконного оборота наркотических средств и психотропных веществ от 20 декабря 1988 года, против транснациональной организованной преступности от 15 ноября 2000 года, против коррупции от 31 октября 2003 года, конвенции Совета Европы об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности от 8 ноября 1990 года, об уголовной ответственности за коррупцию от 27 января 1999 года и об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности и о финансировании терроризма от 16 мая 2005 года. Международным сообществом применяются стандарты в области противодействия отмыванию денег Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ).

Важно обратить внимание на то, что в рассматриваемом постановлении сделана специальная оговорка о том, что крупный или особо крупный размер деяния, предусмотренного статьями 174 и 174.1 УК РФ, определяется исходя из фактической стоимости имущества, составляющего предмет данных преступлений, на момент начала осуществления с ним финансовых операций или сделок, а в случае совершения нескольких финансовых операций или сделок – на момент совершения первой из них. При отсутствии данных о фактической стоимости имущества она может быть установлена на основании заключения специалиста или эксперта.

То есть, следователю необходимо найти таких специалистов и судебных экспертов, которые обладают специальными знаниями как в сфере криптовалют различного вида, включая характеристики соответствующих виртуальных активов, отраженных на аккаунтах держателей криптовалюты определенного вида, так и в соответствующих сферах экономики и финансов. При этом такие специалисты и судебные эксперты должны не только высказать свое мнение о рублевом эквиваленте определенного виртуального актива на аккаунте конкретного субъекта либо записи о конкретной сумме в криптовалюте определенного вида, но и указать в соответствующем заключении на использованную им экспертную методику. Соответствующее требование содержится в ст. 204 УПК РФ. Его выполнение связано, в том числе, с требованиями статей 87 и 88 УПК РФ о проверке и оценке заключения эксперта как доказательства по соответствующему уголовному делу.

Вполне естественно сделать вывод о том, что наиболее высокий уровень специальных знаний о различных особенностях преобразования различных видов криптовалюты в определенные суммы в рублях, евро или долларах, имеется как раз у тех самых посредников, которые занимаются соответствующими обменными операциями. Им хорошо известны и те «тонкости», которые характерны для организации и практической деятельности специализированных бирж криптовалюты. Вопрос лишь в том, насколько легально осуществляется их дея-

тельность и насколько легитимными посчитают выводы таких специалистов и экспертов следователь, а затем прокурор и суд.

Вместе с тем, осуществляя обмен виртуального актива, который фактически дает его владельцу право получения определенного набора сетевых информационных услуг, получившего условное название «криптовалюта» на рубли или другой вид «реальной» валюты, фактически биржевой посредник устанавливает его денежный эквивалент. Поскольку этот «эквивалент» устанавливается на бирже криптовалюты в рамках «рыночных» сделок, то многие авторы используют такие понятия, как «рыночная стоимость» криптовалюты, ее «рыночные котировки» или «рыночный курс».

Однако более глубокий анализ приведенных выше «рыночных» понятий показывает, что они установлены в рамках действующего законодательства. К примеру, понятие «рыночная стоимость» определенного объекта установлена ст. 3 Федерального закона «Об оценочной деятельности в Российской Федерации» № 135-ФЗ в действующей редакции как «наиболее вероятная цена отчуждения объекта оценки на открытом рынке, в условиях конкуренции, когда на свободу действий участников сделки не влияют особые обстоятельства…». То есть, на «открытом рынке» биржи криптовалют должно происходить отчуждение определенного объекта, который в рассматриваемом постановлении Пленума Верховного Суда Российской Федерации от 26 февраля 2019 г. № 1 определен как «виртуальный актив».

Как уже отмечалось выше, Пленум Верховного Суда РФ не дал определения понятию «виртуальный актив», фактически оставив его на усмотрение следователей и судебных экспертов, как и установление размера стоимости этого «актива» в рамках преступлений рассматриваемого вида. То есть, ряд сложнейших вопросов, связанных с толкованием положений уголовного, гражданского, финансового и иного специального законодательства оставлены на усмотрение самих следователей, а также привлекаемых ими экспертов и специалистов. При этом нельзя забывать и о том, что особенности правоотношений участников подобных сделок определяют и содержательные особенности формирования рыночной стоимости предмета конкретной сделки. А предметом сделок рассматриваемого вида является сложная совокупность информационно-сетевых услуг определенного состава и объема.

Соответственно, без использования специальных знаний в различных отраслях права, экономики и информатики судебный эксперт вряд ли сможет провести необходимые исследования для решения соответствующих экспертных задач, поставленных перед ним следователем или судом. Но далеко не каждый эксперт-экономист или специалист по компьютерно-технической экспертизе могут решать соответствующие экспертные задачи, даже в рамках комплексных судебных экспертиз совместно со своими коллегами.

Поэтому необходимо выявить наиболее сложные проблемы, связанные с постановкой соответствующих экспертных задач, а также с разработкой общих и частных экспертных методик, позволяющих выполнять необходимые исследования и формировать обоснованные выводы по поставленным вопросам. Для этого необходимо, прежде всего, выяснить ряд особенностей формирования

указанных «виртуальных активов», их назначения, определяющего ценность данных активов для определенного круга пользователей, а также особенности подготовки и совершения сделок между ними.

Несмотря на то, что Пленум Верховного Суда РФ в указанном Постановлении не счел возможным дать определение понятию «виртуальный актив» применительно к криптовалюте, участники биржи криптовалют понимают, о чем идет речь. Безусловно, различные субъекты проявляют при этом большую или меньшую глубину понимания всех тонкостей структуры данных активов. Более того, многих из них эти тонкости и не интересуют, поскольку данные субъекты заинтересованы лишь в получении дополнительного дохода от биржевых сделок с такими активами.

Но при всех оговорках, большинство субъектов, участвующих в «рыночных» сделках по обмену виртуальными активами, понимают, что данные активы связаны с возможностью получения определенного набора информационных сетевых услуг конкретного содержания и объема. Ведь именно с необходимостью установления определенного эквивалента «стоимости» оказания подобного рода взаимных услуг столкнулись участники создания принципиально новой системы сетевых транзакций на основе технологии «блокчейн». И эта необходимость фактически стала одним из важнейших побудительных мотивов создания первых видов криптовалют.

Таким образом, субъекты описываемых сделок, обмениваясь эквивалентными, на их взгляд, виртуальными активами, каждый из которых позволяет получить определенный набор сетевых информационно-технологических услуг, фактически достигают взаимного соглашения об их эквивалентности. Но при этом неизбежно возникает ряд вопросов о том, каким образом разрешаются конфликтные ситуации между данными субъектами, кто выступает «третейским судьей» в таких конфликтах и на каком основании, а также по каким критериям им разрешаются конфликты подобного рода.

Изучение соответствующих публикаций показывает, что субъекты подобных сделок стараются достигнуть взаимной договоренности без привлечения юристов и огласки встречных претензий. То есть, фактически возникает новая сфере общественных отношений в информационном обществе, правовое регулирование которой осуществляется вне рамок государственной правовой системы. Но правовое регулирование определенной части общественных отношений, включая разрешение споров, не по закону, а «по понятиям», пусть даже самых честных и интеллектуально продвинутых программистов, неизбежно привлечет к ней внимание криминала. Поэтому многие ученые и специалисты обращают внимание на значительный уровень рисков возникновения новых, высококриминальных сегментов теневой экономики.

Попытки формализовать подобные сделки по обмену виртуальными активами, «эквивалентными» по неформальным договоренностям участников таких сделок, на основе положений действующего законодательства, «высвечивают» ряд проблем следующего характера. Прежде всего, каждая из таких сделок по обмену виртуальными активами может рассматриваться как две «встречные» сделки

купли-продажи. Именно такое толкование содержания договора мены отражено в ст.567 ГК РФ.

Фактически в рамках первой сделки право на виртуальный актив, связанный с правом на неопределенное количество неизвестных услуг, которые могут быть связаны с «грязными» деньгами или имуществом, полученным преступным путем, должно переходить к его новому владельцу в обмен на определенную сумму денег. Но на самом деле оно обменивается на право получения определенного набора конкретных сетевых информационных услуг, получившего условное название «криптовалюта», имеющего определенный денежный эквивалент, установленный на бирже криптовалюты. А в рамках второй сделки происходит переход права на конкретный набор сетевых информационных услуг, условно называемый криптовалютой и имеющий определенный денежный эквивалент, на виртуальный актив, связанный с неопределенным набором сетевых информационных услуг, а также с имуществом, полученным преступным путем.

То есть, в рамках каждой из встречных сделок купли-продажи участвуют такие виды виртуальных активов, один из которых имеет денежный эквивалент, а второй – не имеет. Формально, эта пара встречных транзакций должна формировать эквивалент в виде даже не денежного суррогата, а «квазиденежного» суррогата, и создавать определенное представление о возможной «стоимостной» характеристике виртуального актива, связанного с неопределенным набором сетевых информационных услуг. Вместе с тем, как уже отмечалось выше, в соответствии с Федеральным законом «Об оценочной деятельности в Российской Федерации» рыночная стоимость любого объекта определяется наиболее вероятной ценой его отчуждения на открытом рынке. При этом предложение данного объекта участникам рынка осуществляется в виде публичной оферты, в которой описываются характеристики данного объекта, представляющего интерес для неопределенного количества потенциальных покупателей.

