УДК 004.77

ТЕНДЕНЦИИ РАЗВИТИЯ КИБЕРАТАК НА КРИПТОБИРЖИ

Петров И. А.

Финансовый университет при Правительстве РФ, Москва, Россия, Москва

Статья поступила 28.08.2025, принята к публикации 30.09.2025. Опубликована онлайн.

Аннотация. В современном мире происходит стремительное развитие различных типов финансовых активов. Долгое время существовала лишь наличная форма денег, пару десятилетий назад в нашу жизнь вошли безналичные деньги, сейчас не за горами ввод третьей формы денег – цифровые деньги. Однако, их введение содержит много опасностей и вызовов. Одним из таких вызовов являются кибератаки. Каждый год в мире происходит огромное количество преступлений в сфере информационной безопасности, преступления, связанные с криптовалютами являются одними из самых громких и наиболее масштабных. Целью статьи является создание прогноза по ущербу от кибератак на криптобиржи при помощи математических моделей. Будет произведен анализ киберпреступлений относительно их суммарного ущерба. Разумеется, абсолютно полный анализ кибератак на криптобиржи невозможен, поскольку не все атаки на криптобиржи обнародованы во избежание репутационных потерь, однако самые крупные и масштабные безусловно известны и будут рассмотрены в данной статье. Новым словом в финансах стали цифровые валюты центральных банков, которые имеют как сходства, так и различия с криптовалютами. Главным является то, что оба актива функционируют на основе распределенного реестра и имеют общие проблемы кибербезопасности.

Ключевые слова: киберпреступления, кибератаки, криптовалюты, криптобиржи, фишинг, DDoS-атаки, мошенничество

TRENDS IN THE DEVELOPMENT OF CYBERATTACKS ON CRYPTO EXCHANGES

Петров И. А.

University under The Government of Russian Federation, Moscow, Russia

Abstract. There is a rapid development of various types of financial assets in the modern world. For a long time, there was only a cash form of money, a couple of decades ago, non–cash money entered our lives, and now the introduction of a third form of money, digital money, is just around the corner. However, their introduction contains many dangers and challenges. Cyberattacks are one of these challenges. Every year, a huge number of crimes in the field of information security occur in the world, crimes related to cryptocurrencies are among the loudest and most widespread. The purpose of the article is to create a forecast of damage from cyberattacks on crypto exchanges using mathematical models.

An analysis of cybercrimes regarding their total damage will be carried out. Of course, an absolutely complete analysis of cyberattacks on crypto exchanges is impossible, since not all attacks on crypto exchanges have been made public in order to avoid reputational losses, but the largest and most extensive ones are certainly known and will be discussed in this article.

Central bank digital currencies, which have both similarities and differences with cryptocurrencies, have become a new word in finance. The main thing is that both assets operate on the basis of a distributed registry and have common cybersecurity issues.

Keywords: cybercrime, cyberattacks, cryptocurrencies, cryptocurrency exchanges, phishing, DDoS attacks, scams

Введение

Криптовалюты были одними из первых инструментов, которые были созданы на основе технологии распределенного реестра (ТРР). У данной технологии достаточно достоинств, которые сделали популярными и технологию распределенного реестра и криптовалюты, которые функционируют на основе ТРР.

Самой популярной и известной криптовалютой является биткоин. Однако, популярность роста популярности криптовалют беспокоит правительства многих стран.

Особую озабоченность вызвал анонс криптовалюты Libra [1]. Потенциально этой валютой могли пользоваться миллиарды людей, что стало бы серьезным вызовом для мировой финансовой системы.

Понимая достоинства и недостатки криптовалют, правительства различных государств решили ввести новую форму денег – цифровую валюту, эмиссией которой будет заниматься государство.

Криптовалюты и цифровые валюты центральных банков имеют много схожих черт, а потому и угрозы информационной безопасности будут схожими. Поэтому в данной статье будет проанализированы многие известные кибератаки на криптобиржи. Будет исследовано как они производились, к каким последствиям привели.

Целью исследования являются тенденции развития кибератак на криптобиржи. Методом исследования являются синтез, анализ, обобщение. Актуальность исследования заключается в том, что в 2024 году цифровые валюты центральных банков проходят тестирования в некоторых государствах, в частности, в России, и аспект безопасности является ключевым.

Достоинства криптовалют

Для начала постараемся понять феномен криптовалют, почему они стали так популярны.

