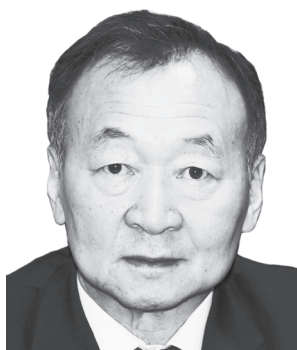


Обеспечение безопасности при использовании криптовалюты

В статье рассмотрены проблемы, возникающие в связи с использованием криптовалют: киберугрозы и информационная безопасность в онлайн-платежах, мошенничество с криптовалютой, противодействие мошенничеству. В России пока нет закона о криптовалюте, но широко используется технология блокчейн, работает криптовалютная биржа, существуют обменные пункты, для хранения криптовалюты применяются «электронные кошельки».

В. В. ЦОЙ,
кандидат технических наук, преподаватель высшей категории, Национальный исследовательский университет «Высшая школа экономики», г. Санкт-Петербург



Н иже проведен анализ разновидностей компьютерных атак, совершаемых в кредитно-финансовой сфере, а также анализ данных о фактах мошенничества с криптовалютой. Этот анализ позволяет разработать рекомендации по обеспечению безопасности от киберугроз и защите информации при осуществлении переводов виртуальных цифровых денежных средств. Такие рекомендации могут быть использованы при разработке законопроекта по криптовалюте.

Обеспечение безопасности при расчетах с использованием криптовалюты

Речь здесь в первую очередь идет о киберугрозах в онлайн-платежах.

Наступила новая эра электронных финансов, а с ней вошли в нашу жизнь и новые риски. В мировом денежном обращении появились новые деньги – криптовалюта (биткоин, лайткоин, пиркоин и др.) – конкуренты официальных денег центральных банков. Как известно, при использовании биткоинов и других валют онлайн-платежи осуществляются без участия специализированных посредников, что вызывает рост киберугроз, связанных с мошенничеством, и это требует развития систем информационной безопасности.

Вследствие широкого развития Интернета, а главное – широкого географического охвата, биткоины стали массово применяться в мошеннических действиях: они используются для взяток, ухода от налогов, бегства капиталов за рубеж, отмывания денег. Существует отдельный Интернет, в котором за криптовалюту можно приобрести товары, находящиеся в незаконном обороте. Изменение курса криптовалюты (биткоина) на мировом рынке дает большую выгоду для спекулянтов.

Е. О. ЦАРЕВ,
эксперт RTM Group



Ю. Е. ДОМБРОВСКИЙ,
кандидат политических наук, адвокат, зам. заведующего кафедрой Российской академии адвокатуры и нотариата



В России криптовалюта находится под запретом по причине того, что она может подорвать монополию Центрального банка. В 2014 г. Минфин РФ предложил законопроект о запрете денежных суррогатов, под определение которых попадают и бонусные баллы, и маркетинговые программы банков и компаний, в том числе операторов мобильной связи. Однако Минэкономразвития РФ против этого закона [1]. Известные государственные деятели и ведущие эксперты в финансово-экономической сфере высказывают разные мнения по поводу использования криптовалюты: «новая финансовая пирамида» (Э. Набиуллина), «игра в казино» (А. Кудрин), «блокчейн – новый Интернет» (Г. Греф) и т. д.

Российские компании и раньше были озабочены проблемами мошенничества с использованием Интернета. А с ростом объема биткоинов в онлайн-платежах мошенничество с криптовалютой становится еще более острой проблемой. Исследование Decisioning Vision 2020, проведенное компанией Experian в России и странах СНГ, показало: интернет-мошенничество считают самой большой угрозой 88% опрошенных финансовых и телекоммуникационных компаний. При этом 90% опрошенных отметили, что кибермошенничество может стать для них основной угрозой в течение следующих 5 лет [2].

Все чаще кражей информации занимаются продвинутые компьютерные хакеры – кибермошенники. Хищение информации при совершении онлайн-платежей с использованием криптовалюты совершается посредством компьютерных атак.

Банк России в 2015 г. создал специализированную организацию FinCERT (Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере) с целью оперативного и непрерывного мониторинга угроз информационной безопасности. Регулятор опубликовал четкие рекомендации по противодействию хакерам, разработал обязательный для всех банков регламент кибербезопасности и стандарт по расследованию подобных преступлений [3].