Применение этих определений к виртуальным активам, вовлекаемым в две встречных сделки купли-продажи, показывает, что ни первая, ни вторая из этих встречных сделок не соответствует указанным требованиям действующего законодательства. Прежде всего, в каждую из них вовлекаются весьма необычные, виртуальные активы, правовой статус которых, не говоря уже об их количественных и качественных характеристиках, не определены. В то же время, второй из данных виртуальных активов, как уже отмечалось выше, дает право его владельцу на получение определенного набора сетевых информационных услуг. Подобные виртуальные активы, получившие условное название «криптовалюта», участвуют в сделках на бирже криптовалюты, в результате совершения которых приобретают определенный денежный эквивалент.

Такие сделки на биржах криптовалюты законодателем не регламентированы, но и не криминализованы. Это подтверждено и уже указанным выше постановлением Пленума Верховного Суда РФ от 26 февраля 2019 г. № 1. То есть, и законодатель, и правоприменитель признают необходимость введения в рыночный оборот криптовалюты, но полного понимания того, как это лучше всего сделать, пока еще нет. Периодически в прессе появляются сообщения, что вскоре будут подготовлены проекты законов о цифровой экономике, о криптовалюте и других нормативных

правовых актов, регламентирующих порядок формирования и совершения сделок по отчуждению виртуальных активов. Но даже концептуальные основы этих законопроектов, не говоря уже о каких-либо деталях на широкое обсуждение юридического сообщества, пока еще не выносились.

Что же касается первого из виртуальных активов, вовлеченного в рассматриваемые встречные сделки, то кроме отмеченных выше правовых и правоприменительных неопределенностей, здесь возникает еще ряд проблем, связанных с криминализацией процесса его обмена на виртуальный актив, связанный с криптовалютой. Прежде всего, поскольку речь идет о криминализации подобных сделок, то и сам этот виртуальный актив признается Пленумом Верховного Суда РФ криминальным. Вполне естественно, что это вызывает ряд связанных с этим новых вопросов о том, кем, когда, каким образом и для каких целей был сформирован данный актив, а также каким образом он связан с «грязными» деньгами либо имуществом, полученным преступным путем, поскольку обмен его на криптовалюту квалифицируется Пленумом ВС РФ, как преступление, предусмотренное ст. 174 и 174.1 УК РФ.

Вполне возможно, что после принятия упоминавшихся выше готовящихся законопроектов о цифровой экономике, криптовалюте и т. д., можно будет уточнить те признаки, на основе которых можно будет идентифицировать данные виды виртуальных активов, как криминальные. Однако рассматриваемое постановление Пленума ВС РФ ориентирует на правоприменение по тем преступлениям, которые выявляются уже сегодня, и по которым возбуждаются и расследуются уголовные дела. При этом все проблемы идентификации важнейших признаков подобных виртуальных активов и установления размера причиненного ущерба приходится решать следователю. В решении многих из них значительную помощь могут оказать специалисты и судебные эксперты, обладающие необходимыми специальными знаниями.

Понятно, что во избежание следственных и экспертных ошибок необходимо найти таких специалистов и судебных экспертов, которые могут не только выполнить соответствующие расчеты, опираясь на «рыночные» котировки криптовалюты определенного вида на определенной специализированной бирже на определенную дату. Эти эксперты должны обладать и специальными правовыми знаниями, позволяющими раскрыть сущностные характеристики транзакций финансового характера с помощью криптовалюты. В свою очередь, для этого необходимо учитывать и основные правовые особенности формирования системы активов, используемых при создании криптовалют.

Исходя из рассмотренных выше особенностей совершения двух встречных сделок купли-продажи виртуальных активов различного вида в рамках их мены, когда один из данных активов имеет признанный судом денежный эквивалент, можно выстроить следующую цепочку событий, происходивших «в обратном порядке». Определенная денежная сумма, полученная на бирже криптовалюты с участием официально зарегистрированного на ней посредника, – виртуальный актив, который дает право его владельцу на получение определенного набора сетевых информационных услуг, и имеет определенный эквивалент в криптовалюте, – виртуальный актив, связанный с неопределенным набором сете-

вых информационных услуг, который может быть связан с криминальными сделками заинтересованных лиц, – определенные виды имущества или прав на имущество, полученные преступным путем либо в результате преступления и вовлеченные в незаконные операции по легализации данного имущества, предусмотренные ст. 174 и 174.1 УК РФ.

Первое звено рассмотренной цепочки транзакций, связанное с обменом на определенную денежную сумму виртуального актива, связанного с криптовалютой, осуществляется с участием посредников специализированных бирж криптовалюты. Кроме того, данные посредники могут обладать определенными сведениями и о втором звене данной цепочки транзакций, связанным с обменом формализованного виртуального актива, имеющего определенный эквивалент в криптовалюте, с неформализованным виртуальным активом, который может быть связан с криминальными сделками заинтересованных лиц. Несмотря на то, что данные виртуальные активы формируются с помощью технологии блокчейн, с помощью данного посредника следователь может получить важные сведения для выявления признаков преступлений рассматриваемого вида.

Соответствующие технологии достаточно сложны, поэтому для их разработки и применения в интересах следствия необходимы специальные исследования с привлечением ведущих ученых – как в сфере информатики и нейропрограммирования, так и в различных сферах юридических и экономических наук. Подобные исследования и разработки, связанные с применением нейросетевых алгоритмов, включая «многослойный оверлей», начались автором и его коллегами применительно к проблемам формирования и оценки активов иного характера более 20 лет назад[1]. Их результаты показали, что для организации таких комплексных, «межнаучных» исследований необходимы серьезные усилия на различных уровнях, обсуждение которых выходит за рамки настоящей работы.

Ф.К. Свободный

Психологические факторы привлекательности криптовалют как средства финансовых расчетов

Аннотация. В статье исследуются психологические детерминанты привлекательности криптовалют для граждан. Основываясь на результатах анализа интернет-публикаций, выделяются такие факторы привлекательности как «Прибыль», «Безопасность», «Удобство». Раскрывается содержание каждого фактора. Указывается на необходимость учета психологических факторов привлекательности криптовалют для действенной правовой регуляции этой сферы общественных отношений.

Ключевые слова: криптовалюта, привлекательность, психологические факторы, прибыль, безопасность, удобство.

[1] Прорвич В.А. Оценка земли в Москве. М.: Экономика, 1996; Атлас оценки земель Москвы. / Под ред. В.А. Прорвича. М.: Экономика, 1999; Прорвич В.А. Стандартизация оценки недвижимого имущества. М.: 2006.

Активное развитие процессов компьютеризации и информатизации современно общества оказало огромное влияние на банковские системы мировых держав, и в первую очередь, - на механизмы осуществления финансовых расчетов безналичным способом. Появились технологии дистанционного банковского обслуживания, стало возможным использование электронных платежных систем, а также цифровых валют, самой известной из которых сейчас является криптовалюта[1]. В современном обществе увлечение криптовалютами распространяется с большой скоростью: если ещё в начале 2010 годов цифровыми валютами интересовались лишь отдельные специалисты из сферы высоких технологий, то уже к 2017 году в мире насчитывалось более 150-ти только официально зарегистрированных криптовалютных компаний[2]. Не осталась в стороне от использования криптовалют и Россия, где, так же, как и во всем мире, наряду с положительными результатами информатизации финансово-кредитной системы отмечается и ряд серьезных негативных моментов, связанных, прежде всего с расширяющийся практикой использования криптовалют в преступных целях. Криптовалюты уже стали эффективным средством финансовых расчетов в сфере незаконного оборота наркотических средств, психотропных и психоактивных веществ, оружия и взрывчатых веществ и т.п. При помощи «виртуальных денег» осуществляется финансирования проституции, террористической и экстремистской деятельности, подделки документов, распространения порнографии и др.[3].

Эффективное и своевременное расследование преступлений, связанных с оборотом криптовалюты, невозможно без соответствующих специальных знаний. Бычков В.В. и Вехов В.Б. акцентируют внимание на необходимости использования в процессе раскрытия вышеуказанных преступлений специальных знаний в сфере компьютерной информации, криптографии, электронных платежных средств и систем[4].

По-нашему мнению, эффективное противодействие использованию криптовалют в противоправных целях невозможно и без учета психологических детерминант этого явления, обусловленных, прежде всего, особенностями потребностно-мотивационной сферы личности современного человека.

Привлекательность криптовалют обусловлена, прежде всего, гедонистической направленностью психологи человека, выраженной в известной поговорке: «хочу, чтобы у меня все было, а мне за это ничего не было». И хотя «принципом стремления к удовольствию» можно объяснить большинство проявлений жизнедеятельности, в каждой конкретной ситуации необходима конкретизация психологических детерминант поведения личности.

