Инженерный вестник Дона, №1 (2026)
ivdon.ru/ru/magazine/archive/n1y2026/10650

Превентивная защита децентрализованных параметрических страховых протоколов от атак на оракулы с использованием флеш-кредитов

Н.С. Бексаев

Петербургский государственный университет путей сообщения Императора Александра I, Санкт-Петербург

Аннотация: Децентрализованное параметрическое страхование представляет собой многообещающую инновацию в индустрии децентрализованных финансов, предлагая автоматизированные и прозрачные выплаты на основе проверяемых внешних данных. Однако эта зависимость от внешних данных, поставляемых оракулами, создает критическую уязвимость. Сложность смарт-контрактов может приводить к непредвиденным последствиям, что было продемонстрировано атаками с использованием флеш-кредита: мгновенного займа, который должен быть возвращен в рамках одной и той же транзакции блокчейна. Эти атаки стали одним из самых разрушительных векторов экономических атак, позволяя злоумышленникам манипулировать ценовыми оракулами и инициировать мошеннические страховые выплаты. Существующие защитные механизмы, такие, как оракулы со средневзвешенной по времени ценой, являются пассивными и не всегда достаточны для предотвращения таких атак. В этой статье представлена оригинальная модель превентивной защиты. Автор формализует атаку на оракулы с использованием флеш-кредита как теоретико-игровую модель с тремя участниками: Злоумышленником, Протоколом и Арбитражером, где в роли последнего выступает автоматическая торговая программа, реализованная в смарт-контракте. Используя математический аппарат, основанный на инварианте автоматического маркет-мейкера, автор определяет точное "окно уязвимости" — экономические условия, при которых атака выгодна для злоумышленника и невыгодна для рыночных арбитражеров. На основе этого анализа предложена архитектура "SC-Guard" — система смарт-контрактов в превентивной защитой от атак с использованием флеш-кредита. Такая система в реальном времени отслеживает транзакции, еще не включенные в блоки, на предмет угроз и динамически изменяет экономические стимулы, субсидируя Арбитражера для нейтрализации атак до их исполнения. Вместо того чтобы пассивно противостоять манипуляциям, предлагается архитектура системы, которая активно делает экономически невыгодными атаки с использованием флеш-кредита, обеспечивая более высокий уровень безопасности для протоколов децентрализованного параметрического страхования.

Ключевые слова: децентрализованные финансы, параметрическое страхование, флеш-кредит, атака на блокчейн-оракул, теория игр, безопасность смарт-контрактов, максимальная извлекаемая ценность, превентивная защита.

Введение

Параметрическое страхование как часть рынка страховых услуг подходит для реализации на блокчейне. В отличие от традиционного страхования, требующего длительной оценки убытков, параметрические полисы срабатывают автоматически при выполнении заранее определенного, объективно измеряемого показателя. Смарт-контракты позволяют кодифицировать эту логику, создавая децентрализованные страховые протоколы (Decentralized protocol of insurance – DePi), которые могут предлагать страхование от задержек рейсов, погодных явлений или сбоев в работе других протоколов децентрализованных финансов.

Фундаментальная проблема этой модели заключается в ее зависимости от внешнего мира. Большинство децентрализованных страховых протоколов полагаются на ценовые оракулы для определения как стоимости залога, так и срабатывания триггеров. "Проблема оракулов" — как безопасно и достоверно доставить реальные данные в детерминированную среду блокчейна — является центральной проблемой [1].

С появлением флеш-кредитов эта зависимость превратилась в критическую экономическую уязвимость. Флеш-кредит — это мгновенный необеспеченный займ в децентрализованных финансах (Decentralized finances — DeFi), который должен быть возвращён в рамках одной и той же транзакции блокчейна. Если заемщик не успевает вернуть сумму кредита в течение этой транзакции, она автоматически отменяется, и кредитор не несёт потерь. Такой кредит не требует залога или проверки кредитоспособности и используется для быстрых операций арбитража или запроса ликвидности. Также они могут иметь сложные и опасные побочные [2] эффекты.

Злоумышленники используют этот капитал для мгновенной манипуляции ценами на активах на децентрализованных биржах, которые служат источником данных для оракулов. Атакующий может купить страховой полис, затем манипулировать оракулом для мошеннического срабатывания условия для выплаты, получить ее и погасить кредит – все это в одной транзакции [3, 4].

