Диапазоны безопасности

Владимир ГЛОТОВ, Дмитрий МИХАЙЛОВ

ПРОБЛЕМЫ БЕЗОПАСНОСТИ КРИПТОВАЛЮТНЫХ СЕРВИСОВ

В настоящее время растет популярность использования технологии Blockchain и связанных с ней криптовалют. В Интернете все большую популярность набирают связанные с Blockchain сервисы, в т.ч. криптовалютные биржи, ICO-площадки. С ростом инвестиций в криптоактивы растет и внимание хакеров к данным технологиям, увеличивается количество специализированных атак, направленных именно на новые Blockchain-сервисы. Растущее внимание к новым технологиям наблюдается во всех странах мира. Не обошла эта тенденция и Российскую Федерацию, причем не только на общенациональном уровне, но и на уровне субъектов РФ. Однако интеграция технологий распределенных реестров в практику финансового и иного регулирования не сопровождается должным вниманием со стороны экспертов в области кибербезопасности. Между тем анализ складывающейся ситуации доказывает, что обеспечение экономической и политической безопасности страны и ее регионов требует самого пристального внимания к этому вопросу. В статье приводятся примеры возможных атак на криптовалютные сервисы, а также варианты защиты от подобных атак.

Ключевые слова: криптовалюта, криптовалютная биржа, криптовалютные миксеры, криптовалютная площадка, смартконтракт, токены, субъекты Российской Федерации, фиатные счета

JEL: C88, G28

Рост интереса к криптовалютам привел к нарастающему росту криптовалютных сервисов, предоставляющих услуги пользователям. Самыми популярными сервисами подобного типа являются криптовалютные биржи и площадки для *Initial Coin Offering* (далее — *ICO*). Набирают популярность также криптовалютные миксеры и другие площадки. Тем не менее именно биржи и *ICO*-площадки являются сегодня *наиболее посещаемыми ресурсами*.

Криптовалютная биржа (далее — криптобиржа) как информационный продукт состоит из компьютерного оборудования и программного обеспечения. Программная оболочка регистрирует пользователя и создает аккаунт, где он пополняет свои цифровые и фиатные счета, либо выводит деньги, размещает ордера на покупку и продажу. Многие биржи предоставляют дополнительные функции — чат, лента новостей, аналитика курсов и т.п.

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. В данной статье мы разберем виды атак на криптовалютные биржи и способы их защиты.

ICO — это криптовалютный аналог *IPO*[1] *и краудфандинга*[2]*, реализованный на базе технологии Blockchai*n.

Инвестиции в проекты с использованием криптовалют позволяют получить большие средства стартапам по всему миру. Любой стартап с помощью достаточно простой процедуры публичного заявления в сети Интернет может начать собирать деньги интернет-пользователей. Процедуру регулирования подобного рода сбора денег начинают регулировать разные страны.

К сожалению, не все стартапы на собранные деньги реализуют свои проекты. Некоторые просто исчезают с денежными средствами, но это не предмет нашего исследования. Интересна другая статистика. Согласно отчету *Chainalysis* (2017) немалая часть инвестиций в *ICO* достается мошенникам, причем *технологическим мошенникам*, жертвами которых становятся интернет-инвесторы.

По данным сервиса *Coindesk*, в 2017 г. в ходе *ICO* было привлечено 2 млрд долл. Ущерб же *ICO* инвесторам *Bloomber* оценил в 225 млн долл., а своих средств лишились 30 000 инвесторов. Конечно, это примерные оценки, так как не всю статистику плохо регулируемого мира ICO можно собрать, плюс колебания курса криптовалют вносят свои поправки.

Одна из крупнейших атак на *ICO* произошла в 2016 г., когда хакерам удалось взломать проект *DAO*. Сумма ущерба составила почти половину всех привлеченных средств — 74 млн долл. США.

