УДК 004.052

СТАТИСТИЧЕСКИЕ УЯЗВИМОСТИ В СМАРТ КОНТРАКТАХ

© 2023 П. Н. Анохин[1] (Орёл, Россия)

Существующие исследования уязвимостей смарт контрактов рассматривают, в основном, технические уязвимости в коде смарт контрактов, обходя вниманием статистические уязвимости, которые могут присутствовать в приложениях даже при идеальной технической реализации. В статье раскрыта суть статистических уязвимостей, на основе анализа реальных обнаруженных уязвимостей в работающих смарт контрактах показан реальный ущерб, дана оценка потенциального ущерба для различных категорий приложений, разработаны рекомендации по методам поиска и вариантам устранения статистических уязвимостей. Материалы статьи представляют практическую ценность для разработчиков и экспертов по безопасности смарт контрактов, позволяя им использовать полученные сведения для поиска и устранения нового типа уязвимостей, делая финансовые приложения на блокчейн технологии более защищенными и безопасными для пользователей.

Ключевые слова: смарт контракт, информационная безопасность, статистическая уязвимость, блокчейн, децентрализованные финансы, статистическое моделирование.

Введение

Разработчики смарт контрактов уделяют большое внимание безопасности своих децентрализованных приложений: смарт контракты часто управляют активами на миллионы и миллиарды долларов, а одна единственная ошибка в приложении может привести к безвозвратным потерям всех или большей части средств.

В то же время, большинство разработчиков и экспертов по безопасности смарт контрактов сосредотачиваются в основном на технических ошибках [1, 2], позволяющих мгновенно или очень быстро похитить или заблокировать активы, уделяя мало внимания и недооценивая статистические ошибки, приводящие к постепенной и медленной потере активов. Различные исследования, посвященные классификации ошибок смарт контрактов [3-9], предлагают различные категории и классы ошибок, однако все предложенные категории, виды и классы ошибок относятся только к техническим ошибкам в исходном коде смарт контрактов. Практикующие специалисты по безопасности также предлагают свои варианты классификации на основе найденных ими ошибок, например в статьях [10, 11], при этом все ошибки в классификациях также носят характер технических ошибок в коде.

В работах [12, 13] впервые упоминаются проблемы смарт контрактов, связанные со статистическими уязвимостями, но только в контексте возможности извлечения прибыли майнером при выборе порядка транзакций (фронт-раннинг и сендвич-атаки). Класс же статистических уязвимостей значительно шире, и аналогичные по ущербу атаки могут осуществляться множеством другим способов, не только майнерами, но и любыми пользователями.

Такие ошибки не позволяют быстро похитить или заблокировать значительные средства, однако они могут приводить к постоянным небольшим потерям: например, 5% активов под управлением в месяц. Но игнорирование таких ошибок чревато долгосрочными негативными последствиями для работы приложения: т. к. потеря средств сказывается на вложениях клиентов таких приложений, то клиенты перестают пользоваться приложением и выводят свои средства, чтобы избежать дальнейших потерь.

[1] Анохин Павел Николаевич – Индивидуальный предприниматель (Орёл, Россия), к. т. н., e-mail: pavel@anokhin.name, тел.: +7 (920) 283-92-14

Цель данного исследования: привлечь внимание других исследователей, разработчиков и экспертов по безопасности смарт контрактов к проблеме статистических уязвимостей смарт контрактов, оценить ущерб от данного типа уязвимостей на конкретных примерах блокчейн приложений, а также разработать рекомендации по методам поиска данного вида уязвимостей и возможные варианты их устранения.

Определение статистической уязвимости

Статистические уязвимости – это уязвимости, связанные с математическим ожиданием долгосрочной прибыли хакера от повторяемых действий, при этом прибыль хакера формируется за счет убытка остальных пользователей. Каждое действие хакера может быть как прибыльным, так и убыточным для него, однако важно то, что из-за статистической уязвимости хакер может быть уверен в долгосрочной прибыли, а пользователи проекта (или определенная группа пользователей: инвесторы, провайдеры ликвидности и т. п.) долгосрочно будут стабильно терять вложенные средства.

Простой пример наличия статистической уязвимости: случайный бросок монеты, при котором ведущий (смарт контракт) принимает ставки в $1 от пользователей на результат броска монеты, выплачивая за правильно угаданный результат броска: $2.02 за выпавший орёл и $1.96 за выпавшую решку.

Если количество пользователей, поставивших на орёл и на решку примерно одинаково, то ведущий получит прибыль. Например, приняв 99 ставок на орел и 101 ставку на решку ($200 всего), ведущий выплатит $199.98 если выпадет орёл или $197.96 если выпадет решка, в обоих случаях ведущий получит прибыль.

Однако, если умный игрок А, заметив высокую выплату за выпавший орёл, будет ставить только на орёл, то математическое ожидание прибыли игрока А за 1 ставку, которое можно посчитать по формуле (1), составит $0.01.

$$M(P_A) = 0.5 \times \$2.02 - \$1 = \$0.01 \quad (1)$$

Если игрок А начнёт игру с балансом $100, то после 10000 бросков математическое ожидание его прибыли будет $100, а конечного баланса – $200, однако реальный разброс из-за случайности бросков может быть большим. Пример изменения баланса игрока А за 10000 бросков приведен на рисунке 1.

