Владимир ГЛОТОВ, Дмитрий МИХАЙЛОВ

ТЕХНИЧЕСКИЕ СРЕДСТВА И ПРИНЦИПЫ РЕГУЛИРОВАНИЯ КРИПТОВАЛЮТ

В современном мире технология BlockChain, так же как и криптовалюты, в качестве формы денежной реализации данной технологии, быстро распространяются и внедряются в различных областях государственного и частного секторов. При этом технология распределенного хранения и обработки данных подразумевает отсутствие централизованного контроля. Подобная децентрализация не всегда удовлетворяет политиков правительств различных стран, которые, как минимум, хотят уберечь собственных граждан от мошенников и препятствовать незаконному финансированию террористов, а как максимум, не хотят неорганизованных денежных потоков, финансирования нелегальных организаций на территории страны.

В данной статье будут рассмотрены политики различных стран в области регулирования криптовалют, а также технические аспекты как вводимого регулирования, так и тех регуляций, которые только могут появиться.

Ключевые слова: атаки на криптовалютные биржи, атаки на криптовалюты, безопасность криптовалют, инфраструктура криптовалют, криптовалюта, национальная безопасность, субъекты Федерации

Регулирование криптовалют сегодня относится к разряду проблем, от эффективности решения которых во многом зависит безопасность современного общества. Именно этим объясняется то внимание, которое уделяется этой сфере как на уровне федерального Правительства, так и на уровне субъектов Российской Федерации. На сегодняшний день во многих странах уже накоплен определенный опыт регуляции криптовалют. Его изучение, по нашему мнению, необходимо для того, чтобы сформировать механизмы, обеспечивающие, с одной стороны, интересы данной сферы финансовых отношений, с другой — интересы государства и проживающего в его границах населения.

На сегодняшний день механизмы регуляции криптовалют правительствами разных стран нельзя назвать совершенными. Вместе с тем можно отметить несколько явно выделяющихся политик регулирования, а именно:

- полное разрешение криптовалют;
- обсуждение статуса и отсутствие решения;

- частичное регулирование;
- запрет криптовалют;
- введение национальной криптовалюты.

Попытаемся кратко охарактеризовать каждый из выделенных типов проводимой политики.

Полное разрешение криптовалют наблюдается в таких странах, как Япония, Германия, Швейцария. Для этих государств характерны крайне благосклонные юрисдикции, в рамках которых криптовалюты являются абсолютно легальными средствами. Иначе говоря, *они приравнены к валюте* как таковой или к законному денежному средству. Законы методично адаптируются под требования *BlockChain* сообщества.

Многие страны пока *только обсуждают статус криптовалют*. Речь в данном случае идет об Австралии, России, Канаде, Франции, Индии. Регуляторы каждой из стран спорят о статусе валюты и механизмах ее регулирования и, очевидно, ждут решений других стран, собирают и анализируют «лучшие практики». Ряд из этих стран, например Индия, уже создала Ассоциацию по криптовалютам и активно прорабатывает нормативную базу, но пока ее не вводит.

Выделяется группа стран, в которых принято решение *вводить регуляцию криптовалют поэтапно*. А потому в настоящее время начинается регулирование лишь некоторых аспектов этого нового рынка. Речь идет, например, о Швеции. В этой стране, в частности, на сегодня запрещена оплата металлолома в криптовалюте.

В США наблюдается тенденция большего регулирования в части *ICO* (*Initial Coin Offering*) — аналога *IPO* для обычных ценных бумаг, но реализуемый для привлечения инвестиций посредством криптовалют. Комиссия по ценным бумагам и биржам США, являющаяся главным органом, осуществляющим функции надзора и регулирования рынка ценных бумаг в стране, подводит под действие американского законодательства о ценных бумагах операции *ICO*. Комиссия таким образом хочет защищать игроков рынка при использовании «нового» метода привлечения капитала.