Хакеры применяют следующие основные типы компьютерных атак в кредитно-финансовой сфере:

- целенаправленные, связанные с подменой входных данных для автоматизированного рабочего места клиента Банка России (АРМ КБР);

- рассылку электронных сообщений, содержащих вредоносное ПО;

- атаки, направленные на устройства самообслуживания;

- DDoS-атаки;

- Reversal-атаки (атаки, связанные с особенностью обработки сообщений об отмене авторизации переводов денежных средств процессинговым центром).

Противодействие таким атакам актуально также при использовании криптовалюты в онлайн-платежах. Хакеры регулярно взламывают компьютерные программы и базы данных различных компаний. О высокой степени надежности криптовалют речи не идет, что подтверждается на практике. Так, в начале 2016 г. в результате хакерской атаки курс биткоина резко упал, а в 2014 г. из-за этого обанкротилась круп-

нейшая биржа по торговле биткоинами Mt.Gox [1]. Можно смело утверждать, что рост объемов операций электронного банкинга с применением биткоинов неизбежно приведет к появлению новых типов мошенничества, связанных с криптовалютой.

Мошенничество с криптовалютой

Прежде чем описывать наиболее популярные схемы мошенничества с использованием криптовалюты, необходимо разобрать общую архитектуру криптоиндустрии. Помимо самих криптовалют, которых в настоящий момент более тысячи, существует еще целая индустрия в первую очередь конвертации криптовалют одной в другую и обмена так называемых фиатных денег, т. е. классических, привычных нам рублей, долларов, евро в криптовалюту и обратно.

Для обмена фиатных денег на криптовалюту по всему миру существуют обменники. Есть они и в России. Наиболее популярных пунктов обмена около сотни, а общее их количество – около 300. Имеются и закрытые обменники, для «своих» клиентов. Можно сказать, что не существует проблем для совершения операций по конвертации криптовалюты в фиатные деньги и наоборот во всех крупных городах Российской Федерации, даже в отношении крупных сумм. Так, в Москве можно в течение одного дня обменять криптовалюту на несколько десятков миллионов долларов и соответствующий эквивалент в рублях.

Помимо обменных пунктов есть и криптобиржи. Это специализированные ресурсы, которые

Abstract. In the article the problems arising in connection with the use of cryptocurrency: cyber threats and information security in online payment fraud, currency fraud. Although in Russia there is no law on bitcoin, but technology of the blockchain is widely used, a cryptocurrency exchange runs, there are exchange offices, storage used cryptocurrency "wallets".

Keywords. Cryptocurrency, bitcoins, cyber security, fraud, information security, online payments, fiat money, crypto currency exchange.

Ключевые слова. Криптовалюта, биткоины, киберугрозы, мошенничество, информационная безопасность, онлайн-платежи, фиатные деньги, криптобиржи.

представляют собой классические трейдинговые системы за единственным исключением – торговля осуществляется в криптовалюте. Существует большое количество различных вариантов транзакций денежных средств на криптовалютных биржах. Ведь криптобиржи используются не для хранения денежных средств, а в основном для игры на разнице курсов.

Рядовые пользователи, помимо криптобирж, используют «электронные кошельки». «Кошельки» могут быть «горячие» и «холодные». К горячим относятся «кошельки», которые создаются на сторонних интернет-ресурсах, в этом случае хранение денег осуществляется в облаке. Холодные «кошельки» устанавливаются на рабочие станции, и хранение денег осуществляется непосредственно на машинах пользователей. Также есть вариант хранения криптовалюты на обычной бумаге – так называемые бумажные кошельки. Доступны сервисы, которые позволяют распечатать на бумаге закрытый ключ и адрес «кошелька». То есть в дальнейшем можно установить приложение, и криптовалюта будет доступна для использования.

В каких мошеннических операциях используется криптовалюта

Если не касаться оплаты различных криминальных услуг и товаров криптовалютой, то самой серьезной проблемой для государств является использование криптовалюты в процессе отмывания денежных средств и ухода от валютного контроля. Для Российской Федерации это чрезвычайно актуально, да и для большинства стран мира также представляет собой серьезную проблему.