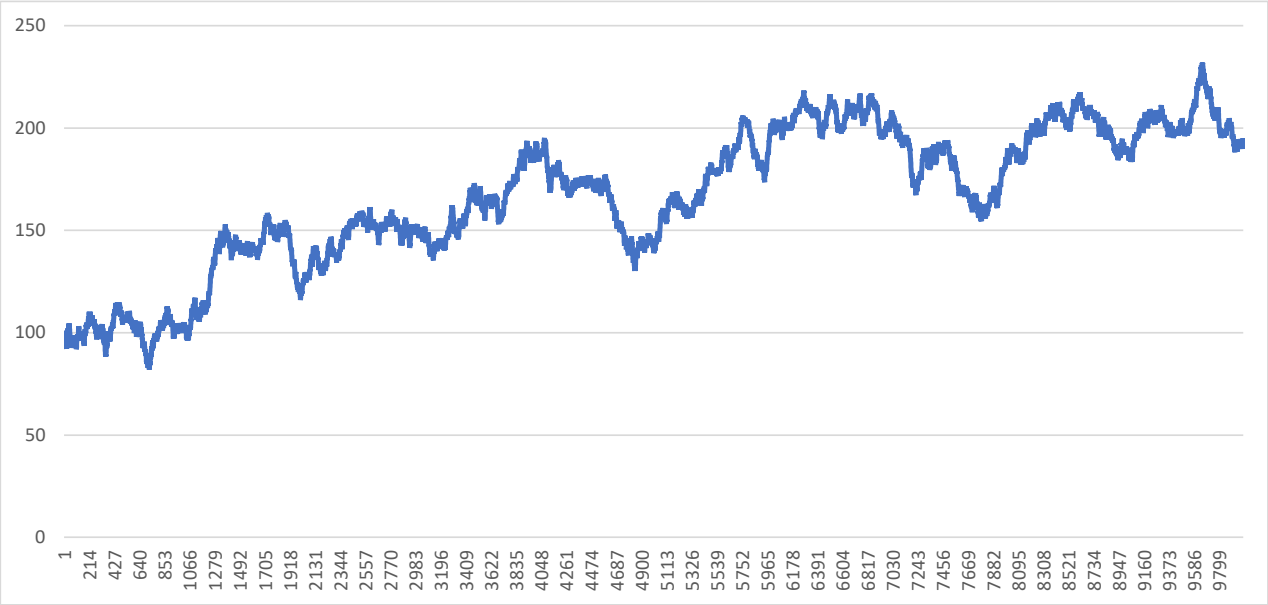

Рисунок 1. Изменение баланса игрока А за 10000 случайных бросков монеты

Как видно из рисунка 1, баланс игрока А то растёт, то падает, однако долгосрочно игрок А имеет прибыль $100 или 100% вложенных средств. Если ставки происходят со скоростью 1 ставка в минуту, то это 100% прибыли за 1 неделю (без реинвестирования). Используя множество аккаунтов, игрок А может таким образом достаточно быстро украсть все средства ведущего (средства, вложенные пользователями или инвесторами смарт контракта).

В данном примере смарт контракт может быть технически совершенным и не иметь ни одной уязвимости в своем коде, однако из-за неправильных параметров выплат будет иметь критическую статистическую уязвимость.

Примеры найденных статистических уязвимостей в реальных смарт контрактах

Статистические уязвимости достаточно часто встречаются в реальных работающих смарт контрактах с миллионами вложенных средств пользователей. При этом команды разработчиков этих приложений, а также аудиторы, проверяющие приложения на отсутствие уязвимостей, зачастую не находят этих уязвимостей, т. к. сосредоточены на поиске технических уязвимостей в коде, игнорируя или не уделяя должного внимания математическому ожиданию прибыли пользователей проекта. Далее приведены некоторые статистические уязвимости из реальных смарт контрактов, которые нашел автор данного исследования и уведомил команды разработчиков о найденных ошибках в рамках программ поиска ошибок Bugs Bounty.

Пример 1. Gains Trade. Арбитраж ставки финансирования

Gains Trade – это децентрализованная биржа, позволяющая торговать (покупать и продавать) бессрочные фьючерсы на блокчейне Полигон [14]. Торги осуществляются по ценам оракула (усредненной цены нескольких крупных бирж) без проскальзывания. Отличительная особенность Gains Trade по сравнению с другими биржами бессрочных фьючерсов (на момент присутствия уязвимости) – отсутствие ставки финансирования.

В традиционных бессрочных фьючерсах ставка финансирования (впервые введенная биржей Bitmex) – это регулярный платеж между держателями длинных и коротких позиций с целью удержания цены бессрочного фьючерса близко к индексу, который фьючерс должен отслеживать. Когда цена фьючерса выше цены индекса, то держатели длинных позиций платят держателям коротких позиций определенный процент от номинала своих позиций (таким образом поощряя закрывать длинные или открывать короткие позиции, сдвигая цену ниже, ближе к индексу). Аналогично, когда цена фьючерса ниже цены индекса, то держатели коротких позиций платят держателям длинных позиций.