В Китае торговля криптовалютами и майнинг (выработка криптовалюты) не запрещены для граждан страны, но запрещены для банковской системы.

Представители трех крупнейших китайских криптовалютных бирж — *BTCC*, *Huobi* и *OKcoin* — регулярно вызываются в Народный банк Китая (*PBoC*), где с ними проводят рекомендационные беседы. Китайский регулятор намерен контролировать все способы движения капитала, в т.ч. криптовалюты. Фактически китайские биржи вынуждаются идти на верификацию пользователей и предоставление информации контролирующим органам Китая.

Скорее всего, такие страны и далее будут плавно вменять запреты и регуляции.

Полный запрет криптовалют практикуется во Вьетнаме, в Таиланде, Бангладеш, Боливии. Соответствующие нормы имеют законодательное оформление. Мотивацией в таких странах почти всегда является желание уберечь граждан страны от спекуляций и мошенничества.

Многие страны задумываются о *целесообразности введения своих национальных криптовалют*, которые будут лишены преимуществ виртуальных валют: децентрализованности и анонимности. Первой по данному пути пошел Эквадор. Надо отметить, что Эквадор не имеет своей валюты и использует доллары США. В 2014 г. правительство Эквадора официально запретило криптовалюту *Bitcoin* и ее аналоги. В следующем году Эквадор планирует запустить собственную криптовалюту и при этом приравнять ее к национальной валюте. Планируется, что данная валюта будет обеспечена реальными активами, хотя пока непонятно какими. Регулированием криптовалюты будет заниматься валютно-финансовый комитет Эквадора. Возможно, многие страны ожидают результатов такого эксперимента Эквадора, чтобы в случае успеха последовать его примеру.

Очевидно, что разница в подходах к регулированию криптовалют в разных странах определяется множеством моментов, основными среди которых являются культурные факторы; особенности государственного устройства и структура экономики страны.

Так, например, развитый рынок ценных бумаг в США, Сингапуре, Гонконге заставил эти страны достаточно быстро принять регуляции, защищающие *BlockChain* как систему инвестиций в ценные бумаги. При этом Индия, например, является лидером мировых денежных переводов: большая часть индусов работает за рубежом. Регуляция криптовалюты в этой стране направлена прежде всего на то, чтобы не навредить денежному потоку в страну. При этом Индия с ее потенциалом к разработке программного обеспечения может стать мировым лидером в технологии, так что регуляция, очевидно, проводится крайне аккуратно.

Другая причина регулирования может быть, например, в странах, откуда «утекают» платежи в т.ч. мигрантов. Простейший пример, связанный с той же Индией: ОАЭ является самым большим источником денежных переводов в Индию, его доля составляет 40%, на втором месте — Саудовская Аравия с долей 30%.

Любые вводимые регулирования, особенно крупными странами, приводят к *скачкам волотильной криптовалюты.*

Так, в 2013 г. Народный банк Китая запретил криптовалютные транзакции для финансовых организаций, что привело к обрушению курса криптовалюты *Bitcoin*. После того как в 2014 г. Налоговая служба США (*IRS*) причислила *Bitcoin* к одному из видов собственности, падение цены на криптовалюту составило 150 долл. В 2017 г. Народный банк Китая ввел очередной запрет, связанный с оборотом криптовалюты, что сказалось на курсе *Bitcoin* еще раз: криптовалюта «просела» на 30%.

Особенности регулирования криптовалюты

Пока криптовалюты выдерживают все испытания. Если посмотреть на любой из предыдущих 7 «крахов» биткоина, то криптовалюта никогда не падала заметно ниже предыдущего максимума, а после только

с большей уверенностью восстанавливала максимальную отметку и побивала новые рекорды. Все это доказывает ее жизнеспособность и заставляет пока неопределившиеся страны задумываться о необходимых регуляциях. Кроме того, все чаще появляется мнение о необходимости формирования системы регулирования криптовалют в рамках союзов: БРИКС, АСЕАН и др.