Достоинствами ТРР, а, следовательно, и криптовалют, являются:

– Возможность проведения анонимных транзакций;

– Низкие комиссии за перевод денежных средств;

– Отсутствие контроля над операциями у государственных органов;

– Безопасность и скорость проведения транзакций.

На волне роста популярности криптовалют, их стоимость многократно возросла. Развитие рынка ЦФА началось в 2009 году. В этот год была выпущена первая криптовалюта, которая регулируется математическими законами. Такая особенность криптовалют позволила осуществлять транзакции с большей безопасностью и шифрованием.

В 2010 году была открыта первая биржа, на которой осуществлялось обращение криптовалют. На рис. 1 приведен график, на котором показан курс криптовалюты Bitcoin.

Как видно из графика, взрывной рост курса начался примерно в середине 2017 года. К этому времени, помимо биткоина, существовало более сотни других криптовалют, которые также начали свой быстрый рост.

Рис. 1. Курс биткоина в долларах США

Эмиссия криптовалют осуществляется различными способами и в каждом из этих способов существуют свои проблемы и уязвимости. Далее рассмотрим более подробно эти способы.

1. ICO. Initial Coin Offering (первичное размещение токенов). Данный процесс схож с традиционным IPO (Initial Public Offering) - первое публичное размещение акций. Только в случае с ICO происходит первое публичное размещение токенов криптовалюты. Пользователь криптовалюты платит определенное количество денег компании, которая осуществляет эмиссию определенной криптовалюты, и получает взамен токены. Токены можно купить как за обычные, фиатные деньги, так и за другие криптовалюты. В зависимости от условий ICO и вида токена, инвестор получает часть прибыли компании либо проценты по займу. Далее инвестор может купить какой-нибудь товар или услуги за данный токен, или продать его в расчете на прибыль. Однако, ICO далеко не всегда приносит прибыль своим инвесторам. На рис. 2 показаны самые успешные ICO и самые неудачные.

.

Рис. 2. Самые успешные и провальные ICO

Как можно понять из рисунка 2, количество убыточных ICO гораздо больше, чем прибыльных. Статистику по ICO за 2023 год можно посмотреть на портале ЦБ РФ. [2] Самым прибыльным ICO на момент 2024 года является ICO Etherium. 7 августа 2015 года Etherium был добавлен на криптобиржу Kraken. Тогда стоимость одного токена составляла 2,77 доллара США. На данный момент цена держится в районе 3500 долларов США.

2. IEO. Initial Exchange Offering (первичное биржевое размещение). В данном случае речь идет о централизованные криптовалютные биржи. Примерами таких бирж являются Binance и Coinbase. Биржи подчиняются законам конкретных стран, обычно это либо США, либо ЕС. Они сотрудничают с регуляторами, у них существуют идентификация клиентов, и биржи могут защищать активы своих клиентов.

3. IDO. Initial DEX Offering (первичное децентрализованное размещение). В данном случае не существует централизованной биржи. Все операции происходят на децентрализованной бирже, которые не хранят деньги клиентов и не заставляют своих клиентов проходить процедуры идентификации, то есть сделки проводятся анонимно. IDO можно представить как доску объявлений, в которой продавец и покупатель договариваются о цене на какой-либо актив, а затем проводится сделка без участия биржи-посредника.

У всех трёх видов размещения токенов существуют как плюсы, так и минусы в плане информационной безопасности.

В случае ICO, проект полностью берет на себя ответственность за сбор средств, рекламу, а также обработку транзакций.

В случае IEO клиент огражден от откровенно мошеннических схем, поскольку биржи подчиняются законодательству определенных стран, и они отчитываются о своей деятельности государству.

Также биржи осуществляют борьбу с отмыванием денег и финансированием терроризма, но так было не всегда. Многие криптобиржи были замечены в отмывании денег, например, BTC-e, которая была причастна к отмыванию денег, украденных у другой криптобиржи Mt. Gox. При помощи таких инструментов как Chainanalysis и ChiperTrace, возможно отследить и изучить криптовалютные транзакции.

У централизованной схемы есть также и недостатки. В этом случае деньги клиентов хранятся на счетах биржи, то есть биржу можно взломать и украсть денежные средства клиентов. Таких случае было уже много. Самым крупным происшествием является взлом биржи Coincheck, в результате которого было похищено свыше 500 миллионов долларов США. Разработчики признали, что активы клиентов хранились на горячих кошельках, а не на холодных как принято, то есть был доступ к внешнему миру.