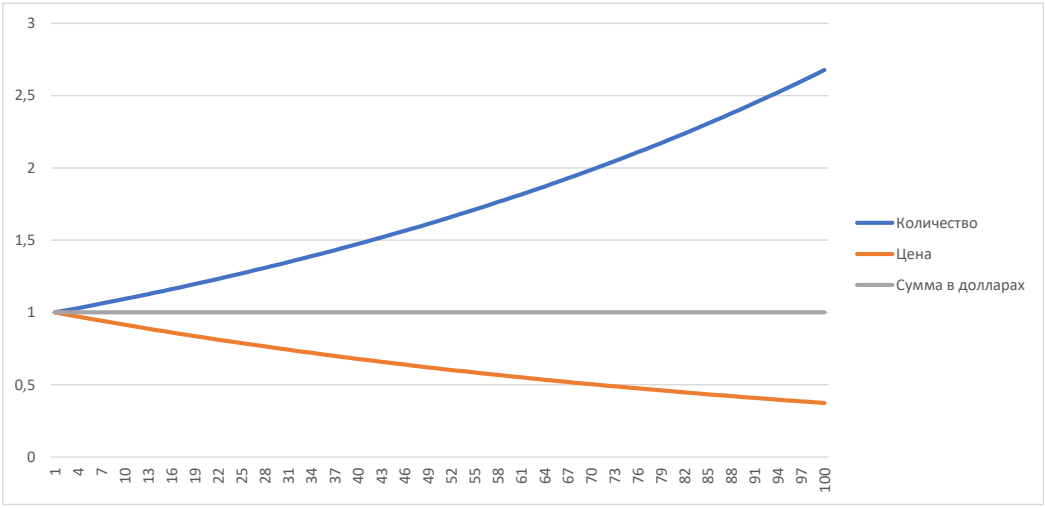

Рисунок 2. Математическое ожидание цены инфляционного токена

Может показаться, что, при торгах по цене оракула, ставка финансирования не нужна, т. к. нет необходимости держать цену фьючерса близко к индексу – торги и так проходят ровно по цене индекса (оракула). Однако это неверно. Ставка финансирования – это также и механизм, нейтрализующий возможности арбитража. Если математическое ожидание изменения цены токена значительно отличается от нуля, то ставка финансирования должна отражать это ожидание. В области криптовалют это чаще всего относится к инфляционным токенам, которые для выплаты определенных наград пользователям проекта выпускают большое количество своих токенов, что приводит к ожидаемому падению их цены. Это происходит, т. к. при постоянной оценке стоимости всех токенов, если количество токенов увеличивается, то цена каждого токена автоматически уменьшается: математическое ожидание вложений в токен (произведения количества токенов на их цену) равно константе (рис. 2).

Без ставки финансирования пользователь может просто открыть короткую позицию по такому токену (продать токен не имея его), получая прибыль от ожидаемого падения цены инфляционного токена. В традиционных биржах ставка финансирования по таким токенам будет сильно смещена в пользу выплаты держателей коротких позиций – держателям длинных позиций, компенсируя выплатами по ставке финансирования ожидаемое падение цены. На рисунке 3 показаны графики прибыли держателя короткой позиции инфляционного токена в классической бирже: прибыль от ожидаемого изменения цены компенсируется точно таким же убытком от выплат по ставке финансирования, таким образом математическое ожидание общей прибыли держателя короткой позиции инфляционного токена равно нулю. В случае же, если ставка финансирования отсутствует, пользователь получает только ожидаемую прибыль от изменения (падения) цены токена, что является статистической уязвимостью.

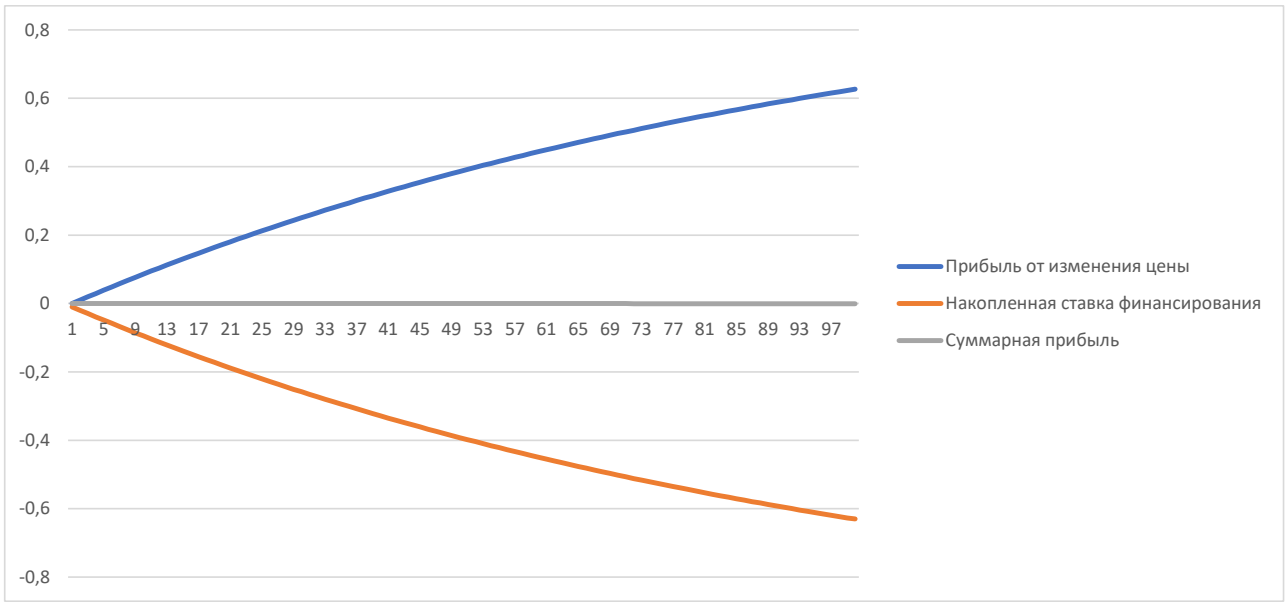

Рисунок 3. Математическое ожидание прибыли держателя короткой позиции инфляционного токена

На момент уязвимости в Gains Trade были доступны торги бессрочными фьючерсами токена AXS (Axie Infinity). При этом в самом проекте Axie Infinity можно было вложить (стейкинг) токен AXS, получая 70-90% годовых прибыль за счет инфляции токена AXS. Таким образом был возможен арбитраж ставки финансирования между проектом Axie Infinity и Gains Trade. Купив AXS и вложив в стейкинг, одновременно захеджировав его цену, открыв короткую позицию в Gains Trade на токен AXS в том же количестве, можно было получить практически безрисковых 70-90% годовых. Эта прибыль образовывалась за счёт отсутствия ставки финансирования в Gains Trade при математическом ожидании падении цены токена

AXS из-за его высокой инфляции. Противоположной стороной в сделке Gains Trade выступает пул провайдеров ликвидности проекта, которые из-за статистической уязвимости имеют математическое ожидание убытка.

