DOI 10.37882/2223–2966.2022.06–2.11

МОДЕЛИ ХРАНЕНИЯ ЦИФРОВЫХ ФИНАНСОВЫХ АКТИВОВ: АНАЛИЗ УГРОЗ И КОНТРМЕРЫ

Диамонд Карильо Джосет Моисес
Аспирант, Финансовый университет при Правительстве РФ
diamondjmd@yandex.ru

Аннотация. Безопасность цифровых финансовых активов зависит от технологии криптовалютных кошельков. В настоящее время на рынке существует множество моделей хранения цифровых финансовых активов, многие из которых наносят ущерб их владельцам из-за слабой безопасности. В данной статье анализируются уязвимости и угрозы, доступные на рынке криптовалютных кошельков. Кроме того, мы разработали рекомендации по противодействию хищению информации и контрмеры направленные на защиту криптокошельков от угроз.

Ключевые слова: электронный кошелек, блокчейн, криптовалюта, криптосейф, холодный и горячий кошелек, толстый клиент, тонкий клиент.

MODELS FOR DIGITAL FINANCIAL ASSETS: THREATS ANALYSIS AND COUNTERMEASURES

Diamond Carrillo Joseth Moises

Summary. The security of digital financial assets depends on the technology of cryptocurrency wallets. Currently, there are many models of storing digital financial assets on the market, many of which harm their owners due to weak security. This article analyzes vulnerabilities and threats available on the cryptocurrency wallet market. In addition, we have developed recommendations on countering information theft and countermeasures aimed at protecting crypto wallets from threats.

Keywords: electronic wallet, blockchain, cryptocurrency, cryptosafe, cold and hot wallet, fat client, thin client.

Введение

В связи с популяризацией и развитием блокчейн — технологий и криптовалют приобретает актуальность вопрос, связанный с обеспечением безопасности их хранения и совершением финансовых операций. Всю совокупность угроз, сопряженных с информационной безопасностью, можно подразделить на три вида:

- антропогенные источники, связанные с действиями, проводимыми субъектом;
- техногенные источники, связанные с применяемыми техническими средствами;
- стихийные источники, сопряженные с действием природных явлений.

Принципиальным отличием криптовалюты от фиатных денежных средств является существование в формате цифрового актива — в этой связи возникает необходимость применения специализированных универсальных кошельков, иными словами, электронного кошелька. Однако даже с его применением обналичивание криптовалюты остается невозможным — проведение всех операций осуществляется посредством сети интернет, что побуждает к необходимости выбора кошелька, обеспечивающего, с одной стороны, возможность хранения актива, а с другой стороны, доступ к широкому набору сервисов и возможностей.

На сегодняшний день вопросам блокчейн — технологий, криптовалют и электронных кошельков посвящено множество литературных и интернет- источников, например, это работы Брайана Патрика Эха, Натаниэля Поппера, Андреаса М. Антонопулоса, Алекса Преукшата, Жозупа Бускета, Ареса Хосе Анхеля, Александра Шульгинова, Андрея Урлина, Михаила Смирнова, Руслана Акста, Михаила Лебедя, Сары К. Тейлор, Хайрула Акрама Зайнола Ариффина, Конга Ли и многих других. Вместе с тем развитие цифровой экономики не останавливается, в связи с чем на смену существующих угроз информационной безопасности приходят обновленные, что требует постоянного развития данного вопроса и совершенствования применяемых контрмероприятий.

Целью данной статьи является анализ существующих в настоящее время моделей хранения цифровых финансовых активов с точки зрения присущих им угроз информационной безопасности, а также поиск адекватных контрмер, направленных на нивелирование указанных угроз.

Для достижения цели исследования последовательно будут решены следующие задачи:

1. рассмотреть многообразие существующих на рынке моделей хранения цифровых финансовых активов (криптовалюты);
2. провести анализ техногенных и антропогенных уязвимостей и угроз в интересах формирования средств противодействия хищения информации;
3. разработать рекомендации по противодействию хищению информации и контрмеры направленные на защиту криптокошельков от угроз;
4. проанализировать кошелек, используемый в Венесуэле для хранения национальной криптовалюты Petro, выявить присущие ему потенциальные угрозы и возможные контрмеры, направленные на их минимизацию.

В самом общем смысле, криптовалютный кошелек представляет собой приложение или устройство, способное обеспечить сохранение конфиденциальной информации, доступность системы блокчейн для пользователя и возможность участия в сделках посредством сети [6].