---

[1] Подробнее см.: Crypto Currency // Forbes. 20.04.2011. URL: https://www.forbes.com.

[2] Подробнее см.: *Global Cryptocurrency Benchmarking Study.* URL: https://www.jbs.cam.ac.uk.

[3] Совещание в Генеральной прокуратуре РФ по вопросам правомерности использования анонимных платежных систем и криптовалют. URL: http://www.genproc.gov.ru/smi/news/genproc/news86432/ (дата обращения: 05.04.2019).

[4] Бычков В.В., Вехов В.Б. Специальные знания, обеспечивающие расследование преступлений, связанных с оборотом криптовалюты // Российский следователь №2 – 2018. С. 8-11.

Для выявления комплекса психологических факторов, обуславливающих привлекательность криптовалют для граждан, нами было проведено исследования включающее в себя анализ публикаций по данной проблематике, представленных в Интернет. Изучались публикации научного характера, рекламные статьи, высказывания на форумах некоторых сайтов. Общее количество анализируемых источников информации составило 32 единицы. В процессе анализа в тестах исследуемых источников выделялись смысловые единицы текста, на основании которых можно было судить о репрезентируемых достоинствах криптовалют как средства финансовых расчетов. Выявленные смысловые единицы анализировались и классифицировались, по критерию мотивационного воздействия на потенциального пользователя криптовалюты.

По результатам проведенного исследования нами были выделена система психологических факторов привлекательности криптовалюты для граждан. В общем виде данная система позиционирована в пространстве трехфакторной модели, векторами которой являются такие факторы, как: «Прибыль», «Безопасность» и «Удобство».

Рассмотрим содержание каждого из указанных факторов более подробно.

Фактор «Прибыль (обогащение)» представлен следующими составляющими:

- возможность получения прибыли без тяжелого, интенсивного, постоянного труда;
- возможность получения сверх прибыли из-за быстрого роста курса обмена крипровалюты;
- возможность постоянного умножения капитала путем автоматической «добычи» криповалюты: майнинг, форжинг;
- отсутствие налогообложения на прибыль;
- отсутствие необходимости оплачивать обязательное посредничество при производстве расчетов.

В первую очередь, по-нашему мнению, криптовалюта сегодня привлекательна для граждан возможностью получения сверхприбыли без существенных материальных, интеллектуальных и физических вложений. Прибыль может достигать более 1000% годовых. Если В 2009 году за 1 000 BTC (Bitcoin –самая популярная на сегодня «электронная монета») давали 0,004$, то уже в 2017 году за 1 BTC давали 19000 $. Рост курса меньше чем за 10 лет составил 4 750 000 000 %. В отличие от «обычных» акций, например, Газпрома, Сбербанка и т.д., курс которых за короткий промежуток времени меняется в пределах 3-5%, курс «криптоденег» может за несколько дней вырасти на 100-150%. Таким образом, вкладывая деньги в криптовалюты люди прежде всего стремятся получить сверхприбыль.

При этом, прибыль от криптовалюты можно добывать не только с помощью «игре на курсе» при операциях покупки-продажи, но и с помощью прямой, постоянной, автоматической (т.е. без участия человека) добычи – майнинга, форжинга и т.д. Майнинг криптовалюты – это генерация новых монет компьютерами, которая осуществляется в процессе выполнения математических расчетов хеш-функций для осуществления транзакций узлами криптовалютной сети. Начать майнинг криптовалют свободно может начать любой человек для этого

необходимо обзавестись «криптофермой» - системой программных и аппаратных средств, которые используются для добычи криптовалютных единиц. Майнинг криптовалют – прямая реализация возможности получения «денег из воздуха» (точнее из электричества), которая всегда привлекала многих граждан.

Прибыльность криптовалюты обусловлена и самой организацией архитекторы компьютерной сети расчтетов, ппостроенной по принципу P2P. Суть данной сети в том, что все операции совершаются между пользователями без посредников, в отличии от привычной финансовой системы, где без посредника, который организует процесс транзакций (и получает за это определенную прибыль от всех совершаемых операций) просто не обойтись.

При использовании криптовалюты все транзакции проходят между конкретными людьми. Необходимость в каком-то посреднике между ними просто отсутствует. Как отсутствует и необходимость производить комиссионные отчисления в пользу посредника за предоставляемые им услуги по организации расчетов.

На прибыльность криптовалюты положительно влияет и тот факт, что криптовалюта, в силу анонимности расчетов и несовершенства законодательства не подлежит налогообложению со стороны государства.

Вторым фактором привлекательности криптовалют является, по-нашему мнению, фактор «Безопасность». Данный фактор представлен следующими компонентами:

- анонимность владельцев криптовалют и участников сделок ними;
- отсутствие контроля за транзакциями со стороны других лиц, организаций и государства;
- отсутствие риска потерять деньги при осуществлении транзакций.

Анонимность владельцев криптовалют и участников сделок ними наиболее весомый фактор привлекательности криптовалюты. Сама идею криптовалюты родилась из необходимости совершать анонимные финансовые транзакции. И сейчас миллионы пользователей криптовалют признаются, что их больше всего привлекает такое качество цифровых валют, как способность обеспечить анонимность участников транзакций. Общеизвестно, что анонимность позволяет избегать ответственности за свои действия (в том числе и за действия противозаконные), обеспечивая гражданам желаемый уровень безопасности.

Привлекательность криптовалюты с точки зрения безопасности пользователя обеспечивается децентрализованным характером криптовалюты. Криптографическая система представляет собой обширную сеть компьютеров, которые взаимодействуют между собой. При этом, отсутствует элемент, отказ работы которого мог бы привести к отказу всей системы. Если в каком-то одном компьютере (узле сети) произойдет сбой, сеть все равно продолжит работать. Децентрализация защищает пользователя криптовалюты от риска потерять деньги при осуществлении транзакций как из-за сбоя в работе оборудования, так и из-за решения участника сделки в одностороннем порядке отменить транзакцию или принудительно вернуть деньги.

Механизм децентрализации также делает невозможным осуществление контроля за транзакциями со стороны других лиц, организаций и государственных

органов, что в купе с вышеобозначенной анонимностью делает криптовалюты еще более привлекательными для пользователей.

Третьим психологическим фактором привлекательности криптовалют является фактор «Удобство». Данный фактор складывается из следующих компонентов:

- легкость осуществления финансовых операций и получения криптовалюты;
- быстрая скорость осуществления транзакций;
- отсутствие необходимости согласования транзакций с государственными органами.

Криптовалюта привлекает граждан своей легкодоступностью: для получения криптовалюты и осуществления расчётов в ней необходимы только компьютер со специальной программой и доступ к сети интернет. При этом добывать и использовать криптовалюты может каждый желающий, без каких-либо ограничений.

Удобство использования криптовалют обуславливается также высокой скорость осуществления внутрисетевых транзакций, и небольшими временными затратами на весь процесс сделки по схеме «реклама-деньги-товар» в целом.

Определенное удобство для пользователей представляет и тот факт, что для криптовалют не имеют значения национальные, территориальные и государственные границы: расчеты в криптовалюте можно осуществлять как внутри страны, так и по всему миру. При этом транзакции не нужно согласовывать с государственными органами, получать разрешение на их осуществление, отчитываться за их проведение и т.д. Более того: при наличии элементарных навыков создать цифровую валюту может любой человек, поскольку многие из криптовалютних имеют открытый исходный код. Чтобы создать или модернизировать такую валюту, не нужно получать разрешение от какого-то органа и, теоретически, каждый человек может создать собственные уникальные «цифровые деньги» и использовать их для финансовых расчетов.

Подытоживая вышесказанное, констатируем высокую привлекательность для граждан криптовалют, обусловленную, прежде всего, согласованной системой психологических факторов. В связи с этим, представляется, что использование только запретительных мер в урегулировании использования гражданами криптовалют будет низкоэффективным. Для действенной регуляции этой новой сферы общественных отношений необходим комплексный подход, предусматривающий учет (и, возможно, нивелирование) психологических факторов привлекательности криптовалют как средства финансовых расчетов и получения прибыли.

О.В. Тушканова

Законодательное регулирование «криптовалют» – мифы и заблуждения

В последние годы проведено немало конференций, семинаров, совещаний и форумов, посвященных осмыслению таких понятий как «блокчейн» и «криптовалюта». В зависимости от профессионального состава участников – программистов и криптографов, банкиров и экономистов, юристов и правоведов существенно изменяется и уровень дискуссии. Если в аудиториях, состоящих из технических специалистов, достаточно давно перестали обсуждать, как устроена технология блокчейн, что такое биткойн, токен, смарт-контракт, ICO и проч., а все выступления посвящаются способам использования технологий распределенных реестров и цифровых активов в государственном управлении, бизнесе, правоприменительной деятельности и т.д., то юристы достаточно часто ведут свои дискуссии на уровне: «что это такое не знаю, но мнение имею», употребляя на трибуне термины «биткойн» и «блокчейн» как синонимы. К сожалению, попытки законодательного регулирования объективно существующих явлений и процессов, без понимания их сущности, не могут привести к хорошему результату.