Несмотря на то, что команда разработчиков Gains Trade была уведомлена о найденной статистической уязвимости, ею было принято решение, что это не является уязвимостью и никаких мер по исправлению уязвимости предпринято не было. В результате этого, из-за существенного дисбаланса открытых коротких позиций и последующего сильного падения цены токена AXS, провайдеры ликвидности Gains Trade потеряли большее 1 миллиона долларов, после чего разработчики Gains Trade убрали токен AXS из доступных для торговли и ввели ставку финансирования для компенсации этой статистической уязвимости.

Пример 2. Integral FIVE и SIZE. Возможность отмены убыточных операций

Integral FIVE и Integral SIZE – это децентрализованные биржи обмена токенов по средней цене оракула за 5 минут (Integral FIVE) или за 30 минут (Integral SIZE) [15]. Средства для обмена предоставляют пользователи – провайдеры ликвидности, получая за это небольшую комиссию от каждого обмена, но неся риски изменения цены токенов.

Процесс обмена для пользователя состоит в следующем:

1. Пользователь вносит средства для обмена в токене A.

2. Средства блокируются в смарт контракте на 5 (30) минут. Никто не имеет к ним доступа в этот период времени.

3. Через 5 (30) минут пользователь может получить из смарт контракта сумму в токене B, равную средней цене токена B по отношению к токену A за прошедший период в 5 (30) минут.

Принципиальным моментом с точки зрения потенциальной статистической уязвимости является безусловный процесс обмена: после внесения средств, пользователь не может отказаться от обмена, в противном случае он мог бы выборочно отменять невыгодные для себя операции обмена, если средняя цена за период хуже текущей рыночной цены.

Однако, смарт контракты Integral FIVE и SIZE имели особенность в обработке обменов: если в смарт контракте не хватало суммы токена B для завершения обмена, то обмен пользователя полностью отменялся (пользователю возвращалась вся сумма токена A). Эту особенность можно было использовать для выборочной отмены заявок обмена непосредственно перед их завершением, когда пользователь уже знает среднюю цену за период, по которой будет осуществляться обмен. Для этого изначально заявка создается на сумму токена B чуть большую, чем есть в смарт контракте, таким образом по истечении 5 (30) минут суммы на обмен не хватит и обмен отменяется. Если же средняя цена за период является выгодной для пользователя (лучше текущей цены обмена), то он может послать минимальное количество токена B непосредственно смарт контракту так, чтобы средств для обмена хватило, таким образом успешно завершая обмен по выгодной для пользователя цене.

Данная статистическая уязвимость позволяла пользователям исполнять только выгодные обмены, тем самым создавая положительное математическое ожидание прибыли пользователя за счет убытка провайдеров ликвидности проекта. Для оценки серьезности данной статистической уязвимости и определения размера потенциальных потерь, было проведено моделирование использования уязвимости на реальных данных из блокчейна, для этого:

1. Из блокчейна были собраны данные оракула, который используется смарт контрактами Integral FIVE и SIZE (Uniswap v2 рынок ETH-USDC в сети Ethereum) (за июнь и июль 2022)

2. С веб-сайта компании Binance были скачаны исторические данные торгов ETH-USDT (за июнь и июль 2022)

3. Была написана программа моделирования исполнения обменов на максимально возможные суммы с применением описанной выше статистической уязвимости.

4. Моделирование проводилось по 3-дневным интервалам. В начале каждого 3-дневного интервала начальные балансы пользователя и смарт контракта устанавливались в 1 USDC. В конце каждого 3-дневного интервала выводились результаты моделирования.

5. Моделирование внутри 3-дневного интервала разбивалось на отрезки по 5 (30) минут.

6. Моделировалась последовательная покупка ETH за USDC (на всю сумму, доступную в смарт контракте), потом продажа ETH за USDC (опять на всю сумму), покупка, продажа и т. д.

7. На последней минуте каждого отрезка, цена биржи Binance сравнивалась с средней ценой оракула первых 4 (29) минут отрезка, и если цена Binance выше (для покупки) или ниже (для продажи) на заранее определенное значение, то осуществлялся обмен по средней цене оракула за 5 (30) минут отрезка.

Результаты моделирования 19 3-дневных интервалов с 1 июня 2022 года по 29 июля 2022 года для проекта Integral FIVE приведены в таблице 1 и на рисунке 4.

Таблица 1

Результаты моделирования убытка от применения статистической уязвимости Integral FIVE

№ интервала	**Количество транзакций**	**Убыток смарт контракта (%)**
1	235	-27
2	151	-13
3	205	-29
4	254	-39
5	369	-71
6	315	-59
7	325	-48
8	264	-33
9	221	-26
10	253	-37
11	207	-28
12	238	-29
13	226	-24
14	184	-25
15	266	-27
16	297	-35
17	336	-48
18	286	-33
19	286	-33
Минимум (по модулю)	151	-13
Максимум (по модулю)	369	-71
Среднее	259	-35
Медианное	254	-33

Как видно из результатов моделирования, смарт контракт Integral FIVE получает существенный убыток от применения статистической уязвимости за любой 3-дневный интервал, в среднем теряя около трети вложенных средств за 3 дня. Суммарно, потенциальные потери смарт контрактов Integral FIVE и Integral SIZE на момент обнаружения уязвимости составляли $1.56 миллионов.