В число наиболее популярных сервисов, имеющих формат электронного кошелька, относятся следующие программные средства, способствующие безопасному хранению данных [4]:

1. Десктопные решения, работающие в формате «толстого клиента», предполагающего присутствие программы на жестком диске компьютера, либо «тонкого клиента», ориентированного на использование удаленных серверов;
2. Аппаратные криптосейфы;
3. Специализированные приложения, устанавливаемые на мобильные устройства;
4. Интернет — хранилища, осуществляющие работу в формате онлайн;
5. Депозитные счета, открытые на криптовалютных биржевых площадках.

Первоначально возникшие хранилища криптовалюты были моновалютными, на текущий момент развитие электронных кошельков фокусируется на принципах мультивалютного хранения, использующем различные программные алгоритмы.

Электронный кошелек, отличающийся качеством и надежностью, должен обеспечивать высокие стандарты безопасности данных для предотвращения к ним несанкционированного доступа третьих лиц, а также обладать следующими отличительными характеристиками:

- наличие двух ключей — как приватного, так и публичного;
- многоступенчатой системой защиты.

Существует достаточно широкая классификация типов электронных кошельков.

Так, по способу хранения данных различаются холодные и горячие кошельки. Упоминание температуры в данном случае указывает на взаимосвязь с технологией блокчейн — в случае холодного кошелька работа осуществляется без непрерывного доступа к сети интернет, при использовании горячего доступ к сети должен быть обеспечен непрерывно.

Горячие кошельки подразделяются на локальные (существует в формате устанавливаемой на компьютер программы), мобильные (представляют собой мобильные приложения) и работающие в формате онлайн (сервисы, в том числе биржевые аккаунты, и криптовалютные счета, внедренные в структуру международных платежных систем). Принцип действия горячего кошелька заключается в загрузке на компьютер специализированной программной среды, позволяющей осуществлять работу с сервисами блокчейн.

К числу преимуществ горячего типа кошельков, по мнению экспертов редакции Profinvestment.com, могут быть отнесены следующие факторы [8]:

- для использования системы не требуется оплата;
- доступ к данным осуществляется на мгновенной основе в момент запуска программы;
- работа с программой осуществляется на принципах максимальной простоты и удобства;
- программа предлагает пользователю расширенный набор дополнительных функций и средств;
- программа поддерживает разнообразные виды монет и токенов.

Самым серьезным недостатком горячего типа кошелька, по нашему мнению, является низкая степень безопасности в связи с повсеместным использованием сети интернет. Также главный редактор платформы Crypto.ru Ищенко В [6]. к числу существенных недостатков горячего кошелька относит риски, существующие в связи с возможностью утери данных по причине сбоя в работе сервиса.

Самыми известными примерами горячих кошельков являются Blockchain.com и Jaxx.

При помощи кошелька Blockchain осуществляется работа с такими криптовалютами, как Bitcoin (BTC), Ethereumr (ETH), Bitcoin Cash (BCH), Stellar (XLM), USD Digital (USD-D) и рядом других. Данный горячий кошелек может быть как мобильного типа, так и онлайн типа. К существенным преимуществам данного вида кошелька относится возможность резервирования ключа, предоставление широкого ассортимента дополнительных

услуг (например, биржевой обмен криптовалют, перевод денег между кошельками с минимальной комиссией, доступность ресурса на большинстве мировых языках).

Горячий кошелек Jaxx также относится к кошелкам как мобильного типа, так и типа онлайн. К числу преимуществ относится поддержка разнообразных и редких криптовалют, отсутствие требования по прохождению регистрации, наличие новостного приложения, биржевых сервисов и инструментов, позволяющих управлять портфелем.

Холодные кошельки в свою очередь подразделяются на бумажные (предполагает ручную запись пароля на бумажном носителе и ввод в систему при каждом последующем входе в нее), аппаратные (наличие внешнего устройства, схожего по внешнему виду с флешкой, на которой осуществляется хранение личных ключей) и локальные (кошельки на персональных компьютерах и мобильных устройствах, не имеющих доступа к сети интернет).

Холодный кошелек представляется самым надежным способом хранения информации, что является его несомненным преимуществом. Однако данный вид кошелька не лишен недостатков, к числу которых можно отнести высокую стоимость аппаратных устройств и неудобство для проведения частых сделок. Примерами холодных кошельков являются такие системы, как Ledger, Trezor и сайт bitaddress.org, способствующий созданию пароля для бумажной разновидности кошелька.