Существующие защитные меры, такие как использование оракулом данных о средней цене актива, взятые по времени, без учета объема торгов (time-weighted average price - TWAP), являются пассивными. Они замедляют реакцию оракула на изменение цены, что может предотвратить самые простые атаки, но они не являются панацеей и уязвимы для более продолжительных или сложных манипуляций.

В данной работе предлагается превентивный, экономический подход [2] к безопасности. Вклад автора заключается в следующем:

1. Теоретико-игровая модель: моделируется атака на оракул как динамическая игра с тремя участниками: Злоумышленником (A), Протоколом (P) и Арбитражером (M), опираясь на существующие работы по игровому моделированию безопасности DeFi [5, 6, 7].

2. Математическая формализация: для точного определения "окна уязвимости" — набора рыночных условий, при которых атака выгодна для A и невыгодна для M используется свойство пулов автоматических маркет-мейкеров (automatic market maker - AMM), которое заключается в том, что он обеспечивает мгновенную ликвидность, автоматически корректируя цену и соотношение активов в пуле через формулу: $R_x * R_y = k$, где R_x и R_y – активы в пуле ликвидности, а k — постоянная величина.

3. Представлена "SC-Guard", архитектура смарт-контрактов, которая отслеживает транзакции, еще не включенные в блоки (далее мемпул), как это описано в основополагающей работе "Flash Boys 2.0" [8], и активно закрывает "окно уязвимости", субсидируя Арбитражеров для того, чтобы любая манипуляция своевременно корректировалась [9].

Анализ атаки на оракул

Атака на DePI с использованием флеш-кредита изображена на рис.1:

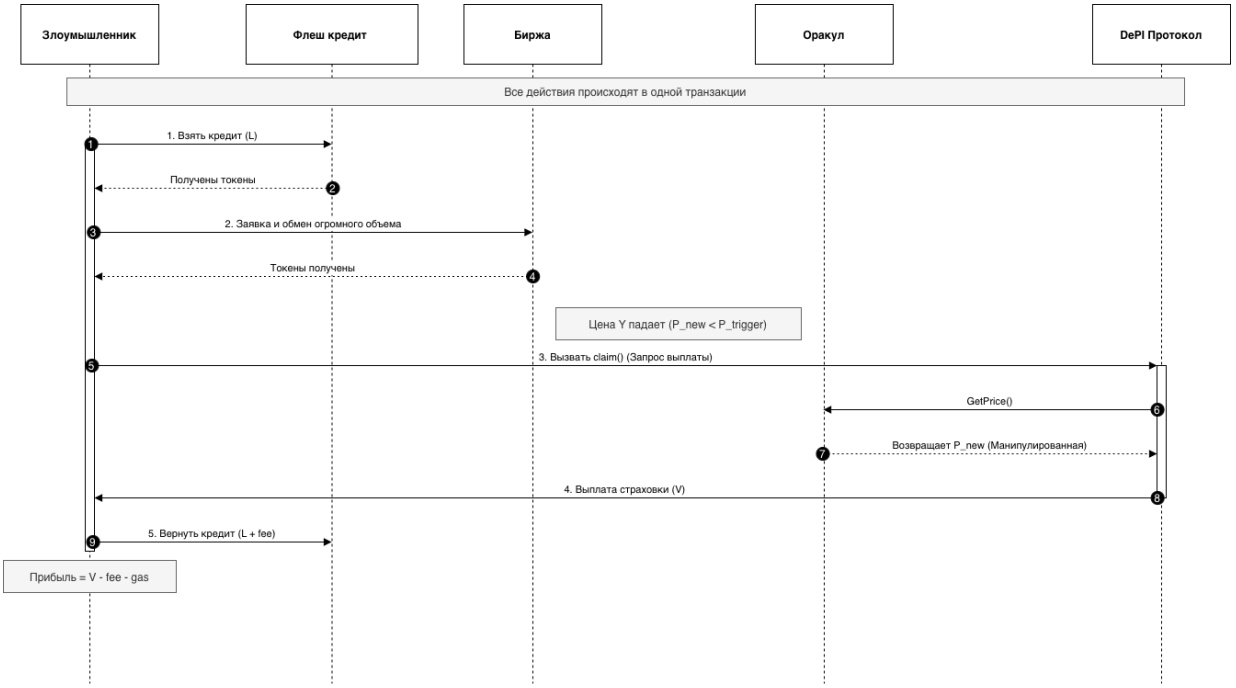

Рис. 1. – Атака с использованием флеш-кредита

На диаграмме изображены из следующих компонентов:

1. Протокол DePI (P): Смарт-контракт, который содержит логику, которая при помощи оракула определяет цену токена Y и в случае, если стоимость токена Y ниже пороговой цены P_T производит страховую выплату V.

2. Оракул (O): Система, которая считывает спотовую цену актива Y с децентрализованной биржи (Биржа).

3. Биржа (наделена функцией AMM): Пул ликвидности, цена в котором определяется инвариантом постоянного произведения $R_x * R_y = k$.

4. Флеш-кредит: Источник, предоставляющий злоумышленнику заем L, в валюте X.

Последовательность атаки:

1. Злоумышленник, ранее купивший полис, берет флеш-кредит L в токене X.

2. Злоумышленник обменивает L токенов X на токен Y на Бирже, вызывая значительное проскальзывание стоимости токена Y и обрушивая его спотовую цену до P_{new}.

3. Протокол DePI (P) обращается к Оракулу (O), который считывает манипулированную цену P_{new}.

4. Поскольку $P_{new} < P_T$, срабатывает выплаты страховки, и протокол P выплачивает Злоумышленнику V.

5. Злоумышленник использует часть выплаты V для погашения флеш-кредита L и платит комиссию $f * L$, где $f \in (0,1]$.

Прибыль Злоумышленника Π_A составляет $\Pi_A = V - f * L - C_{gas}^A$, где C_{gas}^A – затраты на транзакцию. Так выглядит экономическая манипуляция, при которой каждый компонент технически работает штатно. Подобные атаки на уровне протокола, связанные с манипуляцией ценами, являются известным вектором, для обнаружения которого создаются автоматические торговые программы, которые используют стратегию максимальной извлекаемой ценности, для получения прибыли (Maximal Extractable Value – MEV) [10, 11]. Такие программы называются MEV-ботами: они сканируют мемпул на предмет выгодных возможностей, а затем манипулируют

порядком, включением или исключением транзакций в новый блок с целью извлечь прибыль.

Теоретико-игровая модель системы защиты от атаки

Для разработки превентивной защиты необходимо провести моделирование экономических стимулов всех участников. Для чего разработана модель игры "Манипуляция оракулом", опираясь на существующие теоретико-игровые модели [5].

Определим игроков в данной модели:

- Злоумышленник (A): Рациональный игрок, стремящийся максимизировать прибыль (Π_A) путем эксплуатации протокола.
- Протокол (P): В базовой модели пассивен. Его цель — сохранить свой пул капитала (который Злоумышленник пытается украсть).
- Арбитражер (M): Рациональный, нейтральный игрок (обычно MEV-бот [11]), который ищет любую возможность арбитража. Его цель — максимизировать прибыль (Π_M) путем исправления рыночных неэффективностей [12].

Функция выигрыша

Атака Злоумышленника создает искусственную неэффективность: цена P_{new} на Бирже становится намного ниже "истинной" рыночной цены P_M (цена на других биржах). Это создает возможность для Арбитражера.

- Выигрыш Злоумышленника (Π_A):
  - Если M не вмешивается: $\Pi_A = V - C_{gas}^A > 0$ (Атака успешна).
  - Если M вмешивается: $\Pi_A = -C_{gas}^A$ (Атака проваливается, так как M исправляет цену до того, как оракул ее зафиксирует, но затраты C_{gas}^A уже понесены).

- Выигрыш Арбитражера ($П_M$):
  - Если М вмешивается: $П_M = P_{arb} - C_{gas}^M$, где P_{arb}— прибыль от арбитража, а C_{gas}^M — его затраты на транзакцию.
  - Если М не вмешивается: $П_M = 0$.

Равновесие и условия для проведения атаки

Рациональный Злоумышленник будет атаковать только в том случае, если он ожидает, что Арбитражер не будет вмешиваться. Арбитражер не будет вмешиваться, если его ожидаемая прибыль отрицательна или равна нулю ($П_M \leq 0$).