Также в Coincheck отсутствовала защита при помощи мультиподписи. Позже биржа опубликовала 11 адресов, по которым нашлись все похищенные деньги. NEM создали инструмент, благодаря которому можно отследить украденные деньги и автоматически отклонять транзакции с такими токенами. Однако, мошенники могут воспользоваться другими сервисами, являющимися анонимными, или обменником.

В случае IDO средства клиентов хранятся не на площадке или бирже, поэтому деньги нельзя похитить путем взлома информационной системы. Каждый участник сделки несет ответственность за сохранность своих средств индивидуально. Однако, из-за анонимности и отсутствия регулирования, допуск к таким сделкам имеют все желающие.

Среди участников таких сделок много мошенников, причем мошенникам могут являться как проекты, которые собирают деньги через IDO, так и клиенты.

Из-за отсутствия регулирования, в частности в области ПОД/ФТ, при помощи IDO мошенники отмывают огромные суммы денег. Никто не интересуется происхождением денег и как они потом будут преобразованы. Таким образом, IDO очень часто является этапом расслоения или интеграции в схемах по отмыванию преступных доходов. На рис. 3 приведено процентное соотношение между данными тремя видами размещения токенов.

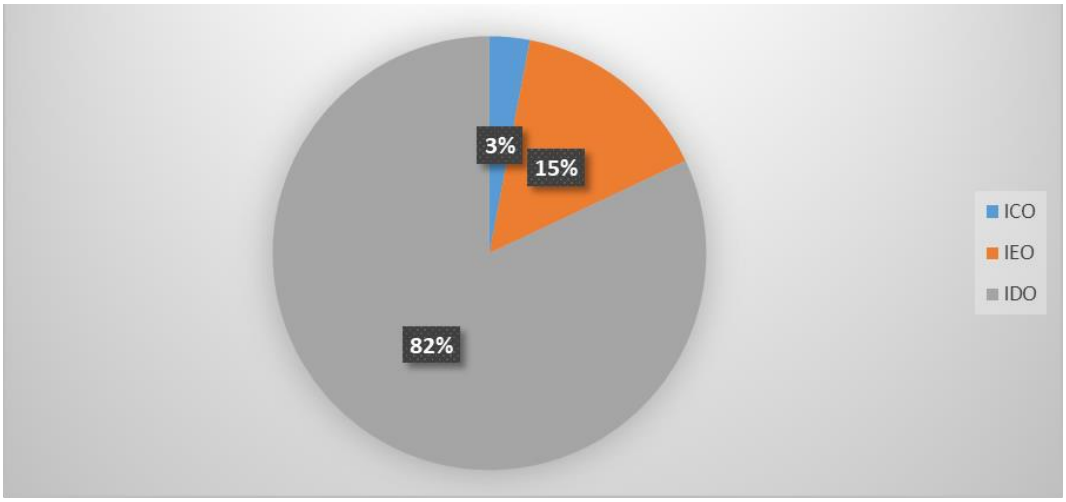

Рис. 3. Распределение долей первичных размещений токенов за 2022-2023 гг. [3

Как можно видеть из графика (рис. 3), 82% процента от всех операций за 2022-2023 гг. по первичному размещению токенов занимает IDO. Это может говорить о том, что данный инструмент обладает высокой привлекательностью из-за отсутствия регулирования, а также анонимности.

Среди наиболее популярных платформ для запуска блокчейн-проектов и сбора инвестиций в формате IDO являются Duckstarter, DSCPad, DAO Maker, Poolz, TrustPad. Среди представленных IDO площадок можно выделить Duckstarter и BSCPad, которые требуют проводить процедуру идентификации клиентов.

В данной статье, из вышеперечисленных способов генерации токенов, нас интересует метод IEO, поскольку согласно статистике, именно данный метод размещения токенов наиболее уязвим угрозам кибератак.

Атаки на криптовалютные биржи

Регулярно приходят новости о том, что произошел очередной взлом криптобиржи. В 2022 году были взломаны криптобиржи Mt. Gox, Upbit, Binance, Bitpoint. В результате данных взломов было похищено более 3,5 млрд. долларов США.

В 2023 году статистика также довольно удручающая. 29 декабря 2023 года вышел отчет Immunefi [4], в котором было сказано, что в 2023 году хакеры и мошенники украли 1,8 млрд. долларов США. На 219 хакерских атак пришлось 1,69 млрд. долларов США потерь, около 103 млн. долларов США было утрачено в результате 100 случаев мошенничества.

Крупнейшими взломами в 2023 году стали атаки на Mixin Network, Euler Finance, Multichain, Poloniex, в которых было похищено 200 млн., 197 млн., 126 млн. долларов США соответственно.