Взлом криптовалютных бирж

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* (далее — *BTC*). Но даже при таком негативном опыте руководство биржи *MtGox* не сделало выводов в области кибербезопасности, и в начале 2014 г. 650 000 *BTC* (на февраль 2014 г. около 480 млн долл.) исчезли со счетов биржи. Состоявшийся суд над президентом *MtGox* Марком Карпелесом хотя и был важным прецедентом в правовом регулировании, но приговор в растрате и манипулировании данными не был вынесен, так как не было достаточно доказательств.

---

[1] Первое публичное предложение акций компании для продажи на бирже.
[2] Привлечение финансовых ресурсов от большого количества людей.

Атаки на биржи становятся все более частым явлением: биржа *Bitstamp* осталась без 20 000 *BTC* (что 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, что привело к обвалу курса *Bitcoin*. Это, пожалуй, стало вторым после взлома *MtGox* случаем взлома бирж, который так существенно повлиял на курс криптовалюты. По утверждениям биржи *Bitfinex* ей 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 новую тенденцию в мире кибербезопасности *Blockchain*. Теперь взломанные биржи все чаще начинают предлагать клиентам выпуск в счет долга специальных токенов, которые позже будут выкупаться по номиналу. Поскольку такие токены начинают свободно торговаться, то пользователи, скорее всего, их распродают по заниженной цене, не веря в восстановление биржы. 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. Так, *Bitfinex* компания решила компенсировать потери клиентов, но помимо этого предоставила им возможность обменять *Fei* на акции *Yapizon* на бирже *Yahoo Japan*.

DDoS (*distributed denial-of-service* — распределенная атака отказа в доступе) — одна из *самых распространенных компьютерных атак*. Ее алгоритм функционирования крайне прост: злоумышленник за счет множества различных подходов создает огромный трафик обращений к атакуемому ресурсу, ресурс с таким количеством обращений справиться не может, и в результате страдают обычные пользователи, которые не смогли получить доступ к ресурсу (сайту, сервису в сети Интернет).

С появлением *Blockchai*n хакеры стараются использовать уже существующие наработки и парадигмы и переложить их на новый лад для того, чтобы использовать возможности *Blockchain*, как правило, в части доступа к деньгам. Для *Blockchain* уже переработаны троянские программы, вирусы-вымогатели, принципы подделки сайтов. С *DDoS*-атакой все не так однозначно, и суть этой неоднозначности лежит в самой природе *Blockchain*.

Итак, *DDoS*-атака в *Blockchain* имеет свою классификацию по критерию объекта атаки. Фактически, *DDoS*-атака может быть направлена либо на саму распределенную систему вычислений или на онлайн-сервисы, которые строятся на базе данной распределенной системы.

Сразу скажем, что *DDoS*-атаки на саму распределенную систему вычислений затруднительны, если вообще возможны, в то время как атаки на онлайн-сервисы, которые строятся на базе данной распределенной системы, случаются достаточно часто.

Противоречие и путаница при оценке защищенности *Blockchain* от *DDoS*-атак возникают как раз из-за разницы в понимании того, что является объектом *DDoS*-атаки.

Разберем атаки на онлайн-сервисы, которые строятся на базе данной распределенной системы. Как правило, в случае с *Blockchain* предметом атаки становятся биржи криптовалют, так как они на сегодня слабо защищены, находятся зачастую в нерегулируемом государством поле и при этом обрабатывают огромное количество денежных операций. Часто целью *DDoS*-атаки является вымогательство. Злоумышленник просит заплатить отступные за то, чтобы прекратить атаку. Иногда *DDoS*-атаки делаются для дискредитации сервиса. Все эти цели традиционных *DDoS*-атак как нельзя лучше подходят для сервисов криптовалют: биржи, где торгуются криптовалюты, очень не любят оттока клиентов и часто готовы платить выкуп.

Надо сказать, что *DDoS*-атаки могут приводить к скачкам стоимости криптовалют. Даже новости об успешности *DDoS*-атак могут пошатнуть курс.

Так, 10 апреля 2013 г. криптовалюта *Bitcoin* обвалилась на 60 долл. — цена за 1 *BTC* колебалась и опустилась до 122 долл. Это произошло после того, как появилось сообщение о *DDoS*-атаке на сеть.