Следовательно, атака возможна и выгодна для Злоумышленника, если существует такой объем L, который создает "Окно уязвимости":

1. Условие срабатывания триггера: $P_{new}(L) < P_T$
2. Условие получения прибыли злоумышленником: $V - C_{gas}^A(L) > 0$
3. Условие бездействия арбитражера: $P_{arb}(L) - C_{gas}^M \leq 0$

Условие 3 является ключевым при построении защиты. Оно возникает, когда манипуляция достаточно велика, чтобы вызвать выплату V, но прибыль от арбитража P_{arb} слишком мала, чтобы покрыть высокие затраты на транзакцию C_{gas}^M.

Математическая формализация окна уязвимости

Рассмотрим расчет стоимости манипуляции (Условие 1). Цена в пуле, исходя из логики работы автоматического маркет-мейкера определяется следующим равенством $R_x \cdot R_y = k$ до атаки $P = R_x/R_y$. Злоумышленник продает $\Delta_y = L$ токенов Y за Δ_x токенов X. Новая цена:

$$P_{new} = \frac{R_x - \Delta_x}{R_y + L} = \frac{R_x - \frac{R_x L}{R_y + L}}{R_y + L} = \frac{R_x R_y}{(R_y + L)^2} = \frac{k}{(R_y + L)^2} \quad (1)$$

Условие срабатывания триггера $P_{new} < P_T$ выполняется, если:

$$L > \sqrt{\frac{k}{P_T}} - R_y \quad (2)$$

Полученное неравенство определяет минимальный размер L_{min}, необходимый для атаки, и, следовательно, минимальную стоимость атаки L_{attack}.

Перейдем к прибыли от арбитража (Условие 3), которой мотивирован Арбитражер. Он видит разницу между P_{new} и истинной рыночной ценой P_M. Он может купить $\Delta y'$ токенов Y в пуле, пока P_{new} не вернется к P_M. Его прибыль P_{new} (игнорируя проскальзывание и не изменяя P_M) составляет:

$$P_{arb} = \Delta y' \cdot P_M - \Delta x',$$

где $\Delta x'$ равна стоимости покупки $\Delta y'$. Прибыль P_{arb} напрямую зависит от глубины манипуляции L.

"Окно уязвимости" — это такое состояние пула (низкая ликвидность L) и рынка (высокие затраты на транзакцию C_{gas}^M), при котором Злоумышленник может найти такой L, что $L \geq L_{min}$ (Условие 1), $V \geq C_{gas}^A(L)$ (Условие 2), но $P_{arb}(L) \leq C_{gas}^M$ (Условие 3).

На рис. 2 визуализирован механизм формирования «окна уязвимости». Сплошная линия представляет собой кривую ивариантa AMM, определяющую ценообразование на децентрализованной бирже.

В нормальном состоянии стоимость Y находится в точке P_{market}. В ходе атаки злоумышленник совершает крупную продажу токенов, сдвигая точку равновесия по кривой вниз до P_{new}, преодолевая пороговое значение P_T. Ключевым элементом диаграммы является заштрихованная область. Она обозначает диапазон цен, при котором страховой случай уже наступил, но

рыночным арбитражерам экономически невыгодно восстанавливать цену, так как затраты на проведение транзакции превышают возможную прибыль. Именно попадание цены в эту зону графика позволяет злоумышленнику провести атомарную атаку без риска быть перехваченным MEV-ботами.