Данная статистика говорит о том, что проблема безопасности цифровых активов стоит очень остро. Рассмотрим данные инциденты более детально.

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) [5].

DDoS-атака имеет свою классификацию по критерию объекта атаки. Данный тип атаки может быть направлен как на саму распределительную систему вычислений, так и на саму платформу вычислений либо на онлайн-площадку, которые и называются криптобиржами.

Атаки на распределенную систему вычислений крайне сложны, поэтому они редко встречаются. Наиболее часто встречаются атаки на онлайн-площадки, в которых защита от кибератак не так совершенна.

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.

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 послетого, 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 [6].

Существует довольно большое количество способов защиты от данного типа угроз. Однако эффективны они только при грамотной эксплуатации, а судя по количеству успешных кибератак, методы защиты от DDoS-атак не всегда эффективны.

Самой распространенной атакой на криптовалютные биржи остается Fishing. Примеров реализации фишинга много, в пример приведем некоторые из них.

Мошенники создают сайты, учетные записи в социальных сетях с названиями известных криптобирж, либо привлекают средства на ICO от имени представителей того или иного проекта [7].

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;

– ссылка на сайт, который полностью имитирует настоящий, но имеет отличие на одну букву в названии, например, Etherium вместо Ethereum

– ссылка на ложный адрес электронного кошелька для перечисления денег.

Как правило, такие сообщения рассылаются в мессенджерах.

Важно отметить, что, как правило, фишеры-санкционеры отправляют средства жертвы в кошелек, отличный от того, на который было получено разрешение, для совершения транзакций от имени жертвы.

Схема работы в цепочке обычно выглядит следующим образом:

– Адрес жертвы подписывает транзакцию, утверждающую второй адрес для расходования средств.

– Второй адрес, который мы будем называть одобренным адресом отправителя, выполняет транзакцию по переводу средств на новый адрес назначения.

Если транзакции разворачиваются таким образом и инициатором сливной транзакции является одобренный адрес отправителя, а не адрес жертвы, как можно было бы ожидать в незлонамеренной транзакции, это, скорее всего, является примером фишинга одобрения. Однако, чтобы узнать наверняка, необходимо дальнейшее расследование.

За 2,5 года убытки от криптовалютного фишинга составили около 1 миллиарда долларов США [8]. При этом на 2023 год пришлось 374 миллиона долларов США потерянных криптоактивов.

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.

Список взломов криптовалютных бирж

Одним из самых крупных происшествий стал взлом криптовалютной биржи Binance в октябре 2022 года. Хакеры украли токены BNB на сумму 570 миллионов долларов. Хакеры атаковали межсетевой мост, связанный с ее цепочкой BNB, что позволило хакерам перемещать токены вне сети.

В августе 2021 года была атакована биржа PolyNetwork. Стоимость потерянных активов составила 610 миллионов долларов. В этот раз хакеры использовали уязвимость протокола кросс-чейн, которая необходима для совместимости различных криптовалют, таких как Bitcoin, Ethereum, Neo. Кросс-чейн реализует функцию переноса активов между различными биткоинами, не конвертируя их при этом через биржи.

По словам программиста Кельвина Фихтера, протокол создает цифровые самоуправляемые сейфы на двух разных блокчейнах. Затем он позволяет пользователю снимать средства из одного ящика только после того, как тот получит подтверждение из другого ящика о том, что соответствующая сумма активов была в него помещена.

Хакеру (или хакерам) удалось найти способ обманом заставить сейфовый ящик высвободить хранящиеся в нем средства без получения законного разрешения от другого блокчейна. Они воспользовались этой уязвимостью 10 августа, чтобы украсть в общей сложности более 610 миллионов долларов.

Взлом криптобиржи KuCoin произошел 25 сентября 2020 года. Потери составили 285 миллионов долларов.

В 2018 году хакеры взломали криптобиржу Coincheck. Было похищено свыше 500 миллионов долларов в криптовалюте NEM. Как именно произошел взлом, неизвестно: сама биржа данные не раскрывает. Известно лишь, что причиной стала проблема в защите, однако это не было инсайдерским преступлением.

Стоит отметить, что ошибки в конфигурировании безопасности этой биржи существовали. Активы клиентов находились на горячих кошельках, а не на холодных, также отсутствовала защита активов при помощи мультиподписи.