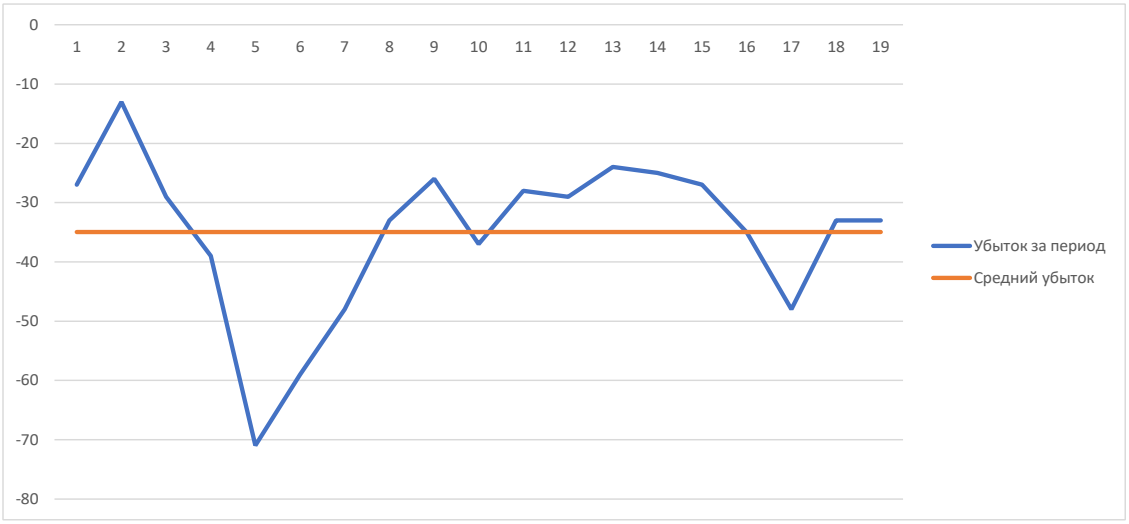

Рисунок 4. Убыток смарт контракта Integral FIVE от использования статистической уязвимости

Разработчики проектов Integral подтвердили наличие статистической уязвимости, впоследствии исправив ее и описав уязвимость и действия по ее исправлению в своем блоге [16].

Оценка потенциального ущерба от статистических уязвимостей

Статистические уязвимости возможны далеко не в любом смарт контракте. Как правило, их можно обнаружить в тех проектах, которые используют цены внешних оракулов для каких-либо операций, и полагаются на математическое ожидание долгосрочной прибыли своих инвесторов или провайдеров ликвидности исходя из предположения того, что цена внешнего оракула является близкой к справедливой цене. В последнее время количество и популярность таких проектов достаточно быстро увеличивается, что обуславливает актуальность проблемы определения, мониторинга и устранения такого типа уязвимостей. На рисунке 5 приведены оценочные вероятности существования статистических уязвимостей в различных категориях приложений. Оценочные вероятности основаны на проценте приложений из общего количества приложений в данной категории, части которых основаны на долгосрочном математическом ожидании прибыли определенной группы пользователей.

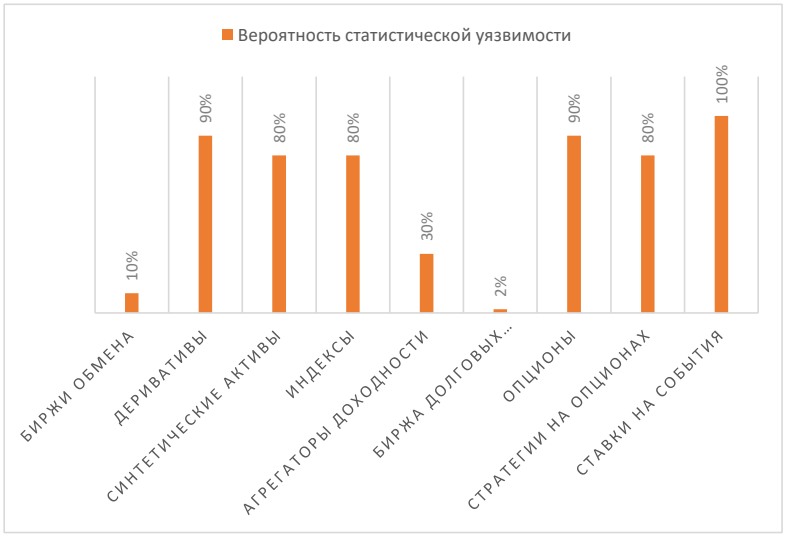

Рисунок 5. Вероятность статистических уязвимостей в различных категориях приложений

В первую очередь статистическим уязвимостям подвержены проекты, связанные с вероятностными событиями (ставки на события), производными финансовых инструментов (деривативы): фьючерсы, опционы, индексы, синтетические активы, а также любые другие проекты, которые их используют (например, агрегаторы доходности, или в меньшей степени – биржи долговых обязательств). Также им подвержены некоторые децентрализованные биржи обмена в случае, если они используют какие-либо статистические методы для определения цены обмена. Биржи, позволяющие вкладывать средства и брать в долг, также могут быть подвержены статистическим уязвимостям, особенно при использовании инфляционных токенов или при ошибках в алгоритмах расчета долгового обеспечения, при этом некоторые технические ошибки реализации, не имеющие прямого применения для потери средств, могут приводить к статистическим уязвимостям и медленному накоплению убытка за продолжительный период времени.