Рассмотрим, как государства могут подойти к этому вопросу. Прежде всего стоит обратить внимание на уже существующие примеры в других технологиях, т.к. прецеденты — это первое, на что обратят внимание регуляторы. Лучший пример, иллюстрирующий борьбу с технологиями, — это запреты и «локализация» мессенджеров. Появившиеся мобильные приложения для обмена короткими сообщениями и звонками позволили пользователям уйти из поля зрения специальных служб различных государств. Массовые случаи использования мессенджеров террористами позволили государствам как юридически (например, в России), так и технически (например, в Турции) ограничить использование данных программ. Вводились блокировки мессенджеров, раскрытие ключей секретных чатов для государственных органов (например, в Индонезии). Китай пошел дальше всего — создал национальную мессенджинговую платформу: идеальный мессенджер *WeChat* (полностью доступный государству) при блокировке всех других программ подобного класса быстро стал номером один в Китае и, кажется, скоро станет номером один в мире. Блокировка программ осуществляется на уровне фильтрования пакетов, характерных для мессенджеров.

В России Президент подписал закон о регулировании мессенджеров, обязывающий идентифицировать пользователей с помощью номера телефона. Фактически это открывает возможность государству к регулированию рассматриваемой сферы. В опубликованном на сайте Совета безопасности России документе предполагается, в частности, усиление правового регулирования мессенджеров.

Любая регуляция технологических решений, как правило, имеет три аспекта.

Первый. Юридическое регулирование.

Второй. Техническое регулирование.

Третий. Специальное регулирование.

Юридическое регулирование относится к сфере функционирования органов государственной власти, соответствующих агентств и парламентов стран. Фактически в каждый стране должны быть приняты и функционировать соответствующие законы и подзаконные акты, предполагающие понятие легальности тех или иных операций, а также меры наказания и контроля.

Специальное регулирование — это работа спецслужб. Откровения Э. Сноудена, публикации *Wikileaks*, скандалы с «закладками» *Huawei*, которые следят за пользователями, показали, насколько технологии вовлечены в работу спецслужб. Для многих спецслужб технологии — это новые возможности. Очевидно, что спецслужбы не игнорируют и криптовалюты.

Согласно ряду открытых данных и публикаций[1], *одной из первых стран*, которая была уличена в использовании в своих интересах криптовалют, стала Северная Корея: хакеры, состоящие на службе у Северной Кореи, взломали кошельки множества пользователей, прежде всего из Южной Кореи. Биткоины стали крайне удобным средством перевода денег в эту страну, ведь мировое сообщество очень старается исключить получение северными корейцами любого рода финансирования, чтобы не допустить развития ядерной программы.

С ростом непризнанных государств, роль биткоина будет также повышаться. Часто режимы непризнанных или воюющих республик поддерживаются из-за рубежа, причем на государственном уровне. Но прямое финансирование в таком случае предается огласке и может повлечь даже санкции ООН. По многим открытым источникам[2] становится очевидным, что уже на государственном уровне при скрытой поддержке государства создаются механизмы скрытых переводов денежных средств. И такая тенденция будет только расти.

Очевидно, многие государства будут стараться получить преимущества за счет проникновения или взлома системы *BlockChain*. Стоит предположить, что спецслужбы будут инвестировать в развитие школы изучения уязвимостей криптовалют. Если верить публикациям хакерских группировок, то АНБ (Агентство национальной безопасности США) имело несанкционированный доступ к межбанковской системе *SWIFT*. То есть традиционная денежная система была объектом взлома спецслужбы, которая использовала уязвимости в операционных системах *Windows* для отслеживания за денежными потоками между банками в интересующих странах. Вряд ли стоит полагать, что анонимный *Bitcoin* или любая другая криптовалюта будут менее интересны спецслужбам.