Основным вопросом, по которому в юридическом сообществе ведутся дискуссии, является: «Как государство должно относиться к криптовалюте?» Мнения меняются от «давайте ее запретим» и «давайте не будем ее признавать» до «давайте ее признаем» или «давайте выпустим свою криптовалюту и посмотрим, что из этого получится». Необходимо отметить, что попытаться запретить можно все, даже восход солнца, но само по себе явление от этого существовать не перестанет, а непризнание «биткойна» приведет к невозможности ареста или конфискации имущества, полученного в результате совершения преступления, признание же влечет необходимость создания понятийного аппарата.

Так, научными и практическими работниками подобран ряд понятий, из которых законодатель пытается выбрать аналог понятию «криптовалюта»: «деньги», «денежные суррогаты», «валюта», «цифровая валюта», «товар», «цифровой товар», «платежное средство», «инвестиционный инструмент», «финансовый актив», «цифровой актив», «криптоактив», «цифровое право» и проч. При этом ситуация с «криптовалютой» все больше напоминает притчу о том, как слепцы пытались понять, что собой представляет слон, ощупывая лишь одну из частей его тела. Это происходит потому, что в понятие «криптовалюта» в настоящее время включают такие абсолютно разнородные сущности как биткойны, эфир, токены, предметы и внутреннюю «валюту» в компьютерных играх и проч., имеющие одну общую основу – цифровое представление, которое адекватно интерпретируется при наличии соответствующего программного обеспечения. Однако для каждой такой сущности существует свой аналог. Так, у понятия «биткойн» много общего с понятием «полезное ископаемое, «токен в ICO» подобен «акции», «предмет в on-line игре» – «товару» и т.п. Понятие «государственная криптовалюта» (эмиссией денежных средств занимается государство, хранение информации о платежных операциях организовано по блокчейн-

технологии) более всего соответствует «фиатным деньгам», поскольку возможность их независимой «добычи» («майнинга») отсутствует. Поэтому представляется, что законодательно нужно определять не один термин «криптовалюта», а несколько различных сущностей, имеющих цифровую природу (появление цифровой среды не привело к появлению абсолютно новых понятий, а лишь спроецировало на нее существующие предметы, явления и процессы).

Важно не запретить незапрещаемое, а законодательно определиться, как с понятийным аппаратом (что и в качестве чего признаем), так и отношением государства к цифровым сущностям: защищаем или не защищаем от преступных посягательств, наказываем или нет за их создание, приобретение, использование и т.п., подвергаем ли налогообложению и что именно («майнинг», обменные операции, прибыль от инвестиций в ICO и проч.).

Одним из важнейших условий обеспечения законности в процессе судопроизводства является возмещения вреда, причиненного преступлением. Если вред является имущественным, то в целях его возмещения на имущество накладывается арест, а в дальнейшем поводится его конфискация. Поэтому необходимо продумать порядок осуществления таких процедур как наложение ареста и конфискация для «криптовалюты». Необходимо отметить, что порядок наложения ареста для каждого ее вида должен быть своим. Поскольку информация, с помощью которой владелец управляет принадлежащими ему «биткойнами», может находиться одновременно на разных носителях и в разных компьютерных устройствах, то для ареста «биткоинов» недостаточно просто записать номер соответствующего кошелька и пароль доступа к нему, или изъять носитель информации (средство вычислительной техники), на котором находятся указанные сведения. Нужно предусмотреть создание аналогичного ресурса следственного органа и при принятии решения об аресте перевести «биткойны» из «кошелька» владельца в «кошелек» следственного органа. В случае отмены ареста, наложенного на имущество, эта операция может быть совершена в обратном порядке. В зависимости от получателя конфискованного имущества (в доход государства или потерпевшему), «биткойны» из «кошелька» следственного органа должны быть переведены либо на соответствующий ресурс Центрального банка Российской Федерации, либо потерпевшему (на аналогичный «кошелек» или путем конвертации в фиатные деньги через соответствующие обменные пункты).

До настоящего времени остаются открытыми вопросы о том, нужна ли судебная экспертиза «криптовалюты», если да, то в каких случаях, в рамках каких экспертных специальностей, а также какие вопросы должны ставиться перед экспертом. К сожалению приходится констатировать, что лица, обладающие правом назначать судебные экспертизы, в своем большинстве недостаточно хорошо разбираются в том, что собой представляет судебная экспертиза, и каким требованиям должны соответствовать выносимые на нее вопросы. Основным критерием правильной постановки вопроса является то, что для ответа на него необходимо провести исследование, а не высказать свое мнение, процитировать нормативный акт или справочник. Поэтому вызывает недоумение, когда эксперт в своем заключении объясняет, что собой представляет «биткойн», как

происходит его «майнинг», и что такое распределенный реестр. В то же время представляется необходимым при раскрытии и расследовании преступлений, использовать специальные знания в сфере обработки компьютерной информации (в рамках осмотров, исследований, судебных экспертиз) в целях поиска сведений о наличии и применении «кошельков» и «криптовалюты» (номеров, паролей, программного обеспечения, следов использования), а также аналитических экспертиз и исследований по извлечению из реестра информации о транзакциях по конкретным «кошелькам».

Э.М.Л. Тчибола

Налогообложение операций с криптовалютой: основные понятия и правовое регулирование

Аннотация. Продукты, основанные на технологии блокчейн, такие как криптовалюты и ICO (Initial Coin Offering), в настоящее время в России используют как крупн ые компании, так и физические лица. Однако до настоящего времени отсутствует должное правовое регулирование в данной области. В статье рассматриваются существующие проблемы в налогообложении операций с криптовалютами и пути их решения.

Ключевые слова: налогообложение, криптовалюта, правовое регулирование.

В России происходит активное внедрение инновационных технологий, что отражено в программе «Цифровая экономика Российской федерации». Продукты, основанные на технологии блокчейн, такие как криптовалюты и ICO (Initial Coin Offering), в настоящее время используют как крупные российские компании, так и физические лица. Однако до настоящего времени отсутствует должное правовое регулирование в данной области.

Цифровые технологии в финансовой области имеют перспективу и открывают новые возможности. Поэтому существует необходимость создания регуляторной среды, позволяющей систематизировать отношения в области использования криптовалют. В этой связи важным является рассмотрение международного опыта регулирования этой области и возможностей его применения в России.

Федеральная налоговая служба России распространила среди налоговых органов документ Минфина, где сообщила о том, что, невзирая на отсутствие законодательного регулирования цифровых денег в стране, пользователи обязаны платить налог с прибыли, полученный от сделок с криптовалютами.

На современном этапе в России порядок налогообложения таких операций еще не установлен. В документе предлагается следующее: до появления определенности в законодательстве ввести определенный налог в соответствии со статьей 220 Налогового кодекса Российской Федерации[1]. Это следует понимать как то, что физические лица должны будут самостоятельно определять сумму, которую они должны перечислить государству за осуществление опера-

ций с цифровыми деньгами, а кроме того, предоставить соответствующую декларацию.

То, что в законодательстве отсутствует правило о налогообложении сделок с применением криптовалюты, еще не означает, что соответствующие налоговые органы не могут рассчитывать на уплату налогов с таких сделок. Минфин неоднократно комментировал эту ситуацию, в т.ч. в недавнем письме от 17 мая 2018 г. № 03-04-07/33234 [2], и справедливо обращает внимание на то, что согласно ст. 41 Налогового кодекса РФ доходом для целей налогообложения называется любая экономическая выгода.

Ключевой вопрос, который состоит в том, по каким правилам будет определяться налоговая база, до сих пор не решен. В настоящее время в Налоговом кодексе нет специального регулирования, для того, чтобы иметь возможность корректно определить налоговые обязательства, возникающие после осуществления операций с криптовалютами. Таким образом, нужно исходить из экономической сущности самих криптовалют и совершаемых с их помощью сделок. В большинстве случаев можно признавать криптовалюту финансовым инструментом и, следовательно, применять уже присутствующие в налоговом законодательстве правила в отношении налогообложения сделок с применением производных финансовых инструментов.

Выявить доходы, полученные от операций с криптовалютами для налоговых органов сейчас в большинстве случаев, является весьма проблематичным, поэтому комментарии Минфина по этому вопросу вероятно будут подвергнуты критическому обсуждению. Однако, с точки зрения правильного налогообложения для добросовестного налогоплательщика такая позиция Минфина совершенно понятна и полностью следует из существующих положений налогового законодательства.

Депутаты Госдумы в первом чтении приняли пакет законопроектов о криптовалютах. По мнению экспертов, документы смогут принести ощутимую пользу в развитии отрасли в стране, но, все же, они требуют доработки.

В Швейцарии, где криптовалюта признана движимым имуществом, ее можно продать на бирже и получить деньги. Следовательно, там существуют официальные агенты продажи криптовалют, ведь с критовалютою возможны не только операции по майнингу, но и ее купля-продажа. Поэтому такую же логику можно применить в России. Ведь при совершении сделки на бирже, закон обязывает участников задекларировать доход и указать его источник.