В феврале 2014 г. цена *Bitcoin* упала на 100 долл. после того, как несколько крупных бирж подверглись *DDoS*-атакам.

Но мошенники могут иметь не только финансовый интерес. Рынок криптовалют только формируется, в частности, появляются новые валюты и часто «разделяются» старые.

Так, в 2015 г. из-за споров по развитию криптовалюты *Bitcoin* (на каких технических принципах ее развивать) разразилась настоящая война в среде евангелистов системы. В это же время на ресурсы *Bitcoin* началась массированная *DDoS*-атака. Форум (*https://forum.bitcoin.com*), сам сайт, майнинговый пул были атакованы, и вряд ли злоумышленниками двигал финансовый интерес. Надо понимать, что мотивация евангелистов нового миропорядка в цифровом мире часто является близкой к мотивации фанатиков, что, безусловно, усложняет не только расследование инцидентов, но и добавляет потенциальные источники атаки.

Защититься от подобных атак *сегодня невозможно*.

Другой тип атак на криптовалютные биржи — кражи средств с таких ресурсов.

Информация о кражах с криптовалютных бирж поступает нередко, но на самом деле очень трудно проверить, действительно ли это результат хакерских атак. Возможно, недобросовестные создатели бирж сами задумали аферу и воплотили ее в жизнь, «утешив» вкладчиков тем, что был совершен взлом. А может быть, часть новостей о взломах — всего лишь попытка очернить конкурентов и способ привлечь

внимание? Однако факт остается фактом. Деньги с криптовалютных бирж время от времени пропадают, и их клиентам необходимо быть осторожными.

В ходе начавшегося краудсейла[3] криптовалютной платформы для трейдеров *Coindash*, сайт проекта *Coindash.io* был предположительно взломан, а адрес контракта *ICO* изменен на адрес взломщика. К моменту написания статьи на фальшивый адрес отправлено 43 438.45 *ETH*, что составляет 7 млн 420 тыс. долл. США по текущему курсу. На главной странице сайта размещено объявление о прекращении краудсейла. Организаторы проекта обещают всем отправившим *ETH* на фальшивый адрес компенсацию в токенах *CDT* (токен платформы *Coindash*).

В многочисленных комментариях отмечается, что вина за взлом полностью лежит на организаторах проекта по нескольким причинам.

Первая. Смартконтракт *ICO* не был опубликован заранее, а появился на сайте в день начала *ICO*. Организаторы проигнорировали многочисленные обращения с просьбами опубликовать смартконтракт и адрес заранее.

Вторая. Сайт проекта размещен на платформе *WordPress*, безопасность которой оставляет желать лучшего.

Третий. Команда проекта *CoinDash* ранее уже подозревалась в мошенничестве при подсчете голосов во время конкурса *Ether.camp*, в ходе которого она заняла первое место

Вызывает удивление тот факт, что средства на фальшивый адрес продолжали поступать *даже спустя три часа после объявления о взломе*. Такое пренебрежение безопасностью вызывает подозрение, что предполагаемый взлом — дело рук инсайдеров или даже организаторов проекта, репутация которых оставляет желать лучшего. Еще до скандальной истории с первым местом на *Ether.camp* основатели проекта оказались замешаны в мошенническом проекте *GETGEMZ*, о чем 7 мая предупреждали пользователи *Bitcointalk*. Интересным совпадением также выглядит тот факт, что взлом произошел за три дня до годовщины хардфорка Эфириума, вызванного ограблением *TheDAO*.

Взлом ICO-проектов

Самая распространенная атака на *ICO* — фишинг, когда преступники собирают деньги на свои кошельки, делая это от имени проекта. Мошенники создают сайты или учетные записи в социальных сетях с названиями, похожими на популярные ресурсы, привлекающие средства на *ICO*. Если, скажем проект называется *WOWMirror*, то мошенники могут использовать надпись *WOWMiror*. Всего одна буква не так заметна невнимательным пользователям. Особенно часто схема применяется с психологическим приемом ранней премиальной покупки токенов.