В таблице 2 и на рисунке 6 приведена оценка риска от статистических уязвимостей в различных категориях смарт контрактов (потенциальные средства, которые могут быть под угрозой потери из-за статистических уязвимостей). Данные о вложенных средствах по каждой категории взяты из открытых источников по данным defillama [17]. Общая сумма потенциального риска составляет 4,582 миллиарда долларов.

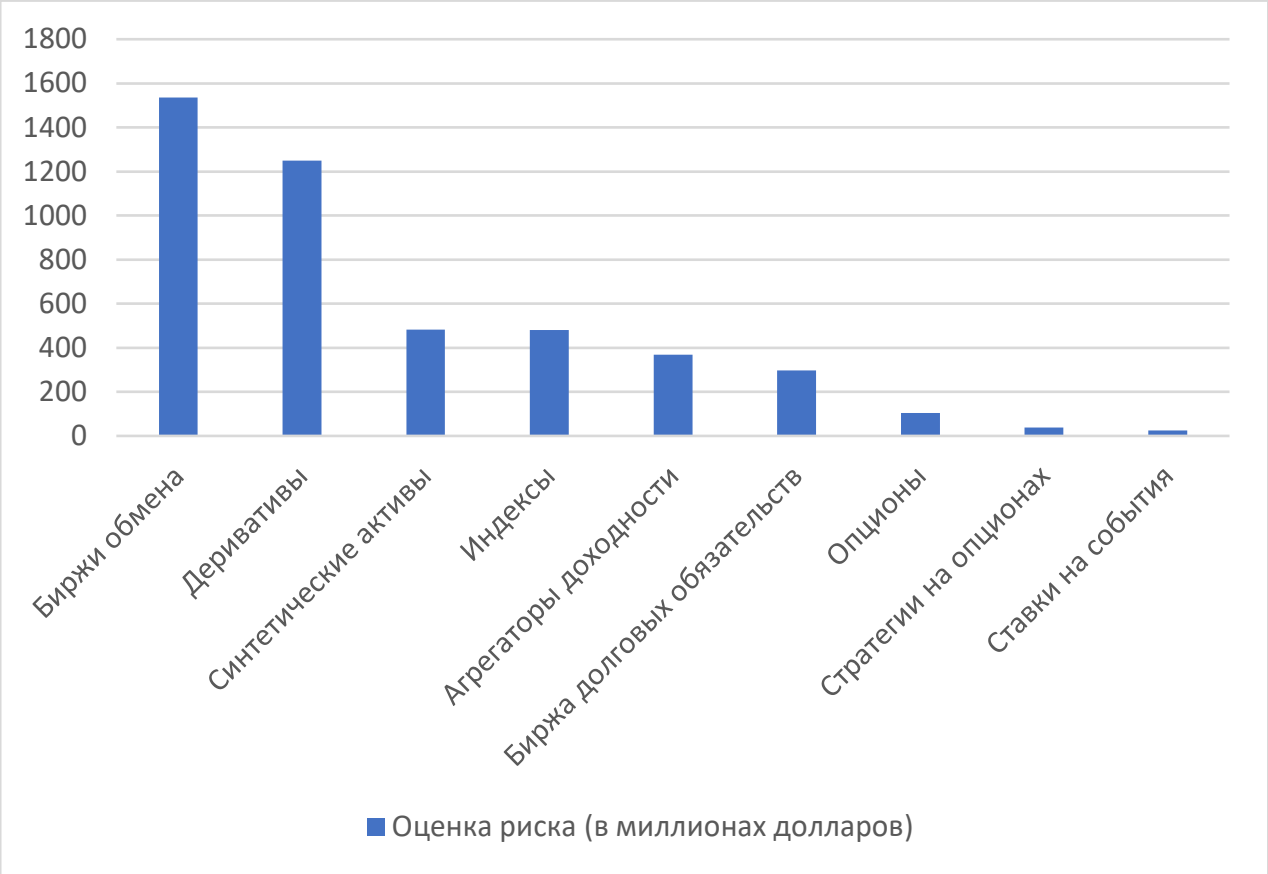

Рисунок 6. Оценка риска от статистических уязвимостей в различных категориях приложений (в миллионах долларов)

Разработчикам и аудиторам, которые работают со смарт контрактами из указанных в таблице 2 категорий, рекомендуется уделять особое внимание возможным статистическим уязвимостям и проводить моделирования различных ситуаций, оценивая влияние различных действий пользователей на долгосрочное математическое ожидание прибыли клиентов.

Таблица 2

Оценка риска статистических уязвимостей в различных категориях смарт контрактов

Категория	**Вложенные средства (в миллионах долларов)**	**Вероятность подверженности статистическим уязвимостям**	**Оценка риска (в миллионах долларов)**
Биржи обмена	15 364	10%	1 536
Деривативы	1 389	90%	1 250
Синтетические активы	604	80%	483
Индексы	601	80%	481
Агрегаторы доходности	1 229	30%	369
Биржа долговых обязательств	14 865	2%	297
Опционы	116	90%	104
Стратегии на опционах	47	80%	38
Ставки на события	24	100%	24
ВСЕГО	**34 239**		**4 582**

Особенности поиска и устранения статистических уязвимостей

В существующих исследованиях по классификации уязвимостей смарт контрактов и методам их предотвращения, поиска и устранения, отсутствует категория статистических уязвимостей. В связи с этим, и на основе опыта анализа статистических уязвимостей множества реальных смарт контрактов, автором разработаны следующие рекомендации по поиску и устранению данной категории уязвимостей в смарт контрактах:

1. На всех этапах разработки приложения основными методами исследования потенциальных статистических уязвимостей должны выступать статистический анализ данных и имитационное моделирование, включающее симуляцию различных сценариев поведения пользователей на основе реальных исторических данных.