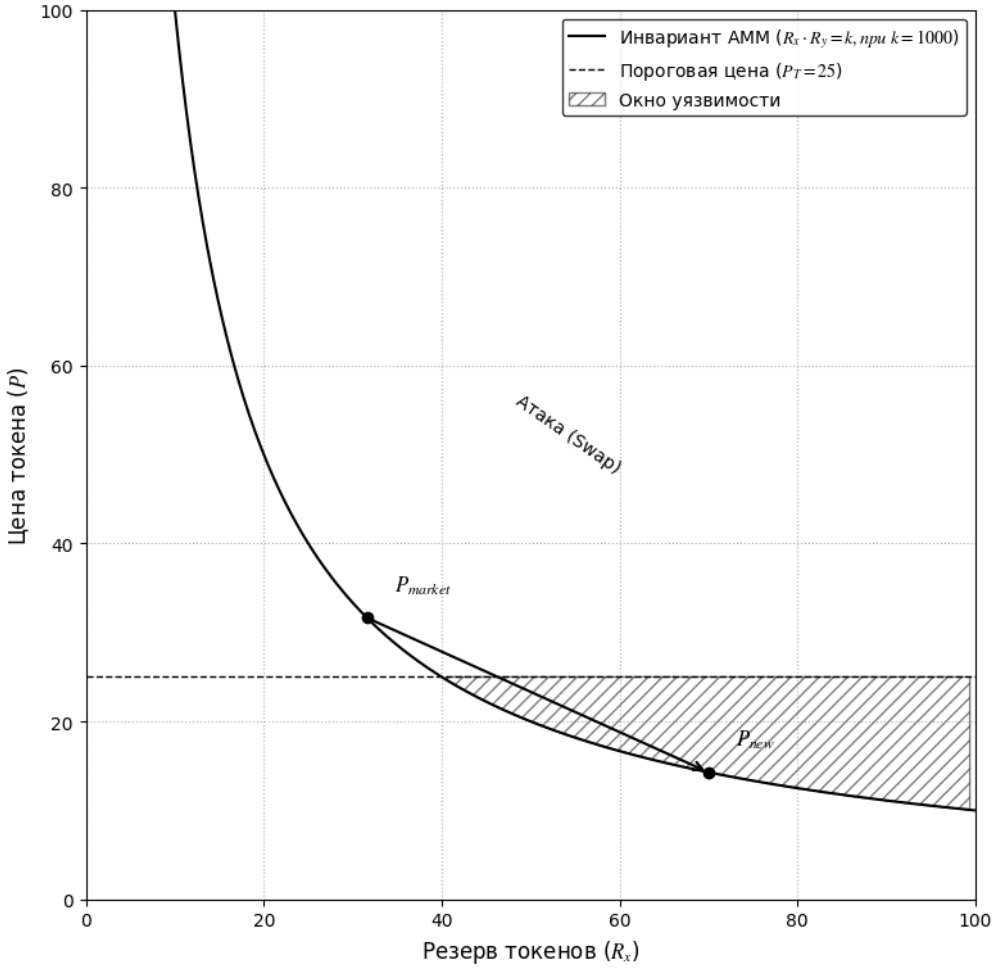

Рис. 2. – окно уязвимости

Предлагаемая система "SC-Guard"

Вместо пассивной защиты TWAP, в данной статье предлагается активная система противодействия атаке, которая делает Условие 3 невыполнимым, с целью гарантировать, что:

$$\Pi_M > 0 \quad \text{всегда, когда } \Pi_A > 0.$$

Система SC-Guard" состоит из трех модулей, развернутых протоколом DePI и изображена на рис. 3:

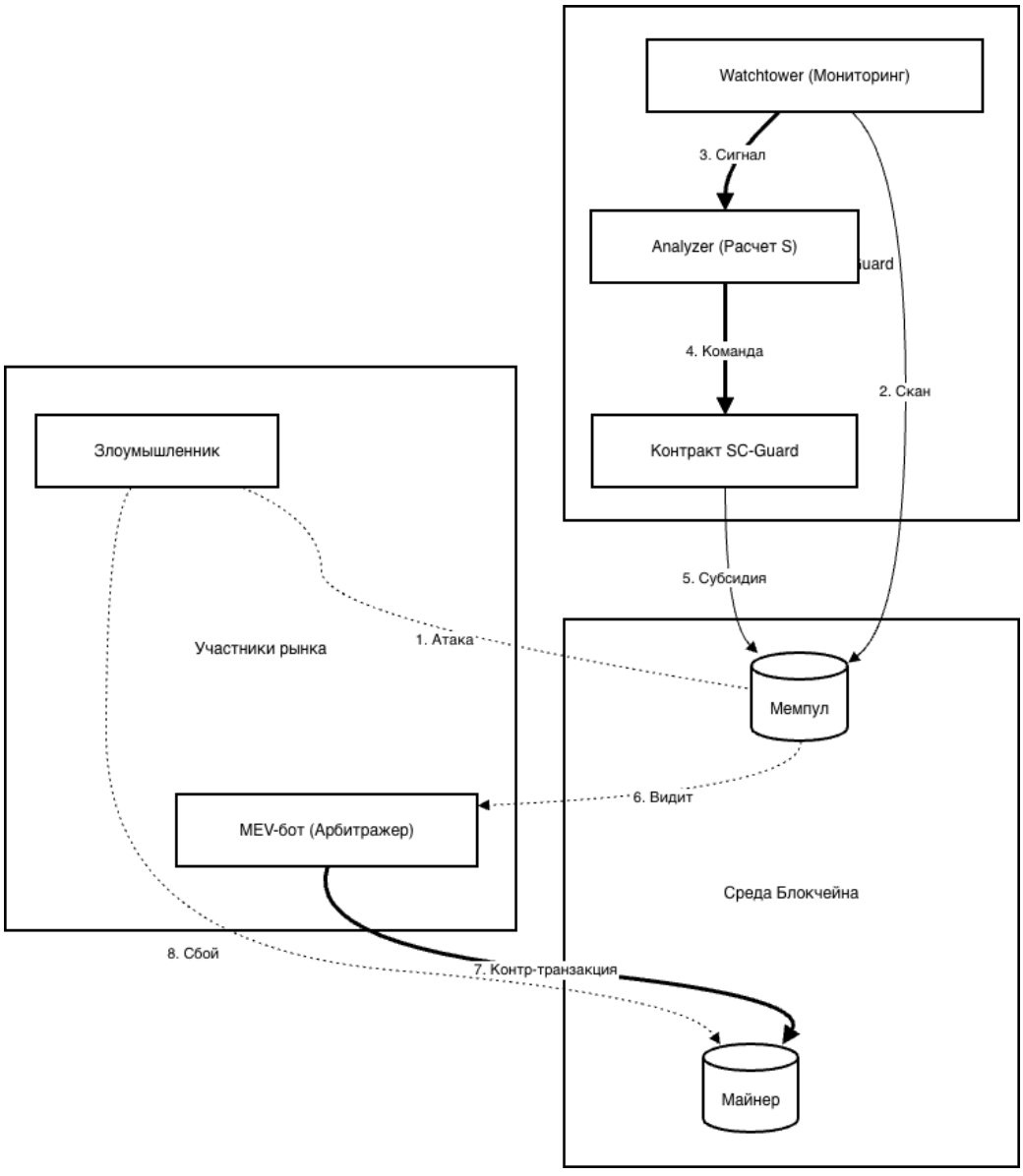

Рис. 3. – Архитектура SC-Guard

1. Модуль Мониторинга (Watchtower): MEV-бот, который сканирует мемпул в поисках транзакций, соответствующих паттерну атаки. Такая концепция мониторинга основана на существующих исследованиях по

безопасности DeFi, таких, как основополагающая работа по MEV-ботам[6], и реальных системах, таких как DeFiRanger [4, 11].

2. Модуль Анализа (Analyzer): Смарт-контракт, который в реальном времени использует расчеты по формулам (1) и (2). При обнаружении подозрительной транзакции в мемпуле, он рассчитывает $P_{new}(L)$, $P_{arb}(L)$ и $C_{attack}(L)$.

3. Модуль Контракт (SD-Guard): Смарт-контракт, который хранит средства протокола и имеет право действовать.

Субсидирование арбитража как механизм реагирования

Когда Модуль Анализа обнаруживает транзакцию в "окне уязвимости" (т.е. $P_{arb}(L) \leq C_{gas}^{M}$. Модуль немедленно действует, выполняя 2 операции:

1. Рассчитывает минимальную субсидию S, необходимую для того, чтобы сделать арбитраж выгодным:

$$S = \left(C_{gas}^{M} - P_{arb}(L)\right) + \epsilon,$$

где $\epsilon -$ дополнительная прибыль.

2. Размещает эту субсидию S в публичном контракте, предлагая ее любому, кто успешно выполнит контр-арбитражную транзакцию, восстанавливающую цену.