Техническое регулирование — это, пожалуй, самый интересный аспект регулирования криптовалют. Как технически можно отрегулировать технологию, которая принципиально строилась на принципах максимальной децентрализации?

Техническое регулирование: глобальный контроль BlockChain технологии

В традиционных централизованных системах все транзакции, перед их исполнением, проверяются на основе информации центрального контролирующего органа. В децентрализованных системах (криптовалютах) всегда есть техническая возможность двойного расходования (англ. *Double-spending*). Это означает, что пользователь может сделать несколько платежей, передающих один и тот же актив, практически одновременно. Информация о них моментально не попадет в очередной блок, и каждый из получателей будет уверен, что совершил валидную

---

[1] См., напр.: North Korea appears to be trying to get around sanctions by using hackers to steal bitcoin / URL: https://www.cnbc.com/2017/09/12/north-korea-hackers-trying-to-steal-bitcoin-evade-sanctions.html.

[2] Congress Looks to Bitcoin and Its Links to Terrorism: «The table is set for this threat to grow significantly» / URL: https://www.inverse.com/article/31672-bitcoin-isis-congress.

операцию. Лишь после того, как одна из транзакций (необязательно выполненная первая по времени) будет включена в блок, остальные транзакции с этим же активом уже не будут действительными. Но некоторое время в параллельных ветках могут находиться транзакции, которые по-разному определят прохождение транзакции.

Вероятность существования параллельных цепочек блоков крайне мала и катастрофически уменьшается с ростом длины цепочки и количества независимых майнеров[3]. Контроль цепочек возможен только при наличии у злоумышленника контроля над достаточно большой долей суммарной мощности майнинга. В таком случае имеется существенная вероятность скрытого выстраивания длинных параллельных цепочек блоков. После их публикации главной будет признана более длинная цепочка, а реальные цепочки будут отменены. Если подконтрольная мощность майнинга меньше 50%, то вероятность успеха экспоненциально снижается с каждым подтверждением.

Перехват 50% майнеров кажется вещью практически нереальной, но, тем не менее, реализуемой при вмешательстве в процесс майнинга государства. Такой метод регулирования может быть, например, введен в централизованном Китае.

Еще одним методом контроля криптовалют может стать *квантовый компьютер*, который позволит расшифровывать на лету любые алгоритмы зашифрованных транзакций. Однако в данной статье этот сценарий рассматриваться не будет — пока квантовые вычисления не способны существенно влиять на криптовалюты. И более того, если какое-то из государств возьмет на вооружение квантовую криптографию, то угроза будет представляться для всего, что так или иначе имеет отношение к Интернету, а не только к технологии *BlockChain*.

Техническое регулирование: контроль на уровне пользователей

Кошельки пользователей — это структуры для хранения криптовалюты, т.е. виртуальных денег на основе *BlockChain*. Кошелек представляет собой фактически две цифры — уникальный идентификатор кошелька (биткоин-адрес, к которому привязаны все деньги) и так называемый секретный ключ.

Имеющийся биткоин-адрес можно диктовать любому, кто хочет перевести денежные средства на этот кошелек, т.е. оплатить что-то на указанный идентификатор (счет). Криптоденьги будут после транзакции привязаны к данному биткоин-адресу.

Чтобы потратить деньги, необходимо скачать специальное программное обеспечение — так называемый программный кошелек. Для отправки денег необходимо будет ввести секретный ключ. После введения секретного ключа и суммы транзакции денежные средства будут списаны со счета.

Существует два типа кошельков: холодный кошелек и горячий кошелек.

---

[3] Майнер — специалист по выработке криптовалюты.

Горячие кошельки подключены к Интернету 24/7, поэтому криптовалюту из них можно потратить в любое время. Но это является большим минусом кошелька, т.к. горячий кошелек может быть доступен хакерским атакам также круглые сутки.