Холодный кошелек Ledger относится либо к аппаратному, либо к локальному типу. Основными его преимуществами является возможность работы с разнообразием криптоактивов, обеспечение высокого уровня безопасности данных, наличие сертификации и проверки подлинности от подделки либо несанкционированного доступа третьей стороны. Различаются кошельки Ledger Nano S и Ledger Nano X — данные системы отличаются размером памяти, стоимостными параметрами и наличием возможности подключения к Bluetooth, кроме того, у кошелька размера S могут возникать сложности с проведением транзакций небольшого объема.

Холодный кошелек Trezor относится к аппаратному типу. Существенным преимуществом данного кошелька является работа с большим количеством криптовалют, наличие высоких стандартов безопасности, простота использования. Среди кошельков Trezor также различаются типы Trezor One и Trezor Model T — существенными недостатками указанных систем является наличие большого количества подделок.

Обобщающими преимуществами аппаратных электронных кошельков, по мнению экспертов платформы Profinvestment.com, является [2]:

- наличие высоких стандартов, обеспечивающих безопасность хранения данных, и защитных механизмов (PIN-код, биометрия);
- мобильность, возможность перемещения устройства;
- наличие защиты от неблагоприятных факторов внешней среды.

К числу основных сложностей могут быть отнесены, как уже было отмечено ранее, высокие затраты на приобретение оборудования, а также периодически возникающие неудобства в связи с отправкой транзакций.

В качестве основного критерия при выборе онлайн — кошелька выступает обеспечение безопасного хранения электронного ключа. На проверенных сайтах доступна технология хеширования данных клиента и сервера, позволяющая нивелировать риски, связанные с утечкой личной информации.

К числу основных преимуществ онлайн — кошельков относится [6]:

- возможность быстрого доступа посредством браузера;
- автономность от работы операционной системы и жесткого диска компьютера;
- снижение риска взаимодействия с вредоносным программным обеспечением;
- возможность совершения транзакции с любого устройства без ограничения.

Однако указанный тип кошелька не лишен недостатков, к числу которых относятся:

- риск похищения ключей в связи с их хранением на сервере;
- возможность спутать доступ к сайту с фишинговой ссылкой, в результате чего повышается риск, связанный с мошенничеством;
- возможности сбоев на сервере, в связи с чем нарушение в проведении транзакции.

Следующим вариантом классификации электронных кошельков является осуществление работы по принципу толстого и тонкого клиента [3]:

- «толстый» кошелек загружает в компьютерную систему весь существующий блокчейн с целью обеспечения полной синхронизации. Сделка проводится в условиях безопасности в связи с отсутствием обращения к посредническим сервисам. К основным слабостям толстого криптокошелька относятся осуществление работы на низких скоростях и наличие повышенных тре-

Таблица 1. Результаты анализа техногенных и антропогенных уязвимостей и угроз криптокошельков

Тип угрозы	Гор. Локальные кошки	Гор. мобильные кошки	Гор. онлайн кошки	Хол. бумажные кошки	Хол. аппаратные кошки	Хол. локальные кошки	Дескт. решения (тонкий кл.)	Дескт. решения (толстый кл.)
АНТРОПОГЕННЫЕ УГРОЗЫ								
Умышл. Действия внешн. Субъек-тов	+	+	+	-	-	-	+	-
Умышл. Действия внутр. субъек-тов	+	+	+	-	-	-	+	-
Случ. Действия внешн. субъек-тов	-	-	-	-	-	-	-	-
Случ. действия внутр. Субъек-тов	-	-	-	-	-	-	-	-
ТЕХНОГЕННЫЕ УГРОЗЫ								
Внешн. технич. угрозы	+	+	+	-	-	-	+	-
Внутр. Технич. угрозы	-	-	-	-	-	-	-	+

(Составлено автором)

бований к устройству, обладающему памятью (например, жесткому диску). Сильными сторонами данного вида кошелька является прохождение сверки информации, отраженной в нем, с иными сетевыми узлами. К числу самых популярных программ, работающих по принципу «толстого клиента», относятся Bitcoin Core, Specter, Armory [6].

- «тонкий» кошелек представляет собой облегченный вариант программы, поскольку скачивание блокчейна не производится, в случае необходимости осуществляется соединение с сетевыми сервисами. Тонкие кошельки обладают меньшей безопасностью в связи с обращением к посредническим сервисам.