То, что криптовалюта не контролируется центробанками государств, обеспечивает (в зависимости от конкретной криптовалюты) высокий уровень анонимности, позволяет совершать

переводы на крупные суммы. Так что популярность криптовалюты все время растет, и ее использование в процессе при отмывании денежных средств вполне закономерно.

В большинстве стран мира, помимо законодательства об отмывании, действует законодательство, регулирующее поступление денежных средств из-за рубежа и вывод капиталов за рубеж. Для того чтобы компания смогла перевести деньги со своего счета в виде займа либо в виде оплаты за какие-то товары или услуги за рубеж, ей необходимо пройти валютный контроль. Аналогично и для принятия денег со счетов иностранных контрагентов, находящихся за рубежом. Это сделано для того, чтобы центробанки государств контролировали приход денег и пресекали незаконные операции.

В случае с криптовалютами никакого валютного контроля не существует. Если где-то фиатные деньги были конвертированы в криптовалюту, то их можно в считанные часы обналичить в любой точке мира (по крайней мере, в крупных экономиках). Центробанки крупных государств считают основным вызовом со стороны криптоиндустрии именно проблемы отмывания и обхода валютного регулирования. Деньги в виде криптовалюты живут своей жизнью и не контролируются банками и регуляторами.

Следующий вид мошеннических операций – это прием денег через сайт обменных пунктов. И помимо популярных обменников, существующих на рынке и работающих хоть и в «серой» зоне, но годами, появляются сайты-клоны, полностью имитирующие данные ресурсы и взаимодействие с оператором. Злоумышленники просто собирают деньги с пользователей и затем скрываются.

Нужно сказать, что почти вся система криптовалютного взаимодействия находится в «серой» зоне, т. е. фактически никак и никем не регулируется. Исклю-

чением являются лишь несколько государств (Япония, Южная Корея, Сингапур), которые признают криптовалюту активом и работают над ее легализацией.

В большинстве стран мира обмен наличных денежных средств на криптовалюту может происходить по следующему сценарию. Происходит встреча с представителем обменника, никто никому не показывает никаких документов, никто никого не знает. Наличные деньги передаются курьеру. После того как курьер удалится в безопасное место и сообщит оператору обменника о том, что деньги приняты, необходимая сумма будет переведена клиенту на криптокошелек, который был указан при формировании заказа. Если происходит обмен криптовалюты на фиатные деньги, то сначала клиент переводит криптовалюту на «кошелек» обменника, в дальнейшем курьер связывается с клиентом, они встречаются в удобном для обоих месте и курьер передает деньги тому, кто назовет номер заказа.

Если деньги переводятся с карточных счетов, безналичными платежами, то, как правило, это выглядит следующим образом: деньги переводятся, например, через карточку Сбербанка на карточку Сбербанка какого-то другого человека, и через какое-то время оператор обменника переводит криптовалюту на тот «кошелек», который был указан при заказе. Нет никаких чеков, никаких гарантий.

Следующий вид мошенничества с криптовалютой – использование сайтов, которые осуществляют обмен карточного фиата на криптовалюту. Схема простая: деньги со стандартных классических карточек типа VISA или MasterCard переводятся контрагенту, под видом оплаты за какой-то товар или услугу. В дальнейшем злоумышленники обналичивают эти деньги. Данный способ покупки криптовалюты наиболее популярен и считается самым надежным, так как боль-

шинство ресурсов, участвующих в этой схеме, требуют подтверждения личности.

Существуют также криптобиржи-однодневки. Смысл в том, что криптобирж во всем мире сотни, если не тысячи, и они работают очень часто без какого-либо контроля. Криптобиржи по своей капитализации и объему транзакций способны дать фору огромному количеству легальных брокеров. На криптобиржах ежедневно обменивается криптоактивов на миллиарды долларов, причем если деньги заведены на криптобиржу, пользователь доверяет свои капиталы контрагенту другой стороны.

Как правило, никто не знает достоверно, кто в действительности контролирует ту или иную криптобиржу, и поэтому возможен вариант, когда она вдруг одномоментно исчезает. Добавим, что активы пользователя на криптобирже не контролируются им в полном объеме. Данные о ключевой информации также хранятся на криптобирже.