В 2014 году крупнейшим взломом криптобиржи стал инцидент с биржей Mt.Gox, о которой уже было упомянуто выше. Украдено было более 460 миллионов долларов. Вскоре выяснилось, что хакеры воровали у компании очень долгое время. После проведенного расследования выяснилось, что закрытый ключ криптобиржи не был зашифрован и был украден еще в 2011 году [9].

Об уязвимости в смарт-контракте омничейн-протоколе Seneca на Ethereum стало известно 29 февраля 2024 года. Уязвимость заключалась в возможности открытого внешнего вызова функции. В том же году, 19 декабря была также обнаружена уязвимость в приложении для iOS криптобиржи OKX. Уязвимость заключалась в возможности удаленного выполнения кода, что могло привести к компрометации конфиденциальных данных и криптоактивов.

Ранее, 14 ноября 2023 года была выявлена уязвимость криптобиржи BitcoinJS. Согласно специалистам, источником уязвимости является функция SecureRandom () из библиотеки javascript JSBN (ее использовали до марта 2014 года), в сочетании со слабостями в основных браузерных реализациях Math.random().

Также стоит упомянуть биржу Bitfinex. Во взломе обвиняют саму Bitfinex, которая владела двумя из трех закрытых ключей на едином устройстве. Также компания не внедрила меры безопасности, предложенные партнером биржи по хранению криптовалют BitGo [10].

Стоит отметить, что найти криптовалютную биржу, которая не взламывалась, почти невозможно. Однако, защита с каждым годом усиливается, становится надежнее. Криптобиржи относятся к кибербезопасности все серьезнее, примером может служить тот факт, что хранение активов на горячих кошельках, связанных с интернетом, стало крайне редким фактом.

Прогноз убытков криптовалютных бирж от кибератак

На основе вышеперечисленных инцидентов можно составить примерный прогноз по нескольким параметрам. Для начала необходимо понять тенденцию по количеству инцидентов от года к году начиная с 2011 года (рис.4).

Как можно видеть из графика на рис. 4, убытки криптобирж с 2011 год по 2022 только росли, и росли очень быстро.

Исключением стал 2023 год, в котором убытки от хакеров снизились на 50%, а также 2020 год. Требования и отношение к информационной безопасности существенно повышаются каждый год, именно с этим связано снижение ущерба от кибератак.

На основе полученных данных проведем прогноз будущих убытков на 2025-2027 годы [11-12] (рис.5).

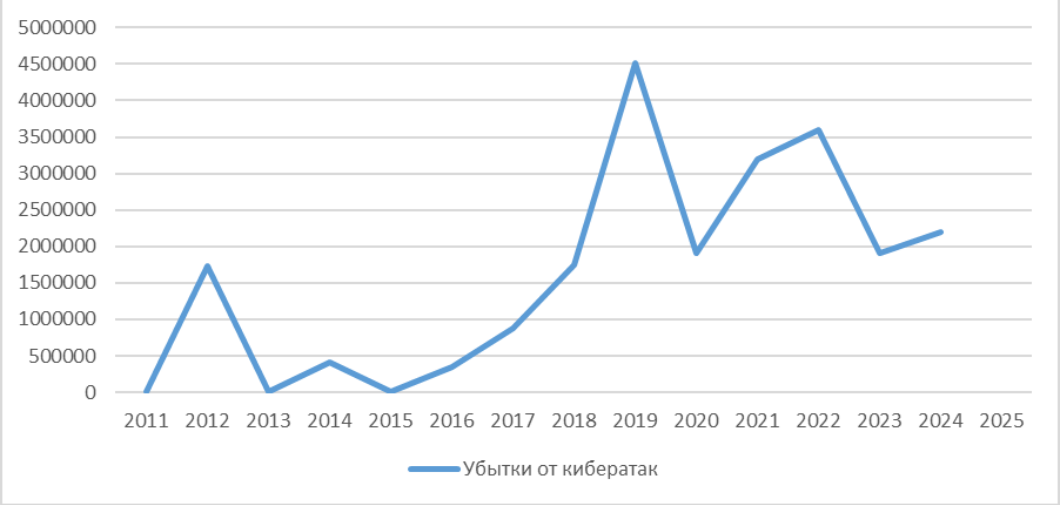

Рис. 4. Убытки криптовалютных биржи от кибератак с 2011 по 2024 год в тыс. долларов США