Результат

Рациональные MEV-боты [6], постоянно сканирующие в поисках прибыли, немедленно увидят эту новую, теперь уже выгодную возможность ($\Pi_M = (P_{arb} + S) - C_{gas}^{M} > 0$). Они будут соревноваться за то, чтобы

вставить свою контр-транзакцию в тот же блок, что и атака Злоумышленника.

С точки зрения Злоумышленника игра меняется. Он больше не может полагаться на Условие 3. Его расчеты теперь показывают, что Арбитражер всегда будет вмешиваться, поскольку Протокол активно субсидирует это вмешательство. Его ожидаемый выигрыш становится отрицательным ($\Pi_A = -C_{attack}$), и атака не будет инициирована [12].

Таким образом реализуется превентивная защита, поскольку угроза вступления в игру Арбитражера устраняет стимул к самой атаке.

Эксперимент и оценка

Для проверки эффективности "SC-Guard" была произведена симуляция атаки в локальном тестовом блокчейне. Использовался тестовый стенд сети Ethereum с помощью фреймворка Hardhat. Это позволило использовать реальные состояния пулов ликвидности Uniswap v2 и реалистичные затраты на транзакцию, используя методологии, аналогичные тем, что применяются в обзорах инструментов анализа смарт-контрактов [11].

Экспериментальная программная реализация системы состоит из следующих элементов:

1. Смарт-контракт, предлагающий полис с выплатой = 100000 USDC (R_x), если цена WETH (R_y), упадет ниже P_T= 3000 USDC, при заданной рыночной стоимости P_M = 3100 USDC.
2. Тестовый реального пула Uniswap v2 WETH/USDC.
3. Контракт, развернутый с фондом субсидий.

4. Скрипт, выполняющий атомарную атаку: заем флеш-кредита в USDC, продажа их за WETH для обрушения цены.
5. Скрипт, отслеживающий мемпул на предмет арбитражных возможностей $\Pi_M > 0$.

Результаты эксперимента

Были протестированы три сценария, с такими настройками параметров атаки L, чтобы они попадали в "окно уязвимости", где P_{arb} был меньше, чем стоимость транзакции для арбитража C_{gas}^{M}.

Таблица №1

Результаты эксперимента

Сценарий	**Описание**	**Результат атаки**	**Прибыль Злоумышленника USDC**	**Затраты протокола USDC**
Базовый	SC-Guard отключена	Успех	$V - f \cdot L - C_{gas}^{A} \approx 85000$	$S \approx 100000$
Сценарий 1	SC-Guard включена	Провал	$C_{gas}^{A} \approx 150$	$S \approx 200$
Сценарий 2	SC-Guard отключена, используется TWAP-оракул	Провал	$C_{gas}^{A} \approx 100$	0

Обсуждение результатов

В базовом сценарии (Базовый) атака прошла успешно, как и ожидалось, что привело к катастрофическим потерям для протокола, это можно видеть на рис. 4 в левой прямоугольной области. В Сценарии 1 (SC-Guard) повел себя штатно. Была обнаружена подозрительная транзакция в мемпуле. После чего была рассчитана стоимость арбитражной транзакции $P_{arb} \approx 50$ USDC, что было ниже $C_{gas}^{M} \approx 200$ USDC.