[3] Краудсейл — (от англ. *crowdsale, crowd* — «толпа», *sale* — «продажа») — коллективное сотрудничество людей, которое заключается в объединении их денег или других ресурсов с целью финансирования стартапов, проектов, кампаний других людей или организаций, выходящих на *ICO*.

Мошенники, отслеживая *ICO*, которые набирают популярность, высылают пользователям письма, где пишут об уникальной эксклюзивной возможности купить токены (вложить деньги) до официального старта, причем по очень низкой цене. В письмах указываются несколько типов ссылок:

- ссылка на сайт, отличающийся от оригинального[4];
- ссылка на сайт, который полностью имитирует настоящий, но, скажем, имеет отличие на одну букву в названии, как уже было показано выше на примере с *WOWMirror*;
- ссылка на ложный адрес электронного кошелька для перечисления денег.

Как правило, такие сообщения рассылаются в мессенджерах.

Характерный пример такого рода мошенничества — это *ICO* проекта *TEZOS*. За несколько часов до открытия *ICO* в сети распространились объявления о том, что *ICO* уже стартовало. Ссылка в сообщении вела не на сайт *tezos.com*, а на сайт *tezos.com.co*. Многие пользователи этого не замечали. Сайт выглядел полностью идентичным официальной странице проекта *TEZOS*. Кроме того, многие пользователи старались быстрее осуществить покупку, так как ложный сайт обещал очень большую скидку и просил ускориться с покупкой, так как время скидок было ограничено.

В примере с *TEZOS* и многими другими *ICO* пользователей обманывал тот факт, что высланная ссылка выглядит в точности как адрес ресурса. Но существует достаточно технологий, позволяющих спрятать внутри *html*-ссылки адрес совсем другой веб-страницы. После перехода по такой ссылке в браузере уже отражается реальный адрес, но пользователь часто забывает это проверить.

Еще один известный пример фишинговой атаки — *preICO Enigma Catalyst*, в ходе которого мошенники похитили около полумиллиона долларов.

Очень часто для усиления эффекта злоумышленники устраивают *DDoS*-атаку на реальный ресурс, подталкивая пользователя находить взамен такому ресурсу ресурс поддельный.

Часто мошенники прибегают к приему «кражи личности», когда личные странички в социальных сетях копируются злоумышленниками, заполняются реальным контентом пользователя (публично доступными фотографиями и т.д.). «Личности» крадут у уважаемых людей, сообщениям которых в социальных сетях с удовольствием верят наивные пользователи.

Одна из самых существенных проблем краж при *ICO* — это плохое регулирование данной области. Отсутствие регулирования *ICO* не накладывает обязательств перед инвесторами, в том числе в области безопасности. Аудиты проектов и смарт-контрактов не проводятся в должном объеме. Некоторые инициаторы *ICO* в случае хищения средств вообще скрывают сам факт, если мошенничество удалось

[4] Такой сайт создается самими мошенниками, но он создается под легендой предпродаж токенов (т.е. пока еще не открылся реальный сайт проекта по продажам токенов); он имеет произвольный дизайн и не имитирует реальный сайт.

обнаружить достаточно рано и ущерб от заявления об атаки может быть существенным.

Защитой против описанных фишинговых атак может быть специальный комплекс мер, который должен включать две составляющие. Во-первых, постоянный мониторинг доменов с созвучным именем. Ведь часто именно на него мошенники будут переводить трафик. Важным является тот факт, что подобный мониторинг может не только остановить, но и предупредить готовящуюся атаку.

Во-вторых, мониторинг форумов и социальных сетей, где может упоминаться проект и на которых могут даваться заведомо ложные данные. Подобный мониторинг также может позволить не только заблокировать, но и выявить подготовку к атаке.

Надо сказать, что мониторинг *не обязательно должен проводиться вручную*. Возможно создание специализированных программных комплексов по обеспечению безопасности *ICO* от фишинговых атак. Пользователям стоит также соблюдать стандартную бдительность при желании инвестиций в *ICO*.