Швейцария адаптировала свои налоговые правила для операций с криптовалютой. У них закон такой: если все движимое имущество – автомобили, яхты – стоит меньше 1 млн. франков, то не надо платить налог на богатство, если больше – необходимо платить.

Также и с криптовалютой – если владеешь ею более чем на 1 млн. франков, то нужно оплатить 0,3% в год.

В числе последних новаций в этой области можно назвать принятый в сентябре 2018 г. французский нормативно-правовой акт, который устанавливает правила для проведения ICO (Initial Coin Offering). Этот закон открывает новые возможности для инвесторов.

Управление по финансовым рынкам Франции (AMF) теперь может одобрять и выдавать разрешения тем компаниям, которые собираются проводить ICO во Франции, но только в том случае, когда эти проекты дают инвесторам гарантии. Эмитенты токенов должны предоставлять AMF полную информацию, что даст возможность покупателям быть осведомлёнными о тех решениях, которые связанны с проводимым ICO.

Стимулом принятия этого закона стала выраженная AMF обеспокоенность недостаточным регулированием токен-сейлов, что являлось фактором риска ICO, и повышало вероятность отмывания денег, денежных потерь и финансирования терроризма.

В России в конце декабря 2017 года Минфин и ЦБ подготовили законопроект о регулировании ICO [3]. Одним из ключевых достоинств данного законопроекта эксперты называют введение крипто-валютной терминологии в правовое поле. Приведем некоторые из определений и комментарии к ним ниже.

Цифровой финансовый актив – в это понятие включены, и криптовалюты, и токены. По тексту закона, все это является имуществом, и любой держатель должен удостоверить право собственности на актив в некоем «реестре цифровых транзакций». Далее по тексту законопроекта становится понятным, что данный реестр – это централизованная «систематизированная база цифровых транзакций». Вносить информацию о праве собственности в такой реестр должен Валидатор.

Интересно, что на данный момент в России не существует ни подобного реестра, ни валидаторов.

Майнинг – деятельность, направленная на создание криптовалюты [4]. По тексту закона майнеры бывают «домашние», которые не превышают лимиты энергопотребления, установленные правительством, и профессиональные, которым предстоит легализовать свою деятельность путем открытия компании или ИП.

Криптовалюта и токен признаны видом цифрового финансового актива.

Смарт-контракт является договором в электронной форме. Интересно, что всем инвесторам, решившим вложиться в ICO с российской юрисдикцией, придется подписывать с организаторами краудсейла контракт в электронной форме или бумажной.

Особенности выпуска токенов – с этой частью законопроекта необходимо внимательно ознакомиться тем, кто решил провести ICO в российской юрисдикции.

В законопроекте указано, что эмитент может выпускать токены и продавать их пользователям. При этом оговаривается, что выпускать токены одного вида может лишь один эмитент. Интересно, что неквалифицированные криптоинвесторы (на данный момент все пользователи криптовалют) смогут приобретать токены на сумму, установленную Банком России.

Отметим, что в предыдущей редакции законопроекта максимальная сумма, на которую можно было купить токены от одного эмитента, составляла 50 тысяч рублей. В новой редакции максимальная сумма не указана вовсе, поскольку Центробанк еще не определился с предполагаемым максимумом.

Стать эмитентом токенов, судя по тексту законопроекта, достаточно сложно, если не сказать, что невозможно. Во-первых, для выпуска токенов требуется очень внушительная документация, конечный состав которой даже не сформирован. Кроме этого, эмитент, как говорилось ранее, должен подписать отдельный договор с каждым покупателем токенов.

С полным списком действий, которые нужно совершить для выпуска токенов в российской юрисдикции, можно ознакомиться в третьей статье законопроекта.

Особенности обращения цифровых финансовых активов. Все владельцы криптовалют и токенов могут обменивать их на рубли или валюту исключительно «через оператора обмена цифровых финансовых активов». По большому счету, это значит, что теоретически должны появиться площадки, прошедшие со стороны регуляторов всевозможные проверки, и только на них пользователь сможет совершить обмен. Однако таких площадок пока нет.

При этом любые операции по обмену пользователь может совершать только после того, как откроет цифровой кошелек у оператора. Для этого он должен пройти процедуру идентификации в соответствии с Федеральным законом № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» [6].

Минфин предлагает ввести понятие цифрового финансового актива, под который будут подпадать криптовалюты и токены, и эти финансовые активы должны рассматриваться в первую очередь как «имущество» [5]. Такое определение позволит защищать права и иметь легальный оборот.

Стратегия, касающаяся развития электронной торговли, предусматривает большой спектр отношений, опосредованных через электронную форму и применяемых, и на внутреннем рынке России, и во время проведения трансграничных торговых операций в сегментах как розничной (B2C), так и оптовой (B2B) торговли.

Очевидно, что обязательным является развитие в Российской Федерации комплекса нормативно-правовых и организационных, а также технических условий, благоприятствующих стимулированию деловой активности всех участников электронной торговли, пропорциональному формированию конкурентной среды и созданию комфортного потребительского климата для всего населения.

Среди других фактов, можно отметить российский стартап, который на базе технологии распределенных реестров создал платформу для страховщиков. Инноваторы заявляют, что она позволяет сделать отрасль более прозрачной, стимулирует рост страхового рынка и снижает стоимость полисов на 30-40%. Эксперты также видят здесь потенциал, но предупреждают – на российском законодательном уровне еще не все вопросы урегулированы.

Технология блоковой цепи, или же блокчейн, появилась меньше 10 лет назад, однако, массовая аудитория узнала и заговорила о ней впервые после выхода криптовалюты биткоин на рынок, поскольку у этой системы есть много вариантов применения, как для интересов бизнеса, так и для государственных нужд.

Эксперты говорят о том, что у блокчейна впереди большое будущее, также и в области страхования. В частности, исследователи KPMG указывают, что при-

менение технологии распределенных реестров позволяет страховщикам повысить эффективность своей работы, понизить затраты на обработку транзакций, улучшить качество обслуживания клиентов, получать более достоверные данные, поднять на более высокий уровень отношения между покупателями полисов и страховщиками, и, как следствие, сделать страховой бизнес более «прозрачным» [6].

Кроме того, следует разработать такую нормативно-правую базу, которая определит допустимые способы защиты всех участников электронной торговли при участии их в электронной сделке.

Действующее гражданское законодательство, а также специальное законодательство об электронной подписи вводят нормативное определение и закрепляют правовую значимость электронного документа, устанавливая знак равенства между обменом электронными документами и письменной формой заключения сделок.

Целесообразно проведения усовершенствования законодательства, которое регулирует электронный документооборот как составную часть электронной сделки. Кроме того, для электронного документооборота необходимо специальное нормативно-правовое регулирование, в качестве составляющей в процедурах общего администрирования всего комплекса электронной торговли.

Отсутствие международных соглашений, которые определяют нормативное регулирование электронного документооборота при трансграничной электронной торговле, не дает возможности обеспечить юридическую значимость документооборота в целом между иностранными и российскими субъектами хозяйствования при осуществлении в электронном виде полного спектра торговых процедур.

Для устранения названных проблем следует детально проработать вопросы принятия отдельного федерального закона об электронном документе, создания законодательной и организационной основ осуществления трансграничного электронного документооборота.

Необходимо провести оценку всех возможных форматов применения в Российской Федерации зарубежной практики, в частности, это создание электронных платежных систем для электронных расчетов B2B, лицензированных Центральным банком РФ, в пределах национального рынка, а также в контексте трансграничной торговли.

Литература

1. Налоговый кодекс Российской Федерации (НК РФ) от 31 июля 1998 года №146-ФЗ с посл. изм. от 27.12.2018 №546-ФЗ.
2. Письмо ФНС России от 04.06.2018 N БС-4-11/10685@ «О порядке налогообложения доходов физических лиц» (вместе с Письмом Минфина России от 17.05.2018 N 03-04-07/33234)
3. Проект федерального закона «О цифровых финансовых активах» от 25.01.2018г. – [Электронный ресурс] – режим доступа:

4. Проект Федерального закона №419059-7 «О цифровых финансовых активах» от 20.03.2018г. – [Электронный ресурс] – режим доступа:http://www.consultant.ru/cons/cgi/online.cgi?req=doc;base=PRJ;n=170084#06072808324953984
5. Россия: парламентский «круглый стол» о криптовалютах – итоги и возможные последствия [Электронный ресурс] // ForkLog. – 04.06.2016. – https://forklog.com/rossiya-parlamentskij-kruglyj-stol-o-kriptovalyuta-itogi-i-vozmozhnye-posledstviya/
6. Федеральный закон «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» от 07.08.2001 №115-ФЗ – [Электронный ресурс] – режим доступа: http://www.consultant.ru/document/cons_doc_LAW_32834/

А.Н. Чаплинский

Виды преступлений, совершаемых с использованием биткоина, и методика их расследования

Аннотация. В условиях стремительного развития цифровой экономики использование в противоправных целях биткоина как наиболее популярной криптовалюты существенно затрудняет деятельность правоохранительных органов по противодействию преступности. Рассмотрены наиболее распространенные виды преступлений с использованием биткоина и рекомендации по их расследованию.