Среди мобильных электронных кошельков классификация производится по типу поддерживаемой операционной системы. По состоянию на июнь 2021 года, распространение операционной системы Android достигло лидерства по числу пользователей, а величина рыночной доли превысила 75%. Одним из лучших электронных криптокошельков, совместимых с операционной системой Android, является Crypto.com, поддерживающий разнообразное количество криптовалют и позволяющий инвесторам получать заработок на процессах лендинга и стекинга. Программа предназначена для осуществления децентрализованного обмена криптовалют. Совместимость программ достигается на базе операционной системы Android Crypto.com DeFi Wallet [6,7].

К числу лучших электронных кошельков, совместимых с операционной системой iOS, относится Trustee Wallet, являющийся мультивалютным решением для биткойнов и альткойнов. Сильными сторонами программы является возможность получения и хранения NFT, а также проведение обменных операций на рубли и иные фиатные валюты.

Обобщим результаты проведенного анализа техногенных и антропогенных уязвимостей и угроз в интересах формирования средств противодействия хищения информации в таблице 1.

Наибольший интерес с точки зрения информационной безопасности представляют антропогенные угрозы, так как действия субъекта (нарушителя) могут быть спрогнозированы и предотвращены. Техногенные угрозы предвидеть достаточно сложно в связи с их масштабностью и непредсказуемостью, их предотвращение напрямую связано с мероприятиями информационной безопасности.

Также для криптовалютных кошельков продолжают оставаться актуальными вредоносные вирусные атаки, например, похищение денежных средств из кошелька пользователя криптовалют посредством вируса-трояна, осуществление несанкционированного проникновения в горячий кошелек пользователя посредством вируса-вымогателя, использование вредоносного вирусного

программного обеспечения для осуществления майнинговых операций [5].

Рекомендуются следующие мероприятия, входящие в число контрмер угроз информационной безопасности криптокошельков:

1. использовать отдельный электронный адрес и сим-карту мобильного устройства, применяемые для осуществления операций с криптовалютными сервисами;
2. применять последовательность действий, связанную с распределением активов:

а) не осуществлять хранение крупных сумм цифровой валюты на криптовалютных биржах в связи с риском проведения хакерской атаки;

б) осуществлять хранение приобретенных на длительный срок биткоинов и альткоинов на кошельках, относящихся к холодному типу либо к аппаратному;

в) на криптобиржах поддерживать объем монет, достаточный для проведения торговой операции;

г) с целью защиты всего объема денежных средств производить диверсификацию криптовалютных активов кратно разным кошелькам;

3. своевременно обновлять программное обеспечение до новейших версий;
4. применять качественное и эффективное антивирусное программное обеспечение, осуществлять его своевременное обновление;
5. использовать дополнительные средства, направленные на обеспечение безопасности, к примеру, технологии аутентификации посредством двух факторов;
6. использовать кошельки с возможностью мультиподписи, осуществляющей процесс идентификации субъекта транзакции с двух или более не связанных между собой устройств;
7. производить резервное копирование кошелька, производить хранение закрытых ключей и кодовых фраз в максимально надежном месте, существующем оффлайн;
8. принимать во внимание репутационную характеристику компании, создавшей электронный кошелек.

Одной из популярных в настоящее время является криптовалюта Petro, действующая в Венесуэле. Для осуществления операций с данной криптовалютой создан специализированный электронный кошелек Petro [1; 9], существующий в онлайн — формате и в формате мобильного приложения (платформа PetroApp, для регистрации достаточно ввести адрес электронной почты и пароль), позволяющий пользователям приобретать валюту и осуществлять торговлю ею на авторизованных биржах, к числу которых относятся Amberes, Bancar и Criptolag, обменивать криптовалюты на фиатные денежные средства либо на другие криптовалюты. Электронный кошелек Petro взаимосвязан с цифровой биржей и национальной банковской сетью, что упрощает процесс операций по купле-продаже валют и их обмену. Еще одной полезной функцией, доступной в цифровом кошельке, является обновленный калькулятор Petro.