Им следует внимательно проверять ссылки, на которые осуществлен переход. Например, в большинстве браузерах на непроверенных ресурсах можно увидеть перечеркнутый замочек на поддельных ресурсах. Пользователи не должны поддаваться порыву быстрого заработка и осуществлять непроверенные необдуманные действия. Важно внимательно проверять адреса электронных кошельков. И, наконец, использовать браузеры с встроенными расширениями по борьбе с фишингом, например, от *Google* или системы с использованием черных списков — *PhishTank* и *GeoTrust*.

Ключевая проблема *ICO*, как уже говорилось ранее, заключается в *отсутствии пока должного регулирования* процесса сбора денег в сети Интернет. Фактически, осуществить кражу при *ICO* могут и сами инициаторы *ICO*. Доказать это или защититься от такого сценария крайне сложно. Уязвимость, время запуска, детали *ICO*, очевидно, известны лучше всех инициаторам. Даже один ненадежный член команды может передать такую информацию дружественным злоумышленникам и тем самым привести к похищению средств.

Информация о кражах токенов с различных ресурсов поступает все чаще, но проверить, действительно ли это результат хакерских атак, *практически невозможно*. Существует множество косвенных данных, позволяющих утверждать, что недобросовестные создатели бирж или фондов сами задумали мошенничество и воплотили план в жизнь, а вкладчикам объявили, что виноваты загадочные злоумышленники.

Еще одна методика мошенников — это *социальная инженерия*, т.е. использование знаний об атакуемом пользователе, его психологии для осуществления целенаправленной компьютерной атаки.

Известные и доступные методы социальной инженерии можно разбирать бесконечно. Самый частый пример — подброшенная флешка. Многие пользователи найденную флешку непременно вставят в свой компьютер, очистят и будут использовать как свою. Приятный подарок. Проблема тем не менее заключается в том, что на таких флешках часто

находится вирус, установку которого пользователь не заметит. В мире атак на криптовалюты такие вирусы уже умеют похищать содержание кошельков пользователей криптовалют, как уже было разобрано в предыдущих главах. Но это далеко не единственный пример.

Ссылки на ложные сайты *ICO* — результат фишинговых атак, разобранный ранее — это также пример социальной инженерии, если рассылка идет таргетированным образом, а в письме или посте в социальных сетях упоминается личная информация пользователя, которая побуждает его открыть ссылку. Социальная инженерия требует внимательного предварительного изучения объекта атаки.

Сделать обзор или разобрать все возможные атаки с использованием социальной инженерии крайне сложно ввиду изобретательности мошенников. Мы разберем один яркий и характерный пример, коснувшийся тысяч пользователей мира криптовалют.

В 2016 г. крупнейшая криптовалютная биржа в Южной Корее *Bithumb потеряла около миллиарда вон* в результате взлома, кроме того биржа позволила утечь в сеть персональным данным около 30 тысяч пользователей *Bithumb*.

Расследование инцидента показало, что крупнейшее опустошение биржи и кошельков пользователей произошло ввиду успешной атаки на самое слабое звено всей системы — персональный компьютер, принадлежащий сотруднику компании. Не был заражен сервер биржи, не был взломан сайт. Просто с использованием методов социальной инженерии мошенники смогли получить полный контроль над компьютером сотрудника. Сотруднику подбросили флешку с вирусом, прекрасно зная административные привилегии его компьютера. Имея компьютер-инсайдер в управлении биржи, злоумышленники смогли получить доступ ко всем необходимым для хищения денег механизмам.

Интересен и другой факт об этой же бирже — *Bithumb*.

Помимо взлома самой биржи преступники использовали социальную инженерию и для получения доступа к кошелькам пользователей. Мошенники звонили по телефону зарегистрированным пользователям биржи и просили продиктовать одноразовый пароль, который приходил с официальной почты биржи *Bithumb*. Многие пользователи откликнулись на просьбы и потеряли все свои деньги.

Как мы видим, мошенники все лучше изучают объекты атаки в криптвалютной индустрии и применяют методы социальной инженерии все чаще.