Показательна в этом смысле история с криптобиржей BTC-e. В течение одного дня с подачи Федерального бюро расследования США был арестован, по предварительной информации, основатель этой биржи, а также были описаны и изъяты сервера ресурса. В дальнейшем пользователи просто не смогли получить доступ к своим «кошелькам» (по состоянию на сентябрь 2017 г. криптобиржа BTC-e восстановила свою работу и частично компенсировала пользователям потери от действий ФБР). Но, повторим, контроль криптобирж остается на стороне создателей, и никаких гарантий в данном случае не существует.

Следующий популярный вид мошенничества – использование тех машин, которые попали в бот-сеть в качестве майнеров (майнеры – это те, кто добывает криптовалюту с помощью своего компьютера, или майнинг-фермы). Раньше у злоумышленников было не очень много

вариантов применения машин, которые они могут использовать для проведения каких-то крупных операций.

Пример: были заражены 10 тыс. компьютеров, из них только одна машина является бухгалтерской, через нее злоумышленники похитили деньги со счета компании путем отправки банального платежного поручения через систему дистанционного банкинга. Остальные 9999 компьютеров злоумышленники использовали для проведения DDoS-атак и еще нескольких вариантов незаконных операций.

Теперь же злоумышленники научились устанавливать соответствующее ПО на зараженные машины и заниматься майнингом криптовалют. И если в бот-сети сосредоточено большое количество машин – десятки и сотни тысяч, то пользователь каждой из них будет чувствовать, что его компьютер чрезвычайно сильно «тормозит», а в это время злоумышленники будут добывать криптовалюту. Что немаловажно – «чистую», т. е. такую криптовалюту, которая не была замечена в криминальных операциях. В дальнейшем ее проще обналичить либо вывести в другие платежные системы.

Самый популярный с середины 2017 г. вид мошенничества – это проведение ICO (Initial Coin Offering – первичное размещение монет/токенов). Нельзя сказать, что все ICO являются мошенническими, большая часть из них, наоборот, к таковым относиться не может. Тем не менее, поскольку никакой регуляции рынка настоящий момент нет и провести ICO достаточно просто, этот путь используется злоумышленниками для сбора криптовалюты с обычных пользователей с последующим исчезновением инициаторов размещения.

Суть в следующем: появляется некий проект, публикуется его описание (white paper); регистрируется сайт, на котором излагается основная информация об идее

новой разработки и размещается призыв: «Нам необходимо 20 миллионов долларов, чтобы этот проект выполнить». Криптосообщество может инвестировать криптовалюту в этот проект. Взамен инвесторы получают так называемые токены этого проекта, и уже через несколько часов или дней эти токены будут торговаться на открытом рынке, в том числе на тех самых криптобиржах, о которых говорилось выше.

Здесь опять же нет никакого регулирования, и если деньги были переведены кому-то, то в дальнейшем этот кто-то может пользоваться полученной криптовалютой по своему усмотрению. И также в истории ICO неоднократно бывало, что проекты или идеи собирали большое количество криптовалюты на реализацию, после чего их авторы исчезали вместе с собранными деньгами.

Что же хочется сказать в итоге? Возникшие за последние несколько лет криптомир и криптоиндустрия, безусловно, не могут уже нигде исчезнуть, они будут существовать в том или ином виде и дальше. И потому задачей, в том числе и государственных институтов, является создание инструментов регулирования этого рынка, в том числе регулирования ICO и рынка обращения криптовалюты. Добавим: в Японии в настоящий момент криптовалюта частично легализована, юридические и физические лица в японских банках могут открывать счета в биткойнах или в другой криптовалюте.

Все эти факты доказывают, что этот рынок будет развиваться, а вместе с ним будут развиваться и варианты использования криптовалют в криминальных целях.

Национальная криптовалюта как условие борьбы с криптомошенничеством

Разработка средств и методов противостояния онлайн-мошенничеству с использованием

криптовалюта – дело непростое и небыстрое, учитывая, что для этих денег характерна высокая степень анонимности, являющаяся одним из их наиболее привлекательных факторов с точки зрения клиентов. Отслеживать эмиссию биткоинов и обложить ее налогом физически невозможно из-за особенностей технологии блокчейн. Рассмотренные выше способы и схемы мошенничества с криптовалютой показывают, что противодействие – задача нелегкая и требующая новых подходов. Необходимо решить вопрос на законодательном уровне, а также нужны профессионалы, обладающие специальными знаниями в этой области.