2. На этапе проектирования приложения, необходимо оценить математическое ожидание прибыли всех пользователей в различных ситуациях как на основе математической модели предполагаемого функционирования приложения, так и на основе имитационного моделирования и симуляции на реальных исторических данных. Важно не ограничиваться только математической моделью, т. к. реальные данные зачастую отличаются (возможно, незначительно) от общепринятых моделей и имеют различные смещения, что в ряде случаев может привести к возникновению статистических уязвимостей. Использование реальных данных позволяет учесть эти смещения и определить недопустимые подходы или потенциальные уязвимости. Устранение статистических уязвимостей на этом этапе заключается в изменении логики работы приложения или выборе других подходов к решению поставленных проблем так, чтобы математическое ожидание прибыли всех пользователей соответствовало целям создания приложения.

3. На этапе реализации, необходимо создавать наборы тестов на основе данных, полученных из математического и имитационного моделирования и симуляции в различных ситуациях, чтобы постоянно контролировать соответствие ожидаемой логики работы и реализации приложения. При необходимости необходимо обновлять математические и имитационные модели, если реализация отличается от начальных предположений. Устранение статистических уязвимостей на этом этапе заключается в контроле соответствия ожидаемой и реализованной логики работы приложения: отклонения могут указывать на появление статисти-

ческих уязвимостей, которые устраняются либо исправлением реализации, либо изменением логики работы приложения (в случае, если реализация приложения выявила новые сценарии, приводящие к статистическим уязвимостям).

4. На этапе тестирования и аудита безопасности, необходимо определить все потенциальные векторы атаки в отношении статистических уязвимостей – это все возможные сценарии, которые могут повлиять на математическое ожидание прибыли любой группы пользователей приложения. Такие сценарии могут включать, например, использование любой функциональности приложения, позволяющей влиять на цену исполнения заявок пользователей, на возможность отмены нежелательных пользователю операций, возможность действий/торгов с использованием устаревших цен и т. п. По каждому такому сценарию необходимо составлять тесты и добавлять их в общий набор тестов приложения. Устранение статистических уязвимостей на этом этапе заключается в рассмотрении всех сценариев, тесты по которым выявят недопустимое отклонение математического ожидания прибыли какой-либо группы пользователей, и исправлении логики работы или реализации приложения для устранения этого эффекта.

5. Перед публикацией приложения в общий доступ необходимо также провести настройку различных параметров приложения на основе статистического анализа и имитационного моделирования. Статистические уязвимости зачастую являются следствием неправильной установки параметров приложения, поэтому нужно удостовериться, что предполагаемые настройки приложения не приведут к статистической уязвимости. Тоже самое необходимо проводить и перед любым изменением настроек уже работающего приложения.

6. После публикации приложения необходим постоянный мониторинг различных параметров работы приложения с целью своевременного обнаружения и реагирования на атаки, использующие статистические уязвимости. Особенностью статистических уязвимостей является долгосрочность их использования, что является одновременно и плюсом и минусом данного типа уязвимостей с точки зрения разработчиков проекта. С одной стороны, обнаружить использование уязвимости такого типа может быть затруднительно, т. к. на небольших промежутках времени эти операции могут не отличаться от обычных действий пользователей, а хакеры, которые пытаются их использовать, могут быть в убытке довольно продолжительное время. С другой стороны, ущерб от таких уязвимостей крайне редко бывает быстрым, потери при своевременном их обнаружении можно сильно ограничить, и у разработчиков есть возможность оперативно исправить ошибки без больших потерь средств. Однако для того, чтобы вовремя отреагировать на начавшуюся попытку использования статистической уязвимости, разработчики всех приложений с потенциальным риском существования этого типа уязвимостей, обязаны иметь набор инструментов для мониторинга использования приложения [18, 19], таких как:

6.1. Мониторинг прибыли пользователей, разбор причин резкого роста или падения прибыли и/или убытка различных групп пользователей проекта (провайдеров ликвидности, инвесторов и т. п.);

6.2. Мониторинг активности использования различных функций приложения, разбор причин резкого роста активности определенных функций (особенно функций, предполагающих редкое использование);

6.3. Мониторинг повторяющихся действий, особенно с крупными объемами средств (многие статистические уязвимости предполагают множество повторяющихся действий, причиняющих максимальный ущерб, как правило, на большие суммы);

6.4. Постоянное моделирование потенциальных экстремальных ситуаций: что произойдет при резком падении или росте цен оракулов и т. п.;

6.5. Автоматическая остановка функций смарт контракта при достижении пороговых значений критических параметров (например, потери больше 10% вложенных средств за короткий промежуток времени, изменение цен оракулов больше чем на 10% за короткий промежуток времени и т. п.).

Устранение статистических уязвимостей на этом этапе заключается в своевременной остановке всего приложения, или его функций, приводящих к уязвимости, оперативный анализ атаки, выявление статистических уязвимостей и исправление реализации или логики работы приложения, после чего возобновление работы приложения.

В настоящее время большинство реально работающих смарт контрактов проектов, которые потенциально могут иметь статистические уязвимости, не выполняют многие из предложенных рекомендаций, в частности, не ведут активный мониторинг использования проекта, а также не проводят имитационное моделирование на реальных данных. Реальные длящиеся во времени атаки, использующие статистические уязвимости, через некоторое время часто находят пользователи проектов, а не их разработчики, что приводит к существенному ущербу пользователям проекта из-за продолжительности атаки и несвоевременного устранения проблемы. Соблюдение рекомендаций, предложенных в данной статье, позволит множеству блокчейн проектов обнаружить и устранить статистические уязвимости, а также своевременно отреагировать на реальные атаки с использованием статистических уязвимостей, предотвратив существенные потери активов пользователей.