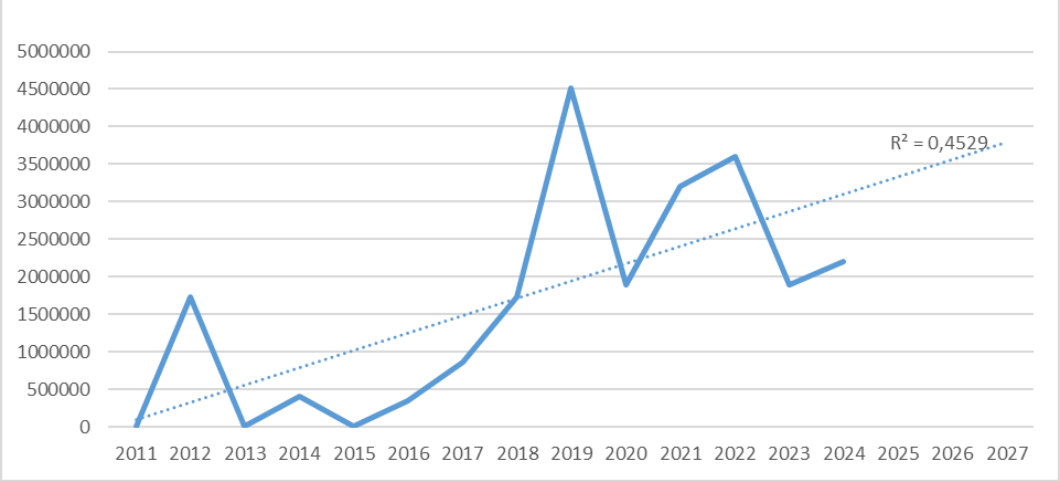

Рис. 5. Убытки криптовалютных биржи от кибератак с 2011 по 2024 год в тыс. долларов США и прогноз при помощи метода линейной аппроксимации

При осуществлении прогнозирования использовался метод линейной аппроксимации с величиной аппроксимации равной R^2=0,4868 (1). Определение получается из равенства теоремы Тейлора (2).

$$f_a^*(x) = f(a) + f'(a)(x-a). \quad (1)$$

$$f(x) = f(a) + f'(a)(x-a) + R_2 \quad (2)$$

Далее приведем прогноз на основе экспотенциального сглаживания с доверительным интервалом. На рис. 6 приведён график прогноза по убыткам криптовалютных бирж от кибератак на 2024-2026 гг.

Прогноз производился при помощи метода экспотенциального сглаживания с доверительным интервалом 95%.

Как на рис. 5, так и на рис. 6 мы видим прогноз на увеличение убытков.

Рис. 6. Убытки криптовалютных биржи от кибератак с 2011 по 2024 год, в тыс. долларов США и прогноз при помощи метода экспотенциального сглаживания

Подгонка модели экспоненциального сглаживания к каждому временному ряду измеряется среднеквадратичной ошибкой прогноза (RMSE), которая равна квадратному корню из среднего квадрата разницы между моделью экспоненциального сглаживания и значениями временного ряда [13].

$$\text{Forecast RMSE} = \sqrt{\frac{\sum_{t=1}^{T}(c_t - r_t)^2}{T}}, \quad (3)$$

где T – количество временных шагов, c_t – подогнанное значение из экспоненциального сглаживания, а r_t – необработанное значение временного ряда во времени t.

Ущерб от кибератак связан не только с кражей средств с кошельков клиентов, после успешной кибератаки, цена того или иного актива может заметно колебаться [14].

Отчасти поэтому ущерб от кибератак нельзя назвать точным за какой-то определенный год. Мы можем определить лишь тренд и динамику этого явления. Тренд, который мы видим из графиков на рис.5 и 6 объясняется ростом популярности и стоимости криптовалют, что явилось огромным соблазном для разного рода группировок, например Lazarus. Также многие криптобиржи пренебрегают элементарными правилами информационной безопасности.

Выводы

Популярность такого финансового инструмента как криптовалюта, стало как плюсом, так и минусом.

К плюсам можно отнести, что число криптовалют с каждым днем становится все больше, у инвесторов появляется больше возможностей для инвестиций.

К минусам отнесем тот факт, что криптоиндустрия привлекла к себе большое число мошенников, хакеров. Они наносят огромный ущерб отрасли, криптобиржи теряют свои деньги, также как и их клиенты. К наиболее распространенным атакам отнесем DDoS, фишинг, атаки через различные бреши в защите, в том числе и криптографических протоколов.

В данной статье приведены статистические данные о совокупном ущербе от кибератак на криптобиржи с 2011-2024 годы, а также сделан прогноз на 2025-2027 гг. Методы математической статистики указали возрастающий тренд, однако стоит учитывать другие факторы. Уровень защиты криптобирж растет, также как и требования к ней.