Как известно, криптовалюты в России находятся под запретом, но чтобы предотвратить возможное участие компаний в отмывании денег с помощью биткоина, в 2015 г. Минфин РФ внес предложение об уголовной ответственности в виде 4 лет тюремного заключения и штрафа в размере 500 тыс. руб. за выпуск и использование криптовалют физическими лицами. Для топ-менеджеров банков за подобные операции было предложено наказание в виде тюремного заключения на срок до 7 лет [1]. Это можно объяснить тем, что в дискуссии о криптовалютах участвуют в основном юристы, которые спорят главным образом о подпадании таких операций под действие соответствующих статей Уголовного кодекса.

Готовится законопроект о криптовалюте, который запретит частным лицам, не имеющим сертификата квалифицированного инвестора, покупать и продавать на криптовалютных биржах. Правительство также планирует легализовать технологию блокчейн и использовать ее для своих целей (например, в

национальной платежной системе) и даже создать российскую криптовалюту, оперативно разработать законодательный документ, предусматривающий создание единой биржи, деятельность которой будет регулироваться Росфинмониторингом.

Создание своей криптовалюты обеспечит возможность осуществлять больший контроль со стороны государства и ЦБ за оборотом криптовалюты в финансовом пространстве Российской Федерации, так как для выполнения того или иного платежа посредством криптовалюты сначала необходимо будет поменять ее на национальную валюту РФ и уже ею производить оплату за товары и услуги.

Учреждение национальной криптовалюты может стать существенным инструментом в решении проблем, связанных с интеграцией в пространство Российской Федерации блокчейн-технологий и систем финансовых отношений, основанных на криптовалютах. При этом национальная криптовалюта, благодаря встраиванию в ее архитектуру системы государственного контроля за перемещением криптоденежных единиц, может стать специальным буфером между глобальным крипторынком и экономическим пространством Российской Федерации.

В случае встраивания такой криптоденежной системы классические криптовалюты (биткоины или лайткойты) становятся неким аналогом золота и серебра, которые имеют признанную во всем мире стоимость, хотя и не могут прямо использоваться для оплаты конкретных товаров и услуг, но при желании быстро конвертируются в национальную валюту, что может быть четко регламентировано специальным законодательством.

Такой подход, с одной стороны, сможет создать достаточно эффективный механизм интеграции систем, основанных на блокчейн-технологиях и криптовалюте в экономическое, политическое, правовое и информационное пространство Российской Федерации без существенных потерь в части контроля и государственного регулирования, а с другой стороны, даст временный ресурс для разработки и построения в стране полноценной информационной экономической системы.

■ **ВЫВОДЫ**

Сегодня необходимо:

- отслеживать тенденции и весь процесс развития киберугроз со стороны злоумышленников (хакеров), регулярно взламывающих компьютерные программы и базы данных криптовалют; уделять особое внимание информационной безопасности;

- разрабатывать эффективные способы противодействия мошенничеству с криптовалютой аналогично применяемым в противодействии легализации (отмыванию) доходов, полученных преступным путем;

- при возможном признании на государственном уровне криптовалюты в России – разработать специальное законодательство, регулирующее общественные отношения, связанные с использованием криптовалюты;

- согласиться, что учреждение национальной криптовалюты позволит, с одной стороны, упорядочить общественные отношения, связанные с использованием криптовалют на территории Российской Федерации, с другой, даст временный ресурс на создание полноценной системы правового и фактического регулирования оборота криптовалют в стране.

Список литературы

1. Шмелев В. В. Криптовалюта – деньги XXI века? // Банковское дело. 2017. № 3. С. 52–56.
2. Костин Т. С., Прокопенко И. Г. Онлайн-мошенничество: современные угрозы безопасности и прогнозы // Банковское дело. 2017. № 6. С. 42–49.
3. Фролов Д. Б. FinCERT: основные задачи и направления развития // Банковское дело. 2016. № 2. С. 74–76.