Ключевые слова: криптовалюта, биткоин, преступления с использованием биткоина.

Биткоин является крупнейшей в мире криптовалютой с капитализацией, превышающей более 90 млрд. долларов США. Популярность биткоина, в том числе при использовании в противоправных целях, предопределена возможностью круглосуточного осуществления транзакций, трансграничным характером, относительной закрытостью (анонимностью) переводов, децентрализованной эмиссией и др.

Практика использования криптовалют свидетельствует о том, что биткоин используется и как платежное средство для совершения противоправных действий, и как предмет преступного посягательства.

Как платежное средство биткоин хорошо зарекомендовал себя в пределах даркнета и постепенно стал валютой, которую выбирают для расчета при торговле наркотиками, поддельной валютой, скомпрометированными данными, включая платежные карты или учетные записи в онлайн-сервисах, вредоносным программным обеспечением, оружием и др. Кроме того биткоины выступают средством легализации доходов, полученных преступным путем. Несколько сервисов, включая биткоин-обменники, провайдеры биткоин-кошельков, микшеры и альтернативные валюты обеспечивают более высокую степень конфиденциальности при легализации доходов, полученных преступным путем. По нашему мнению, нецелесообразно отдельно выделять виды пре-

ступлений, где биткоин используется в качестве платежного средства, поскольку они будут аналогичны «традиционным» преступлениям с использованием фиатных денег.

Наиболее распространенными преступлениями, в которых биткоин выступает в качестве предмета преступного посягательства являются: 1) мошенничества посредством биткоин-миксеров; 2) распространение вредоносного программного обеспечения с требованием перечисления биткоинов за восстановление работоспособности; 3) хищения биткоинов.

Мошенничества, совершаемые биткоин-миксерами, как правило, работают в двоичном режиме, если депозит относительно мал - средства отмываются, но как только он достигает определенного порога - он забирается оператором миксера.

Одним из направлений криминального использования биткоинов является их оборот в качестве средства оплаты распространителям вредоносного программного обеспечения за восстановление работоспособности заблокированных посредством их применения компьютеров. Программы-вымогатели (блокировщики) поражают традиционные компьютерные устройства, в том числе серверы, а также мобильные телефоны, смарт-телевизоры и любые устройства, работающие на одной из основных операционных систем.

Хищение биткоинов осуществляется как правило путем распространения вредоносных программ. Обычно биткоин-пользователей атакуют троянские программы с дистанционным управлением, которые охотятся за их биткоин-кошельками, частными ключами или логинами для онлайн-сервисов, связанных с биткоином. Если файл кошелька не зашифрован или если даже вход заблокирован паролем, ничего не мешает злоумышленнику опустошить кошелек жертвы. Нередки кражи личного (закрытого) ключа жертвы. Вредоносные атаки буфера обмена - хорошо отлаженный вид преступлений, обычно используемый для замены хранящейся в буфере обмена URL-ссылки на вредоносные вебсайты. При атаках на биткоин-пользователей вредоносное ПО может обнаруживать биткоин-адрес, скопированный в буфер обмена, и заменять его закодированным биткоин-адресом, принадлежащим злоумышленнику. Это хитрый ход, так как вирусное ПО не требует пароль или сетевое сообщение обратно злоумышленнику. Более продвинутые версии вредоносного ПО содержат тысячи биткоин - адресов и автоматически выбирают тот, который ближе всего к предполагаемому получателю платежа.

Расследование преступлений с использованием биткоинов сопряжено с рядом сложностей, обусловленных особенностями функционирования системы блокчейн. Следует отметить, что до настоящего времени не существует универсальной методики расследования уголовных дел, связанных с использованием биткоинов. Вместе с тем практика расследования указанных преступлений позволяет дать ряд рекомендаций, призванных помочь правоохранительным органам в расследовании и поиску злоумышленников.

1. При расследовании в первую очередь необходимо проверить биткоин-адреса преступника, которые, как правило, известны потерпевшему при помощи поисковых систем. Нередки случаи, когда биткоин-адреса отображаются в

сообщениях, подписях или профилях участников онлайн-форумов, таких как *www. bitcointalk.org.* Анализ общедоступной информации, размещенной на данных ресурсах, позволяет получить сведения о человеке, который создал сообщение, включая его ник, контактные данные и списки всех сообщений вместе с отметками времени. Кроме того, администраторы могут запрашивать IP-журналы, сводки действий, личные сообщения и дополнительные данные о контакте.

2. Еще одним инструментом получения криминалистически важной информации является использование блокчейн-обозревателей. Начиная с 2009 года все биткоин-транзакции записываются в блокчейн - большую публичную базу данных, хранящую все данные в незашифрованном виде. Но блокчейн не хранится централизованно, а находится у тысячи частных лиц и компаний по всему миру, где работают биткоин-клиенты. Любой человек может загрузить файлы в блокчейн и попытаться проанализировать данные, импортировать их в базу данных или запросить их. Однако, поскольку это слишком громоздко, большинство следователей полагаются на общедоступные и свободные в использовании блокчейн- обозреватели. Блокчейн-обозреватель используется для запроса блокчейна и отображения результатов в удобном пользовательском интерфейсе. Существуют разные мнения о том, какой обозреватель лучше, но самым популярным является *www.blockchain.info.* Существует много других блокчейн-обозревателей, однако все они предоставляют пользователям идентичную информацию только в другом интерфейсе. Одним из исключений является *www.blocktrail.com*, который анализирует данные, размещенные на ресурсе *www.bitcoin.org* для метаданных, о которых можно узнать только, используя коммерческие сервисы.

3. Целью анализа и отслеживания биткоин-потока с одного биткоин-адреса на другой является установление связи между хотя бы одним адресом с реальным субъектом. В этом смысле полезным может быть ресурс www.walletexplorer.com. Следует иметь в виду, что информация, предоставляемая с помощью *walletexplorer* и схожими коммерческими сервисами, не содержит установочных данных лица, которому принадлежит биткоин-адрес, а содержит лишь сведения используемых объектах, таких как обменник, провайдер кошелька, платежный процессор, торговый или игровой сайт. В этом случае необходимо отправить запрос с целью получения более подробной информации об интересующем объекте. *www. walletexplorer.com* остается лучшим общедоступным ресурсом, который связывает несколько миллионов биткоин-адресов с кошельками, которыми управляют сотни крупнейших компаний.

4. С целью получения более полной информации целесообразно использование некоторых коммерческих инструментов для отслеживания биткоинов. Существует ряд коммерческих инструментов, которые можно использовать для отслеживания биткоин-транзакций и определения владельцев биткоин-адресов. К ним *относятся Chainalysis, Elliptic, Blockseer, Ciphertrace, Skry или Bitanalysis.* Эти сервисы предоставляют дополнительную информацию и удобство использования инструментов с открытым исходным кодом. По сравнению с *Walletexplorer* эти сервисы предлагают улучшенное обнаружение биткоин-

кошелька, больше биткоин-кошельков, связанных с владельцами и графическую визуализацию связей между кошельками. Некоторые сервисы также предоставляют дополнительную информацию по биткоин-адресам, собранную с веб-сайтов или сайтов даркнета.

5. В конечном итоге биткоины конвертируются в фиатные денежные средства. В связи с этим значительную роль в расследовании занимают биткоин-обменники. Именно биткоин-обменники содержат информацию об отдельных клиентах, их именах, подтвержденных контактных данных, IP-журналы, журналы активности, все биткоин-адреса и адреса других криптовалют, используемые биткоин-пользователем для обмена валют, отправки личных сообщений, платежных данных, удостоверения личности и подтверждения домашнего адреса.

6. Целью расследования преступлений, связанных с использованием биткоина является установление подозреваемых, их совершивших, а также восстановление биткоинов, которые были похищены или использованы для преступной деятельности. Существуют два основных способа изъятия биткоинов:

А) получение доступа к файлу *wallet.dat* подозреваемого в сочетании с паролем или поиском закрытого ключа или с ID-кошелька, как правило, в текстовом файле или распечатанном на бумаге;

Б) сотрудничество с представителями сторонних организаций, которые имеют доступ к биткоинам подозреваемого. При установлении факта хранения подозреваемым биткоинов на одной из онлайн-бирж (обменников) или кошельков, целесообразно направление соответствующего запроса о приостановлении операций по ним.

Следует отметить, что приведенный алгоритм поисковых мероприятий в сети Интернет прежде всего призван помочь правоохранительным органам в установлении лиц, причастных к совершению противоправных действий. Конкретный перечень следственных действий определяется следователем, исходя из фактических обстоятельств совершенного преступления.