В 2023 году ущерб существенно снизился, однако показатель одного года еще не говорит о развороте тренда на снижение, что подтверждают данные 2024 года.

В работе были использованы данные из отчетов различных компаний, таких как Group-ib, Ciphertrace, Positive Technologies, Лаборатория Касперского.

Список литературы

1. Arun Kumar Singh Sandeep Saxena Varun Shukla, Analysis of Futuristic Currency: Facebook's Libra: Cryptology and Network Security with Machine Learning (april 2024). - DOI: 10.1007/978-981-97-0641-9_36
2. Криптовалюты: тренды, риски, меры. Москва, 2022 год [Электронный ресурс] https://www.cbr.ru/Content/Document/File/132241/Consultation_Paper_20012022.pdf (дата обращения 25.04.2025 г.)
3. Cryptocurrency Crime and Anti-Money Laundering Report CipherTrace Cryptocurrency Intelligence February 2021 [Electronic resource] URL: https://ciphertrace.com/2020-year-end-cryptocurrency-crime-and-anti-money-laundering-report (дата обращения 25.04.2025)
4. Report on cyberattacks on crypto exchanges Immunefih [Электронный ресурс]. URL: https://assets.ctfassets.net/t3wqy70tc3bv/4hZTbqxDJqaWGlOtwVVUkb/0d7b472c0bd15e2338968c3b0dc869d0/Immunefi_Crypto_Losses_January_2024.pdf (дата обращения 20.04.2025)
5. Matt Levine. Blockchain for banks probably cannot hurt // Bloomberg View. [Электронный ресурс]. URL: http://www.bloomberg view.com/articles/2015−09−01/ blockchain-for-banks-probablycan-t-hurt
6. Coindesk, July 2015. "Details of $5 Million Bitstamp Hack Revealed". [Электронный ресурс]. URL: https:// www.coindesk.com/unconfirmed-report-5-million-bitstamp-bitcoin-exchange (дата обращения 25.04.2025.).
7. Глотов В., Михайлов Д. Проблемы безопасности криптовалютных сервисов // Федерализм. 2018. № 1. С. 134-143.
8. Ahmed H. Elsayed & Ricardo M. Sousa (2022): International monetary policyand cryptocurrency markets: dynamic and spillover effects, The European Journal of Finance (PDF) International monetary policy and cryptocurrency markets: dynamic and spillover effects. [Электронный ресурс]. URL: https://www.researchgate.net/publication/360629498_International_monetary_policy_and_cryptocurrency_markets_dynamic_and_spillover_effects (дата обращения 30.04.2025)
9. CoinTelegraph, Feb. 2015. "3-Way Bitcoin Exchange Hack Dwarfed by 15-month $300 million Bank Heist" [Электронный ресурс]. URL: https://cointelegraph.com/news/3-way-bitcoin-exchange-hackdwarfed-by-15-month-us300-million-bank-heist (дата обращения 25.04.2025).
10. Coindesk, Mar. 2014. "Poloniex Loses 12.3% of its Bitcoins in Latest Bitcoin Exchange Hack". [Электронный ресурс] URL: https://www.coindesk.com/poloniexloses-12-3-bitcoins-latest-bitcoin-exchangehack/ (дата обращения 25.04.2025).
11. Отчет ЦБ РФ за 2023 г. «Обзор операций, совершенных без согласия клиентов финансовых организаций» [Электронный ресурс] URL: https://cbr.ru/analytics/ib/operations_survey/2023/(дата обращения 25.12.2024).
12. Отчет ЦБ РФ за 2021 г. «Обзор операций, совершенных без согласия клиентов финансовых организаций» [Электронный ресурс]. URL: https://cbr.ru/analytics/ib/operations_survey/2021/ (дата обращения 25.12.2024).
13. Щукина И. Методика оценки эффективности закупочной деятельности заказчиков в Севастополе // Федерализм. 2018. № 1. С. 231-239
14. Non-linearities, cyber attacks and cryptocurrencies - Guglielmo Maria Caporale, Woo-Young Kanga, Fabio Spagnoloa, Nicola Spagnolo Finance Research Letters, DOI: 10.1016/j.frl.2019.09.012.