Заключение

В данной статье дано определение статистическим уязвимостям в смарт контрактах, показан реальный денежный ущерб от этого типа уязвимостей на примерах найденных уязвимостей в реальных смарт контрактах на суммы больше 1 миллиона долларов в каждом случае, произведена оценка потенциального ущерба от уязвимостей данного типа для различных категорий приложений, которая составила более 4,5 миллиардов долларов. Разработаны и предложены рекомендации для разработчиков и аудиторов по поиску, мониторингу и устранению статистических уязвимостей.

Отсутствие глубоких исследований данного типа уязвимостей смарт контрактов при одновременном существенном риске финансовых потерь от их применения свидетельствуют о важности поиска данного типа ошибок и о необходимости дальнейших исследований в этой области.

СПИСОК ИСТОЧНИКОВ

1. Hu B. A comprehensive survey on smart contract construction and execution: Paradigms, tools, and systems / B. Hu [et al.] // Patterns. – 2021. – № 2. – URL: https://doi.org/10.1016/j.patter.2020.100179.
2. Kushwaha S. S. Ethereum Smart Contract Analysis Tools: A Systematic Review / S. S. Kushwaha [et al.] // IEEE Access. – 2022. – Vol. 10. – pp. 57037-57062 – URL: https://doi.org/10.1109/ACCESS.2022.3169902.
3. Atzei N. A survey of attacks on Ethereum smart contracts (SoK). / N. Atzei, M. Bartoletti, T. Cimoli // Proceedings of International Conference on Principles of Security and Trust. – 2017. – pp. 164-186. – URL: https://doi.org/10.1007/978-3-662-54455-6_8.
4. Delmolino K. Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab. / K. Delmolino [et al.] // Financial Cryptography Workshops, ser. Lecture Notes in Computer Science. – 2016. – Vol. 9604. – pp. 79-94. – URL: https://doi.org/10.1007/978-3-662-53357-4_6.
5. Chen J. Defining smart contract defects on Ethereum / J. Chen [et al.] // IEEE Trans. Software Eng. – 2022. – № 48. – pp. 327-345.
6. Zhang P. A framework and dataset for bugs in ethereum smart contracts / P. Zhang, F. Xiao, X. Luo. // ICSME. IEEE. – 2020. – pp. 139-150.
7. Classification of smart contract vulnerabilities. [Электронный ресурс] – URL: https://github.com/smartdec/classification (дата обращения: 06.07.2023).

8. Dingman W. Classification of smart contract bugs using the NIST bugs framework / W. Dingman // SERA. IEEE. – 2019. – pp. 116-123.

9. D. Perez. Smart contract vulnerabilities: Vulnerable does not imply exploited / D. Perez, B. Livshits // USENIX Security Symposium. [Электронный ресурс] – 2021. – URL: https:// www.usenix.org/system/files/sec21-perez.pdf (дата обращения: 06.07.2023)

10. Most common smart contract bugs of 2020 [Электронный ресурс] – 2020. – URL: https://medium.com/solidified/most-commonsmart-contract-bugs-of-2020-c1edfe9340ac (дата обращения: 06.07.2023)

11. DASP - TOP 10 [Электронный ресурс] – URL: https://dasp.co/ (дата обращения: 06.07.2023)

12. Daian P. Flash boys 2.0: Frontrunning in decentralized exchanges, miner extractable value, and consensus instability / P. Daian [et al.] // 2020 IEEE Symposium on Security and Privacy (SP). – 2020. – pp. 910-927.

13. Zhou L. High-frequency trading on decentralized on-chain exchanges / L. Zhou [et al.] // 2021 IEEE Symposium on Security and Privacy (SP). – 2021. – pp. 428-445.

14. Gains Trade [Электронный ресурс] – URL: https://gains.trade/ (дата обращения: 10.07.2023)

15. TWAP Trading on Ethereum and Arbitrum DEX. Trade with SIZE | Integral [Электронный ресурс] – URL: https://integral.link/ (дата обращения: 13.07.2023)

16. Update to recent vulnerability report. The post mortem. [Электронный ресурс] – 2022. – URL: https://integral.link/update-to-recent-vulnerability-report-the-post-mortem/ (дата обращения: 13.07.2023)

17. Defi Llama. [Электронный ресурс] – URL: https://defillama.com/ (дата обращения: 13.07.2023)

18. DeFiRanger: Detecting Price Manipulation Attacks on DeFi Applications [Электронный ресурс] – 2021. – URL: https://doi.org/10.48550/arXiv.2104.15068 (дата обращения: 13.07.2023)

19. Zhou L. On the just-in-time discovery of profit-generating transactions in defi protocols / L. Zhou [et al.] // 2021 IEEE Symposium on Security and Privacy (SP). – 2021. – pp. 919-936.

STATISTICAL VULNERABILITIES IN SMART CONTRACTS

© 2023 P. N. Anokhin (Orel, Russia)

Existing research of the smart contract vulnerabilities focus mainly on technical vulnerabilities, without paying attention to statistical vulnerabilities, which can be present even in the applications with technically perfect implementation. In this article statistical vulnerabilities essence is described, damage from these vulnerabilities is calculated based on analysis of real vulnerabilities in working smart contracts, potential damage is estimated in different application categories, recommendations are developed about the methods offered to discover and mitigate statistical vulnerabilities. Article materials are of practical value for developers and smart contract security experts, allowing them to use the knowledge gained to discover and mitigate new vulnerability type, making financial applications on blockchain technology more secure and safe for end users.

Keywords: smart contract, information security, statistical vulnerability, blockchain, decentralized finances, statistical modeling.