Литература

1. Официальный интернет-портал Президента Республики Беларусь. Декрет № 8 от 21 декабря 2017 г. О развитии цифровой экономики http://president.gov.by/ru/official_documents_ru.
2. Филатова М.А. Анализ криптовалюты в мировой финансовой системе с позиции уголовного права (на примере Bittcoin) // Уголовное право в эпоху финансово-экономических перемен: материалы IX Российского конгресса уголовного права, Москва, 29-30 мая 2014 г. / Моск. гос. ун-т; редкол.: В.С.Комиссаров (отв. ред.) [и др.]. – М., 2014, с. 216-223.
3. Информационный бюллетень Следственного комитета Республики Беларусь № 2 (10), 2018 тема номера: «расследование уголовных дел о преступлениях в сфере информационных технологий» о практике расследования преступлений против информационной безопасности.

Т.В. Черемисина

О правовом статусе криптовалюты сквозь призму ее экономической сущности

Аннотация. В статье анализируется взаимосвязь права и экономики в эпоху цифровых денег и электронных кошельков. Исследуется правовой статус и экономическое значение криптовалюты, приведены различные определения понятия «криптовалюта» и высказывания ученых по данной проблеме. Предлагается законодательно закрепить термин «криптовалюта» и признать ее как возможным предметом преступления, так и средством его совершения.

Ключевые слова: криптовалюта, биткоин, объекты гражданских прав, экономика, право, преступность, хищение, взятка.

В 1999 году вышел в свет роман Нила Стивенсона «Криптономикон», в котором описано, как группа программистов-математиков пытается создать первую криптовалюту, преодолевая сопротивление правительств и крупных бизнес-структур[1].

И только через 10 лет, в 2009 году, появилась первая криптовалюта – биткоин. При этом проводить с ним финансовые операции стали спустя два года, когда появились электронные кошельки для хранения биткоина. Хотя информация о личности его создателя долгое время не афишировалась, сейчас им считается японец Натоси Накамото.

Что же представляет собой криптовалюта в экономическом и правовом смысле? Можно ли ею заменить фиатную валюту (выпускаемую государством-эмитентом, обеспечивающим ее номинальную стоимость)?

Криптовалюта (от англ. cryptocurrency) – это цифровые монеты (валюты), эмиссия и учет которых основаны на криптографических методах, а функционирование системы происходит децентрализованно в распределенной компьютерной сети. Как правило, криптовалюты защищены от подделки, могут храниться в электронных кошельках и переводиться между кошельками[2].

Сайт «Википедия» определяет криптовалюту как разновидность цифровой валюты, создание и контроль за которой базируются на криптографических методах, учет такой валюты децентрализован. Функционирование данных систем основано на технологии блокчейн, информация о транзакциях обычно не шифруется и доступна в открытом виде. Для неизменности базы цепочки блоков транзакций используются элементы криптографии (цифровая подпись на основе системы с открытым ключом, последовательное хеширование)[3].

---

[1] Neal Town Stephenson. Cryptonomicon, N.Y.: Avon Books, 1999 - 918 pp.

[2] Марамыгин М.С., Прокофьева Е.Н., Маркова А.А. Экономическая природа и проблемы использования виртуальных денег (криптовалют) // Известия УрГЭУ. 2015. № 2. С. 37-43.

[3] Сайт «Википедия». Режим доступа: https://ru.wikipedia.org.

Пленум Верховного Суда Российской Федерации от 07.07.2015 № 32 определяет криптовалюту как денежные средства, преобразованные из виртуальных активов[1].

Итак, если криптовалюта является средством платежа, то может ли она выполнять функцию денег в экономическом смысле и заменить их?

Чтобы разобраться в этом вопросе, рассмотрим, какие функции выполняет привычная валюта в каждой стране:

- мера стоимости – все товары и услуги, включая запрещенные в гражданском обороте, измеряются количеством денежных единиц, а не других товаров. Разнородные товары обмениваются на основании денежного выражения их стоимости. Также по показателю цены можно сравнивать разные товары. Денежная единица является эталоном для товаров. Физическое или юридическое лицо вправе самостоятельно определить стоимость своего товара и наименование единицы, в которой он реализует товар, например, биткоин;

- средство обращения – в обращении товаров деньги используются в качестве посредника. Их легко обменять на другой товар. Потребитель может приобрести товар за деньги, в любом населенном пункте страны проживания и за ее пределами. В настоящее время в интернет-среде криптовалюты можно обменять как на товары, так и на фиатные деньги;

- средство платежа. Деньги используются при регистрации и оплате долгов. Также эту функцию деньги выполняют при взаимодействии с финансовыми органами или, когда в них выражают финансовые показатели. В настоящее время Российская Федерация не признает использование криптовалюты как законного средства платежа;

- средство накопления. Неиспользованные деньги имеют свойство переносить в будущее покупательскую способность лица, не имея «срока годности». Если деньги не участвуют в обороте и их количество увеличивается, они выполняют функцию накопления. Покупательская способность денег зависит от инфляции. Криптовалюта активно аккумулируется на электронных кошельках владельцев. Различают «горячие» кошельки, когда работа с блокчейном происходит напрямую через Интернет, и «холодные», не требующими для операции с накоплениями постоянного доступа в Интернет и считающиеся более защищенными, чем «холодные»;

- мировые деньги. Воплощают в себе материализацию общественного богатства. Моментально конвертируясь из одной валюты в другую, деньги функционируют как всеобщее платежное и покупательное средство. Криптовалюта, для которой нет государственных границ, имеет все шансы стать универсальной валютой, не прибегая к услугам национальных банков и налоговых организаций.

[1] Постановление Пленума Верховного Суда РФ от 07.07.2015 № 32 (ред. от 26.02.2019) «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем».

Процесс эволюции денег на самом деле никогда не останавливался, и сегодняшние «виртуальные деньги» - лишь новая, но не последняя ее ступень.

В.А. Перов отождествляет криптовалюту с традиционной валютой, указывая, что виртуальная денежная единица отлична от привычной всем монеты только тем, что ее нельзя взять в руки. Виртуальная монета защищена от подделки, только не методом чеканки на ней определенного рисунка или символа, как на обычной монете, а методом шифрования, то есть сама «монета» представляет собой последовательность из зашифрованной информации, которую невозможно скопировать. В отличие от привычных на сегодняшний день денег, которые, прежде чем появиться на счету какого-либо лица или организации, должны быть кем-то эмитированы, то есть изготовлены и выпущены в оборот, криптовалюта эмитируется непосредственно в интернет-сети и никоим образом не связана с какой-либо имеющей хождение валютой или финансовой системой какого-либо государства[1].

Преимущества криптовалюты по сравнению с фиатными деньгами: открытость, возможность ее добычи любым пользователем при соблюдении определенных условий, анонимость операций.

В случае с криптовалютой доказательством наличия монеты в интернет-сети служит блокчейн, то есть определенного рода учетная запись, содержащая индивидуальную информацию каждой виртуальной монеты и также цепочки транзакций (операций), ею пройденных. Таким образом, созданная денежная единица может быть использована для оплаты товаров и услуг. Хранится данная валюта децентрализованно, то есть распределяется по электронным криптокошелькам пользователей интернет-сети[2].

Авторы статьи «Экономическая природа и проблемы использования виртуальных денег (криптовалют)» выделяют следующие особенности, предопределяющие весь процесс эволюционного развития денег:

- быстрая реакция на достижения научно-технического прогресса;
- увеличение скорости обращения денег и, как следствие, скорости проведения платежей.
- рост доступности инструментов платежа и контролируемости процесса перевода средств.

Кроме того, существуют два ограничивающих фактора: цена ускорения платежа (величина комиссий и прочих издержек на проведение выбранного способа расчетов) и безопасность платежа (стремление к минимизации риска потери средств во время расчетной сделки)[3].

Федеральный закон «О национальной платежной системе» от 27.06.2011 № 161-ФЗ определяет электронные деньги как предоплаченный финансовый продукт, который:

---

[1] Перов В.А. Выявление, квалификация и организация расследования преступлений, совершаемых с использованием криптовалюты: учеб.-методич.пособие – М.: Юрлитинформ, 2017. С 21.

[2] Там же. С. 22.

[3] Марамыгин М.С., Прокофьева Е.Н., Маркова А.А. Экономическая природа и проблемы использования виртуальных денег (криптовалют) // Известия УрГЭУ. 2015. № 2. С. 37-43.

- представляет собой денежное обязательство эмитента;

- выпускается после получения эмитентом денежных средств в размере, не меньшем выпускаемой стоимости;

- не требует использования при трансакции банковских счетов;

- принимается в качестве средства платежа экономическими субъектами иными, нежели эмитент;

- информация о размере денежной стоимости хранится в электронной форме на устройстве во владении держателя[1].

Итак, электронные деньги полностью моделируют деньги реальные. Относится ли к ним криптовалюта?

Под денежными средствами понимаются наличные денежные средства в валюте Российской Федерации или в иностранной валюте, а также безналичные денежные средства, в том числе электронные денежные средства, под иным имуществом - движимое и недвижимое имущество, имущественные права, документарные и бездокументарные ценные бумаги, а также имущество, полученное в результате переработки имущества, приобретенного преступным путем или в результате совершения преступления (например, объект недвижимости, построенный из стройматериалов, приобретенных преступным путем)[2].