References

1. Arun Kumar Singh Sandeep Saxena Varun Shukla, Analysis of Futuristic Currency: Facebook's Libra: Cryptology and Network Security with Machine Learning (april 2024). DOI: 10.1007/978-981-97-0641-9_36

2. Kriptovalyuty: trendy, riski, mery. Moskva, 2022. URL: https://www.cbr.ru/Content/Document/File/132241/Consultation_Paper_20012022.pdf (Access date: 25.04.2025).

3. Cryptocurrency Crime and Anti-Money Laundering Report CipherTrace Cryptocurrency Intelligence February 2021. URL: https://ciphertrace.com/2020-year-end-cryptocurrency-crime-and-anti-money-laundering-report (Access date: 25.04.2025).

4. Report on cyberattacks on crypto exchanges Immunefih URL: https://assets.ctfassets.net/t3wqy70tc3bv/4hZTbqxDJqaWGlOtwVVUkb/0d7b472c0bd15e2338968c3b0dc869d0/Immunefi_Crypto_Losses_January_2024.pdf (Access date: 20.04.2025)

5. Matt Levine. Blockchain for banks probably cannot hurt // Bloomberg View. URL: http://www.bloomberg view.com/articles/2015−09−01/ blockchain-for-banks-probablycan-t-hurt

6. Coindesk, July 2015. "Details of $5 Million Bitstamp Hack Revealed". URL: https:// www.coindesk.com/unconfirmed-report-5-million-bitstamp-bitcoin-exchange (Access date: 25.04.2025).

7. Glotov V., Mihajlov D. Problemy bezopasnosti kriptovalyutnyh servisov [Security issues with cryptocurrency services], Federalizm. 2018. N 1. pp. 134-143.

8. Ahmed H. Elsayed & Ricardo M. Sousa (2022): International monetary policyand cryptocurrency markets: dynamic and spillover effects, The European Journal of Finance (PDF) International monetary policy and cryptocurrency markets: dynamic and spillover effects. URL: https://www.researchgate.net/publication/360629498_International_monetary_policy_and_cryptocurrency_markets_dynamic_and_spillover_effects (Access date: 30.04.2025).

9. CoinTelegraph, Feb. 2015. "3-Way Bitcoin Exchange Hack Dwarfed by 15-month $300 million Bank Heist". URL: https://cointelegraph.com/news/3-way-bitcoin-exchange-hackdwarfed-by-15-month-us300-million-bank-heist (Access date: 25.04.2025).

10. Coindesk, Mar. 2014. "Poloniex Loses 12.3% of its Bitcoins in Latest Bitcoin Exchange Hack". URL: https://www.coindesk.com/poloniexloses-12-3-bitcoins-latest-bitcoin-exchangehack (Access date: 25.04.2025).

11. Otchet CB RF za 2023 g. «Obzor operacij, sovershennyh bez soglasiya klientov finansovyh organizacij» [Report of the Central Bank of the Russian Federation for 2023 "Review of transactions carried out without the consent of clients of financial institutions"] URL: https://cbr.ru/analytics/ib/operations_survey/2023/(Access date: 25.12.2024).

12. Otchet CB RF za 2021 g. «Obzor operacij, sovershennyh bez soglasiya klientov finansovyh organizacij» [Report of the Central Bank of the Russian Federation for 2021 "Review of transactions carried out without the consent of clients of financial institutions"] URL: https://cbr.ru/analytics/ib/operations_survey/2021/ (Access date: 25.12.2024).

13. Shchukina I. Metodika ocenki effektivnosti zakupochnoj deyatel'nosti zakazchikov v Sevastopole [Methodology for assessing the effectiveness of procurement activities of customers in Sevastopol] Federalizm, 2018, N 1. pp. 231-239.

14. Non-linearities, cyber attacks and cryptocurrencies - Guglielmo Maria Caporale, Woo-Young Kanga, Fabio Spagnoloa, Nicola Spagnolo Finance Research Letters, DOI: 10.1016/j.frl.2019.09.012.

СВЕДЕНИЯ ОБ АВТОРЕ/ ABOUT THE AUTHOR

Иван Андреевич Петров, аспирант, старший преподаватель кафедры информационной безопасности Факультета информационных технологий и анализа больших данных, Финансовый университет при Правительстве РФ, 125167, Москва, проспект Ленинградский, д. 49/2, iapetrov@fa.ru

Ivan Andreevich Petrov, Postgraduate, Senior Lecturer, Department of Information Security, Faculty of Information Technology and Big Data Analysis, Financial University under The Government of Russian Federation, 49/2 Leningradsky Ave., Moscow, Russia, 125167

ORCID: 0009-0008-9475-8870