Холодный кошелек хранит криптовалюту в автономном режиме, т.е. холодный кошелек никогда не подключен к сети Интернет. Фактически холодный кошелек — это место хранения адреса таким образом, чтобы хакер технически не мог получить доступ.

Оплата при использовании холодного кошелька происходит следующим образом.

1. Компьютерная программа создает дескриптор транзакции
   transaction: {from:<address0>, to: <address1>, amount: <amount>, message: <message>};
2. Компьютерная программа отправляет транзакцию в холодный кошелек;
3. Холодный кошелек шифрует *transaction.message* при помощи секретного ключа в новую переменную *signedMessage*, иначе говоря, подписывает транзакцию;
4. Отсылает транзакцию обратно в компьютерную программу;
5. Компьютерная программа отправляет транзакцию в блокчейн;
6. Майнеры сверяют правильность транзакции, прогоняя через специальную функцию
   verifyTransaction(publicKey: <from>, message: <message>, signedMessage: <signedMessage>);
7. Функция verifyTransaction убеждается, что так подписать *message* способен только человек с публичным ключом publicKey:<from>. Никто другой, кроме как владелец настоящего privateKey, не мог получить такой signedMessage для PublicKey:from;
8. Таким образом, приватный ключ никогда не покидает холодный кошелек, холодный кошелек остается всегда холодным и безопасным.

Все большую популярность приобретают аппаратные кошельки. Такой кошелек представляет собой небольшое электронное устройство с автономным дисплеем и питанием. На устройстве хранятся секретные ключи таким образом, чтобы их нельзя было извлечь. Устройство присоединяется к компьютеру, подключенному к сети Интернет и контролирует транзакции.

Так как регулирование на уровне инфраструктуры для государства может представляться тяжелым, то технически проще всего контролировать именно кошельки пользователей. Как минимум, необходимость такой регуляции может быть вменена государством для любых компаний, имеющих государственную аккредитацию. Все больше банков, авиакомпаний принимают криптовалюту уже сейчас. В случае введения национальных криптовалют государство захочет быть уверенным в том, что валюта в безопасности. На уровне централизации валюты (как в Эквадоре) сделать это может быть проблематично, а обязать пользователей иметь сертифицированные кошельки проще.

Сертифицированный кошелек — это, во-первых, идентификация пользователя, а значит, исключение возможности анонимности.

Во-вторых, контроль и учет денежных средств.

В-третьих, защита пользователя от хакеров и взлома.

Первый и второй пункты фактически нивелируют преимущества криптовалюты как абсолютно открытой системы, но при этом также снижают вероятность отмывания денежных средств и незаконного сбыта.

Защита пользователей от взлома — это также немаловажная и, наверное, *единственная принимаемая сообществом функция* такого контроля.

Выявляется поразительное совпадение трендов роста инвестиций в проекты на базе *BlockChain* в сети Интернет и рост прибыли киберпреступников за последний год.

Так, за 2017 г. объем инвестиций в проекты на базе *BlockChain* вырос в два раза, и, что удивительно, общая прибыль киберпреступников увеличилась также пропорционально. Несовершенство методов защиты технологий и слабое регулирование рынка со стороны государства, очевидно, переориентировало киберпреступников именно на технологию *BlockChain*. При этом почти все атаки злоумышленников направлены на взлом кошельков.

В основном атаки совершаются за счет вирусов, которые, например, как вирус *Trojan.Coinbitclip*, проникнув на компьютер, следит за тем, когда в буфере обмена появляется строка, похожая на адрес биткоин-кошелька. Вирус тут же подменяет его на свой адрес, и деньги отправляются злоумышленнику. Еще одной набирающей популярность атакой является атака, направленная на похищение резервной версии (бекапа) компьютеров. Как правило, оставленная «в бекапе» версия горячего кошелька имеет тот же пароль, что и новая версия. После получения доступа к старой версии злоумышленник может с легкостью взломать текущий кошелек. Очевидно, что злоумышленники будут модернизировать все множество существующих обычных вирусов и дальше, чтобы направить их на похищение криптовалют.