Минфином России еще в 2018 году подготовлен проект Федерального закона «О цифровых финансовых активах», где указано, что цифровые финансовые активы, будучи объектами гражданских прав, не являются законным средством платежа на территории Российской Федерации. Тем не менее, законодатель относит к ним криптовалюту и токен. Вопрос определения стоимостного выражения криптовалют законодатель оставляет открытым[3].

Следовательно, на сегодняшний день биткоины, не являясь фиатной валютой, тем не менее, обладают всеми характеристиками денег и выполняют их функции.

Создает ли такое положение дел проблемы в уголовно-правовом поле? Да, криптовалюты стали часто использоваться и как средство для проведения анонимных операций по купле-продаже наркотических средств, легализации денежных средств или иного имущества, полученного преступным путем, получении (дачи) взятки. При этом, само понятие «криптовалюты» в уголовное законодательство до сих пор не введено.

Но постепенно объективная реальность стала изменять реальность правовую. В начале 2019 года внесены изменения в указанное выше постановление Пленума Верховного суда РФ «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным

---

[1] Федеральный закон «О национальной платежной системе» от 27.06.2011 № 161-ФЗ // Российская газета. № 139. 30.06.2011.

[2] Постановление Пленума Верховного Суда РФ от 07.07.2015 № 32 (ред. от 26.02.2019) «О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем.

[3] Проект Федерального закона № 419059-7 «О цифровых финансовых активах» (подготовлен Минфином России) // Режим доступа: http://sozd.duma.gov.ru/bill/419059-7/

путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем», которые можно рассматривать как шаг к признанию нефиатных инструментов обращения.

Так, статья 10 Постановления Пленума указывает, что обязательным признаком составов преступлений, предусмотренных статьями 174 и 174.1 УК РФ, следует понимать сокрытие преступного происхождения, местонахождения, размещения, движения имущества или прав на него. Такая цель может проявляться, в частности:

- в совершении финансовых операций или сделок с использованием электронных средств платежа, в том числе принадлежащих лицам, не осведомленным о преступном происхождении электронных денежных средств. Следовательно, суды, применяя данное положение на практике, приведут законодателя к признанию криптовалюты предметом преступления.

Кроме того, с 01.10.2019 вступит в силу новая редакция ст. 128 ГК РФ, и к объектам гражданских прав будут относиться вещи (включая наличные деньги и документарные ценные бумаги), иное имущество, в том числе имущественные права (включая безналичные денежные средства, бездокументарные ценные бумаги, цифровые права); результаты работ и оказание услуг; охраняемые результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации (интеллектуальная собственность); нематериальные блага.

Итак, криптовалюта не является фиатной денежной единицей какого-либо государства, но обладает свойствами валюты и получает все большее распространение в экономике. Пока российское законодательство не устанавливает уголовную ответственность за хищение криптовалюты, но Пленум Верховного Суда РФ признал ее объектом гражданских прав. Следовательно, содержимое электронных кошельков теоретически может быть предметом хищения и других преступлений, например, получения взятки. Тем не менее, роль биткоина в развитии права и экономики пока можно только спрогнозировать. Одно из таких предположений – законодательное определение понятия «криптовалюты» и конкретизация ее как предмета преступления, а в ряде случаев - средства его совершения.

Сведения об авторах

Федоров Александр Вячеславович – заместитель Председателя Следственного комитета Российской Федерации, кандидат юридических наук, профессор, Заслуженный юрист Российской Федерации.

Багмет Анатолий Михайлович – и.о. ректора Московской академии Следственного комитета Российской Федерации, кандидат юридических наук, доцент, Почетный сотрудник Следственного комитета Российской Федерации, генерал-майор юстиции.

Беломытцев Николай Николаевич – адъюнкт научно-педагогического факультета Академии МВД Республики Беларусь, майор милиции.

Бурынин Сергей Сергеевич – научный сотрудник Научно-исследовательского института ФГКОУ ВО «Московская Академия Следственного комитета Российской Федерации».

Быкова Елена Георгиевна – доцент кафедры уголовного права и криминологии Екатеринбургского филиала Московской академии Следственного комитета РФ, кандидат юридических наук, майор юстиции.

Вепрев Сергей Борисович – заведующий кафедрой информационных технологий Московской академии Следственного комитета Российской Федерации, доктор технических наук.

Волеводз Александр Григорьевич – заведующий кафедрой уголовного права, уголовного процесса и криминалистики, заместитель декана Международно-правового факультета по научной работе Московского государственного института международных отношений (Университета) Министерства иностранных дел Российской Федерации, доктор юридических наук.

Голоскоков Леонид Викторович – заведующий кафедрой гражданско-правовых дисциплин Московской академии Следственного комитета, кандидат философских наук, доктор юридических наук, доцент, капитан юстиции.

Грошиков Кирилл Константинович – заместитель начальника нормативно-правового отдела Юридического управления Росфинмониторинга.

Иванов Антон Владимирович – начальник департамента международного сотрудничества Центрально-Казахстанской академии, г. Караганда (Республика Казахстан), магистр экономических наук.

Казаков Александр Алексеевич – заведующий кафедрой уголовного процесса Екатеринбургского филиала Московской академии Следственного комитета РФ, кандидат юридических наук, доцент, майор юстиции.

Кинсбурская Вероника Андреевна – доцент кафедры банковского права и финансово-правовых дисциплин Юридического факультета им. М. М. Сперанского Института права и национальной безопасности Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации, главный специалист Правового департамента Ассоциации российских банков, кандидат юридических наук.

Кирков Александр Недялков – научно-исследовательская лаборатория по кибербезопасности - УниБИТ, заведующий лабораторией, доктор, Болгария.

Кондратьев Игорь Владимирович – заведующий кафедрой уголовного права и процесса Центрально-Казахстанской академии, г. Караганда (Республика Казахстан), канд. юрид. наук, доцент.

Моисеенко Марина Анатольевна – доцент кафедры предварительного расследования преступлений в сфере экономики Московской академии следственного комитета Российской Федерации, к.ю.н., доцент.

Нестерович Сергей Александрович – доцент кафедры информационных технологий Московской академии Следственного комитета Российской Федерации, кандидат технических наук

Новиков Александр Михайлович – к.э.н., доцент кафедры корпоративных финансов, инвестиционного проектирования и оценки факультета «Высшая школа финансов и менеджмента» РАНХиГС.

Пальчикова Мария Валерьевна – доцент кафедры государственно-правовых дисциплин Средне-Волжского института (филиала) ВГУЮ (РПА Минюста России), кандидат юридических наук, доцент.

Перов Валерий Александрович – заведующий кафедрой предварительного расследования преступлений в сфере экономики института повышения квалификации Московской академии Следственного комитета Российской Федерации.

Печегин Денис Андреевич – старший научный сотрудник отдела уголовного, уголовно-процессуального законодательства; судоустройства Института законодательства и сравнительного правоведения при Правительстве Российской Федерации, кандидат юридических наук.

Прорвич Владимир Антонович – доктор юридических наук, доктор технических наук, профессор, Почетный профессор Московской академии Следственного комитета Российской Федерации, профессор кафедры экономической экспертизы и финансового мониторинга МИРЭА – Российского технологического университета.

Свободный Феликс Константинович – доцент кафедры психологии ФГКОУ ВО «Московская академия Следственного комитета Российской Федерации», кандидат психологических наук, доцент, майор юстиции.

Тушканова Ольга Владиславовна – старший инспектор отдела исследования проблем технико-криминалистического и экспертного обеспечения расследования преступлений управления научно-исследовательской деятельности (научно-исследовательского института криминалистики) Главного управления криминалистики (Криминалистического центра) Следственного комитета Российской федерации.

Тчибола Эйми Мурфи Лубеши – аспирант Департамента правового регулирования экономической деятельности Финансового университета при Правительстве Российской Федерации.

Чаплинский Александр Николаевич – адъюнкт научно-педагогического факультета Академии МВД Республики Беларусь, подполковник милиции.

Черемисина Татьяна Владимировна – научный сотрудник Научно-исследовательского института ФГКОУ ВО «Московская академия Следственного комитета Российской Федерации.

Содержание

ИСПОЛЬЗОВАНИЕ КРИПТОВАЛЮТ
В ПРОТИВОПРАВНЫХ ЦЕЛЯХ И МЕТОДИКА ПРОТИВОДЕЙСТВИЯ
материалы Международного научно-практического «круглого стола»

(Москва, 25 апреля 2019 года)

Редакционная коллегия обращает внимание, что статьи представлены в авторской редакции. Ответственность за аутентичность и точность цитат, имен, названий и иных сведений, а также за соблюдение законов об интеллектуальной собственности несут авторы публикуемых материалов

Подписано в печать 20.07.2019

ISBN 978-5-6041504-7-4

Формат 60х90 1/16
Усл. печ. л. 8
Тираж 100 экз.
Печать офсетная
Заказ № 222

Отпечатано в типографии Московской академии
Следственного комитета Российской Федерации,
ул. Врубеля, д. 12