Безопасность операций электронного кошелька Petro обеспечивается посредством проверки личности (при проведении операций система запрашивает соответствующие документы), а также наличием буквенно-цифрового кода аутентификации, состоящего из шести символов, чувствительного к регистру. Действие кода продолжается пятнадцать минут, каждая последующая попытка входа требует его обновления. Посредством данного цифрового пароля при вводе обеспечивается проверка каждой инициированной сессии. Данное средство безопасности направлено на защиту интересов пользователей службы от возможных мошеннических операций с использованием личных данных. Также безопасность операций с криптовалютами обеспечивается за счет того, что национальное агентство Sunacrip отслеживает деятельность поставщиков услуг виртуальных активов и может отзывать лицензии у тех из них, кто не соблюдает правовые нормы комплексной криптоактивной системы (таким примером могут быть организации Criptomundo и Cave Blockchain). Пользователям не рекомендуется осуществлять операции с организациями, не прошедшими авторизацию в национальном агентстве Sunacrip. Однако в связи с тем, что электронный кошелек Petro относится к онлайн — типу, ему по-прежнему присущи угрозы, связанные с действием антропогенных сил (внешние и внутренние, обусловленные умышленными действиями субъектов), в этой связи для минимизации угроз к нему применимы мероприятия информационной безопасности, рассмотренные в статье выше.

Выводы

В данной статье были рассмотрены основные классификации и виды существующих электронных кошельков (холодные и горячие, работающие по принципу толстого и тонкого клиента, электронные кошельки, опирающиеся на операционную систему iOS и Android) с точки зрения имеющихся у них преимуществ и недостатков, а также присущих им техногенных и антропогенных уязвимостей и угроз. В результате проведенного анализа было выявлено, что наиболее безопасными для хранения криптовалюты являются холодные кошельки бумажного, аппаратного и электронного типа — они не подвержены внутренним и внешним антропогенным и техногенным угрозам ввиду действующих для них стандартов безопасности, однако обладают также се-

рьезными недостатками, такими как дороговизна аппаратных устройств и неудобство в случае необходимости проведения сделок часто.

Несмотря на достаточное развитие технологий блокчейн и появление широкого ассортимента криптокошельков, обладающих различными характеристиками, в большинстве случаев достаточно существенно влияющими на них угрозами остаются угрозы антропогенного и техногенного характера. На текущий момент данная группа угроз не представляет значения только для холодных кошельков, для остальных необходима проработка действующих, способных приносить устойчивый эффект мероприятий информационной безопасности.

Также в данной статье с точки зрения классификации и возможного действия внутренних и внешних угроз рассмотрен электронный кошелек для национальной валюты Венесуэлы Petro. Было выявлено, что для данного типа кошелька приняты достаточно серьезные меры защиты, однако его приверженность к онлайн — типу делает его уязвимым для угроз, связанных с действием антропогенных сил, что побуждает к принятию комплексных мер, направленных на их предотвращение, описанных в данной статье.

ЛИТЕРАТУРА

1. Jose Antonio Lanz Venezuela's largest bank opens up petro cryptocurrency wallet registrations // Electronic source: https://finance.yahoo.com/news/venezuelas-largest-bank-opens-petro-202518019.html
2. Аппаратные кошельки для криптовалют: обзор криптокошельков Ledger, Trezor, Safepal, Keepkey, CoolWallet и других // Электронный источник: https://profinvestment.com
3. Биткоин-кошелек: выбор хранилища и инструкция по использованию // Электронный источник: https://kurs-bitcoina.ru/bitcoin-koshelek/#i-10
4. Выбор лучшего мультивалютного кошелька для криптовалюты на 2021 год // Электронный источник: https://mycryptocurrency24.com/sposoby-vyvoda-deneg/vybor-luchshego-multivalyutnogo-koshelka-dlya-kriptovalyuty-na-2020-god
5. Глотов В.И., Михайлов Д.М. Минимизация рисков в кредитно-финансовой сфере (блокчейн).— Экономика. Налоги. Право.— 2017.— № 6.— с. 16–23.
6. Ищенко В. Рейтинг лучших кошельков для криптовалюты // Электронный источник: https://crypto.ru/koshelki-kriptovalyut
7. Конг Ли, Daojing He, Сенкун Чжу, Сэмми Чан Яо Ченг Криптовалютные кошельки на базе Android: атаки и Контрмеры.— Международная конференция IEEE по блокчейну (Блокчейн).— 2020.
8. Холодные и горячие криптовалютные кошельки: обзор, примеры, преимущества и недостатки // Электронный источник: https://profinvestment.com
9. Официальный сайт Petro // Электронный источник: http://www.petro.gob.ve/

Журнал «Современная наука: актуальные проблемы теории и практики»