Эффективно с такими атаками можно бороться с использованием аппаратного кошелька. Удаленно украсть криптовалюту невозможно, злоумышленнику нужен физический доступ к устройству. Для взлома кошелька злоумышленнику требуется всего 20 секунд. Так, аппаратный кошелек *Trezor*, например, при подключении источника питания автоматически загружает свою память (*SRAM*), где хранятся ключи. Загрузка происходит без проверки, введен ли *PIN*-код пользователя. Если перед включением устройства подключиться напрямую к двум контактам внутри *Trezor*, то память можно просто скачать и далее с помощью специального программного обеспечения, кстати опубликованного в сети Интернет, просто извлечь из нее секретные ключи. Такая же проблема имеется и у другого производителя кошельков — *Keepkey*.

На рынке сегодня все аппаратные кошельки производятся частными компаниями и, разумеется, не сертифицированы ни одной страной. Безопасность во многом определяется открытостью их архитектуры и доступностью для изучения сообществу. Кошельки при поставке, как

правило, имеют голографический стикер. Производитель предупреждает, что если при получении устройства наклейка повреждена, то пользователю следует обратиться в службу поддержки.

Строго говоря, аппаратный кошелек — это средство криптографической защиты информации. Подобные средства в России подлежат, например, сертификации ФСБ России. Кроме того, частично за подобную сертификацию, по ряду классов, может отвечать Федеральная служба по техническому и экспортному контролю (далее — ФСТЭК). Уже существующее законодательство нашей страны крайне просто можно адаптировать для регулирования именно криптокошельков, как средств защиты информации. Сертификация выпуска аппаратных кошельков может стать первым шагом при регуляции поля криптовалют, причем не только в России.

Последующим шагом будет обязательное внедрение таких устройств для всех государственных органов или компаний, которые попадут под специализированный приказ.

Важно, что в России выпуск специальной техники и внедрение ее в государственные органы — это уже отлаженный процесс, как, кстати, и в США и ЕС. В России средства защиты информации сертифицируются ФСТЭК уже достаточно давно, а в стране действует обширная сеть лабораторий с лицензией данной службы, которые могут сертифицировать решения.

Сертификация кошельков, очевидно, потребуется не только для контроля за оборотом криптовалюты. К сожалению, существующие на сегодня аппаратные кошельки не так неуязвимы. Уязвимости, позволяющие злоумышленникам красть криптовалюту, существуют и для таких устройств. Более того, подобного рода атаки уже имели место быть. Чтобы рассмотреть подробнее, *как мошенники могут взломать аппаратный кошелек*, покажем, что из себя представляют такие устройства.

Один из самых популярных аппаратных кошельков на сегодня — это уже упоминавшийся кошелек *Trezor*, который производится чешской компанией *SatoshiLabs*. Аппаратный кошелек используется для подписи транзакций, которые подтверждаются через небольшой дисплей. То есть для того, чтобы осуществить (подтвердить) платеж, необходимо физически на устройстве ввести подтверждающие данные, а значит, степень защищенности компьютера пользователя не должна иметь значения. Кошелек работает с разными валютами: *MultiBit, Mycelium, Electrum*. Более того, устройство может использоваться для хранения альткойнов.

Для начала работы с кошельком пользователю необходимо подключить его к компьютеру и в браузере перейти на сайт компании *myTrezor.com* для выполнения дальнейших инструкций. С сайта скачивается и устанавливается программа-плагин для браузера.

Кошелек достаточно хорошо защищен от атак со стороны программ-кейлогеров: это специальные программы, которые в скрытом режиме попадают на компьютер пользователя и могут записывать набираемые комбинации клавиш, а значит, и пароли, после чего пересылать злоумышленнику. Использование *Trezor* позволяет достаточно

хорошо защитить кошелек: на его экране генерируется случайный код, а в браузере предлагается ввести *PIN*-код, исходя из расположения этих цифр на экране устройства. Так как порядок цифр каждый раз генерируется случайно, то необходимо работать с аппаратным кошельком перед каждым вводом *PIN*-кода.