Защищаться от социальной инженерии крайне сложно. Любая атака с использованием такой тактики *практически всегда уникальна*, а часто рассчитана на индивидуальную психологию жертвы. Только личная бдительность и повышение уровня компьютерной грамотности могут помочь пользователям не стать жертвой атаки. К сожалению, даже самый искушенный пользователь может стать жертвой мошенничества, если близорукость проявит другой член *Blockchain*-сообщества, как показал разобранный южнокорейский пример.

* * *

Количество атак, направленных на уязвимость криптовалютных бирж и *ICO*-площадок, будет увеличиваться с течением времени: слишком большое вознаграждение стоит за атакой. Защитой от таких рисков в части бирж 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. В случаях с *ICO* изменение ситуации возможно только при условии появления более строгих регуляций и развития механизмов проверок и аудитов *ICO*-платформ, что будет востребовано только после соответствующих обязательных для проектов проверок и аудитов.

Список литературы

1. Хакеры распробовали DDoS-атаки на криптовалютные биржи, сайт газеты «Ведомости»/ URL: https://www.vedomosti.ru/technology/articles/2017/11/09/741036-hakeri-rasprobovali-ddos-ataki

2. Major DDOS attack hit Bitcoin.com, новостной портал News Bitcoin. URL: https://news.bitcoin.com/ddos-attacks-bitcoin-com-uncensored-information/

3. Русскоязычный информационный сайт Bitcoin. URL: https://bits.media/mtgox-koloss-na-koshachikh-lapkakh

SECURITY PROBLEMS OF CRYPTO-CURRENCY SERVICES

Currently, both BlockChain technology itself and crypto-currencies, associated with this technology, are growing in popularity. In the Internet, the services related to BlockChain are gaining more and more popularity, including crypto-exchanges, ICO-sites. With the growth of investments in crypto assets, the attention of hackers to these technologies also grows; the number of specialized attacks directed namely at new BlockChain services is increasing. The growing attention to new technologies can be seen in all countries. This tendency hasn't passed by Russian Federation — both at the all-national level and at the level of the subjects of the Federation. However, active integration of BlockChain technologies into the practice of financial and other regulation is not currently accompanied by the due attention of the experts in the sphere of cybersecurity. The analysis of the actual situation shows that the provision of economic and political security of the country demands watchful attention to this question. The article provides the examples of possible attacks on crypto-currency services as well as the options for the protection against such attacks.

Keywords: crypto-currency, crypto-currency exchange, crypto-currency mixers, crypto-exchange platform, smart contract, tokens, subjects of the Russian Federation, fiat accounts

JEL: C88, G28

Дата поступления — 19.03.2018 г.

ГЛОТОВ Владимир Иванович
кандидат экономических наук, профессор, заведующий лабораторией финансового мониторинга;
Федеральное государственное бюджетное учреждение науки Институт социально-политических исследований РАН / 119333, Москва, ул. Фотиевой, д. 6, к. 1.
e-mail: professor.ispi.ran@gmail.com

GLOTOV Vladimir I.
Cand. Sc. (Econ.), Professor; Head of the Laboratory of Financial Monitoring; Federal State Budgetary Institute of Science Institute of Socio-Political Research, RAS / 6, building 1, Fotieva St., Moscow, 119333.
e-mail: professor.ispi.ran@gmail.com

МИХАЙЛОВ Дмитрий Михайлович
кандидат технических наук, доцент;
Федеральное государственное бюджетное образовательное учреждение высшего образования Московский государственный технический университет им. Н.Э. Баумана / 105005 г. Москва, 2-я Бауманская ул., д. 5, стр. 1.
e-mail: dm@esc-center.ru

MIKHAYLOV Dmitry M.
Cand. Sc. (Technics), Associate Professor;
Federal State Budgetary Institute of Higher Education Bauman Moscow State Technical University / 5, building 1, 2nd Bauman Str., Moscow, 105005.
e-mail: dm@esc-center.ru

Для цитирования
Глотов В., Михайлов Д. Проблемы безопасности криптовалютных сервисов // Федерализм. 2018. № 1. С. 134—143.