После ввода *PIN*-кода на экране аппаратного кошелька высвечиваются одно за другим 24 случайно сгенерированных слова, которые необходимо записать. Эта фраза может быть использована для восстановления кошелька. Чтобы повысить доверие к устройству, производитель предоставляет его открытый код, позволяющий всему сообществу убедиться, что в устройстве нет так называемых «закладок» — частей кода, которые могут скрыто передать данные производителю.

Исследования инженеров Джоша Датко (*Josh Datko*) и Криса Картье (*Chris Quartier*) показали, что при всей защищенности кошелька *Trezor* его можно взломать через уязвимость микроконтроллера *ST32F05* производства *STMicroelectronics*. Чтобы воспользоваться уязвимостью, злоумышленнику нужен физический доступ к устройству *Trezor,* т.е. точно быть уверенным, что никто не завладеет вашей криптовалютой, можно, только если кошелек всегда находится в поле зрения пользователя.

К сожалению, такая же проблема имеется и у другого производителя кошельков — *Keepkey*.

Регуляции государства к требованиям таких кошельков будут, очевидно, накладывать на производителя определенные требования для блокирования возможностей злоумышленника.

Регулирование инфраструктуры криптовалют

Регулирование криптовалюты в целом — это только вершина айсберга. Разрешение или запрет тех или иных криптовалют и в целом инфраструктуры вокруг криптовалют — это только первый вопрос, на который старается ответить государство. Если криптовалюты принимаются и допускаются страной, то встает вопрос *обеспечения безопасности окружающей инфраструктуры*, например криптовалютных бирж.

Биржи для осуществления транзакций с криптовалютами — один из ключевых элементов инфраструктуры денежных операций в системе *BlockChain*. Как и любая инфраструктура со слабой степенью защиты, но с солидным оборотом денежных средств, система бирж становится любимой точкой атаки злоумышленников.

Взломы бирж начались уже при открытии первых площадок, и первыми жертвами киберпреступников стали крупнейшие в то время биржи *Bitcoinica* и *Tradehill*. *Bitcoin* еще не был так популярен, и эти события практически не освещались.

Изменил все взлом японской биржи *MtGox* в середине 2011 г. Это был один из первых случаев, хорошо освещенных в средствах массовой информации и повлиявший на курс *Bitcoin*. Но даже при таком негативном опыте руководство биржи *MtGox* не сделало выводов в области кибербезопасности, и в начале 2014 г. 650 000 биткоинов (на февраль 2014 г. около 480 млн долл.) исчезли со счетов биржи. Состоявшийся

суд над президентом *MtGox* Марком Карпелесом хоть и был важным прецедентом в правовом регулировании, но приговор в растрате и манипулировании данными не был вынесен, т.к. не было достаточно доказательств.

Надо сказать, что атаки на биржи становятся все более частым явлением: биржа *Bitstamp* осталась без 20 000 BTC (что на курс в моменте составляло больше 5 млн долл.). Крупная китайская биржа *Bter* дважды потеряла деньги — сначала $1,65 млн долл., а потом уже через год и вовсе закрылась, раздав клиентам остатки активов в качестве компенсации.

В 2016 г. была взломана биржа *Bitfinex* в США. Это привело к обвалу курса *Bitcoin*, что является, пожалуй, вторым после взлома *MtGox* случаем взлома бирж, который так существенно повлиял на курс криптовалюты. По имеющимся оценкам, бирже *Bitfinex* принадлежала почти половина торговых объемов в паре *BTC/USD*. К расследованию обстоятельств взлома *Bitfinex* подключилось ФБР США.

Взломанные биржи часто просят хакеров за вознаграждение вернуть украденное, но это не всегда удается. Бирже *Bter* хакер вернул украденное в первый раз, а бирже *Bitfinex*, которая публично обратилась к хакеру через свой сайт, ответ никто не дал. Чтобы восстановить имя *Bitfinex* предложила своим клиентам компенсации, тем самым породив тенденцию в мире кибербезопасности *BlockChain*. Теперь взломанные биржи все чаще начинают предлагать своим клиентам выпуск в счет долга специальных токенов, которые позже будут выкупаться по номиналу. Так как такие токены начинают свободно торговаться, то пользователи, скорее всего, их распродают по заниженной цене, не веря в восстановление биржи. В итоге *Bitfinex* выкупила все токены *BFX* по заявленной цене.

Корейская биржа *Yapizon* потеряла примерно 40% сразу после взлома *Bitfinex* из-за хакерской атаки. Имея корейскую юрисдикцию, биржа подала заявление в отдел расследования киберпреступлений в Сеуле. Как биржа *Bitfinex* решила компенсировать потери клиентов, но помимо этого предоставила им возможность обменять *Fei* на акции *Yapizon* на бирже *Yahoo Japan*.

Примерно такая же ситуация наблюдается при проведении *ICO* в различных странах мира. Мошенничеств и атак на подобные площадки в разы больше, чем на биржи, и примеров можно привести ничуть не меньше.

Защититься от подобных атак на сегодня почти невозможно. Именно мошенничества с биржами заставляют государства предпринимать регуляции. Так, в Китае все биржи были просто запрещены, но сделано это было не по причине технической беззащитности бирж от атак (это был только повод), а все же больше для регулирования обменных операций. Многие страны, очевидно, поступят так же. При этом многочисленные взломы бирж вряд ли прекратятся: слишком большое вознаграждение стоит за атакой. Защитой от таких рисков для пользователей может стать правило распределять риски между несколькими биржами. К сожалению, ведущие компании в области кибербезопасности только присматриваются к новой картине атак, а создатели криптобирж пока пренебрегают безопасностью в угоду быстрой прибыли. Очевидно, что

одним из шагов, которые предпримут в ближайшее время государственные органы различных стран, будет *введение серьезных регуляций по отношению к биржам, и прежде всего технических.*

На уровне теории *BlockChain* специалисты в области защиты информации предлагают целый набор средств на уровне логики выполнения транзакций, который мог бы сделать использование криптовалюты куда более безопасным. Приведем пример: на сегодня для совершения транзакции необходим номер кошелька пользователя и его секретный ключ. При частых операциях с ключем и идентификатором, очевидно, они могут быть целью атак хакеров. Но если каждый пользователь получит собственный ключ отмены транзакций, то львиную долю онлайн преступлений можно просто отменить. Ключ отмены транзакций может действовать, например, только 12 часов. Этого времени достаточно для отмены операции или отправки операции на «следственное мероприятие». То есть в случае массового обвала биржи при хищении все имеющие отношения транзакции могут быть отменены в течение 12 часов.

* * *

Проведенный анализ основных тенденций в сфере распространения криптовалют позволяет сделать следующие выводы.

Первый. В ближайшее время все больше стран будут вводить регуляции в области криптовалют, ориентируясь прежде всего на структуру собственной экономики.

Второй. С большой долей вероятности, регуляция начнется с государственных органов, которые перейдут к применению технологии *BlockChain,* где вводить требования будет проще всего.

Третий. Технически регуляция будет проходить через сертификацию аппаратных кошельков, используемых для работы с криптовалютами внутри различных стран. Сертифицированные аппаратные кошельки могут поддерживать несколько валют и в определенный момент могут начать поддерживать только одну из них (при удаленном обновлении прошивки).

Четвертый. Скорее всего, ни одна из стран не сможет ввести техническую регуляцию на уровне майнинга.