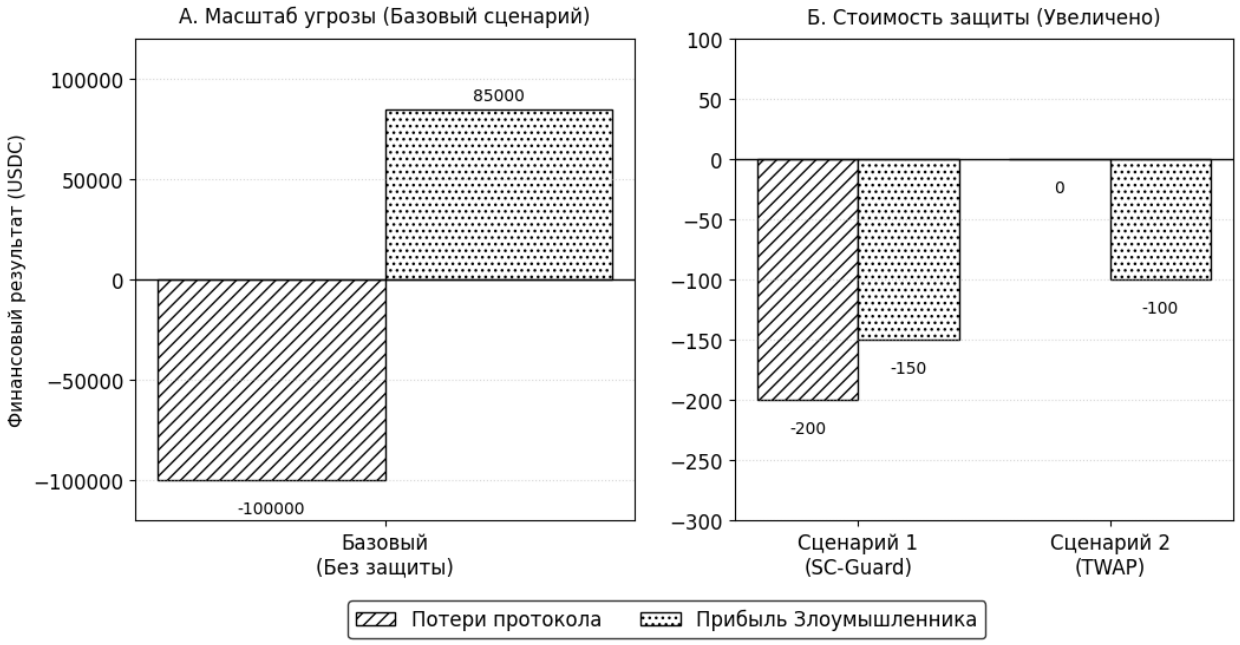

Рис. 4. – Сравнение финансовых результатов (раздельный масштаб)

Была предложена субсидия $S = (200 - 50) + 50 = 200\ USDC$. Арбитражный бот обнаружил эту субсидию, рассчитал свою новую прибыль $P_M = 50 + 200 - 200 = +50\ USDC$ и выполнил арбитраж, опередив вызов Злоумышленника. Цена была восстановлена, и требование Злоумышленника было отклонено, что привело к потере им только затрат на транзакцию. Протокол понес незначительные, контролируемые расходы в размере $S = 200\ USDC$, предотвратив потерю $V = 100000\ USDC$.

Сценарий 2 (TWAP) показывает, что TWAP-оракул также является эффективной защитой от этого конкретного вектора атаки. Однако предложенный в этой статье фреймворк предназначен для защиты протоколов, которые должны использовать спотовые цены или где TWAP нецелесообразен. Система SC-Guard функционирует как активный "автоматический выключатель» для любого оракула, основанного на спотовой цене.

Дальнейшие исследования

В ходе анализа векторов угроз было выявлено, что использование злоумышленниками приватных пулов транзакций может позволить обойти модуль мониторинга мемпула (Watchtower), скрыв транзакцию атаки до момента ее включения в блок. Для нивелирования данного риска может быть предложен механизм временной блокировки выплаты [13].

Для этого предлагается модифицировать логику смарт-контракта DePI, разделив атомарную операцию выплаты на две последовательные фазы:

1. Инициация требования, которая происходит в момент фиксации триггерного события (манипулированной цены);
2. Исполнение выплаты и фактический перевод средств, который станет доступен только спустя интервал $\Delta_t = 1$ блок после инициации.

Данная модификация, принципиальная схема которой изображена на Рис.5 значительно меняет модель безопасности по двум причинам:

1. Поскольку флеш-кредит обязан быть возвращен в рамках одной атомарной транзакции, злоумышленник технически не может использовать будущую страховую выплату, которая доступна через интервал времени Δ_t

для погашения займа. Это полностью устраняет вектор атаки с использованием заемных средств [14].

2. Даже если манипуляция ценой была проведена скрытно через приватный пул, она становится публичной сразу после майнинга блока. Интервал Δ_t предоставляет системе «SC-Guard» гарантированное временное окно для анализа состояния рыночной стоимости R_x и R_y. Если система обнаруживает, что выплата была запрошена на основе манипулированной цены, она активирует механизм субсидирования арбитража. Арбитражеры восстанавливают рыночную цену в последующем блоке и условие выплаты аннулируется до момента перевода средств.

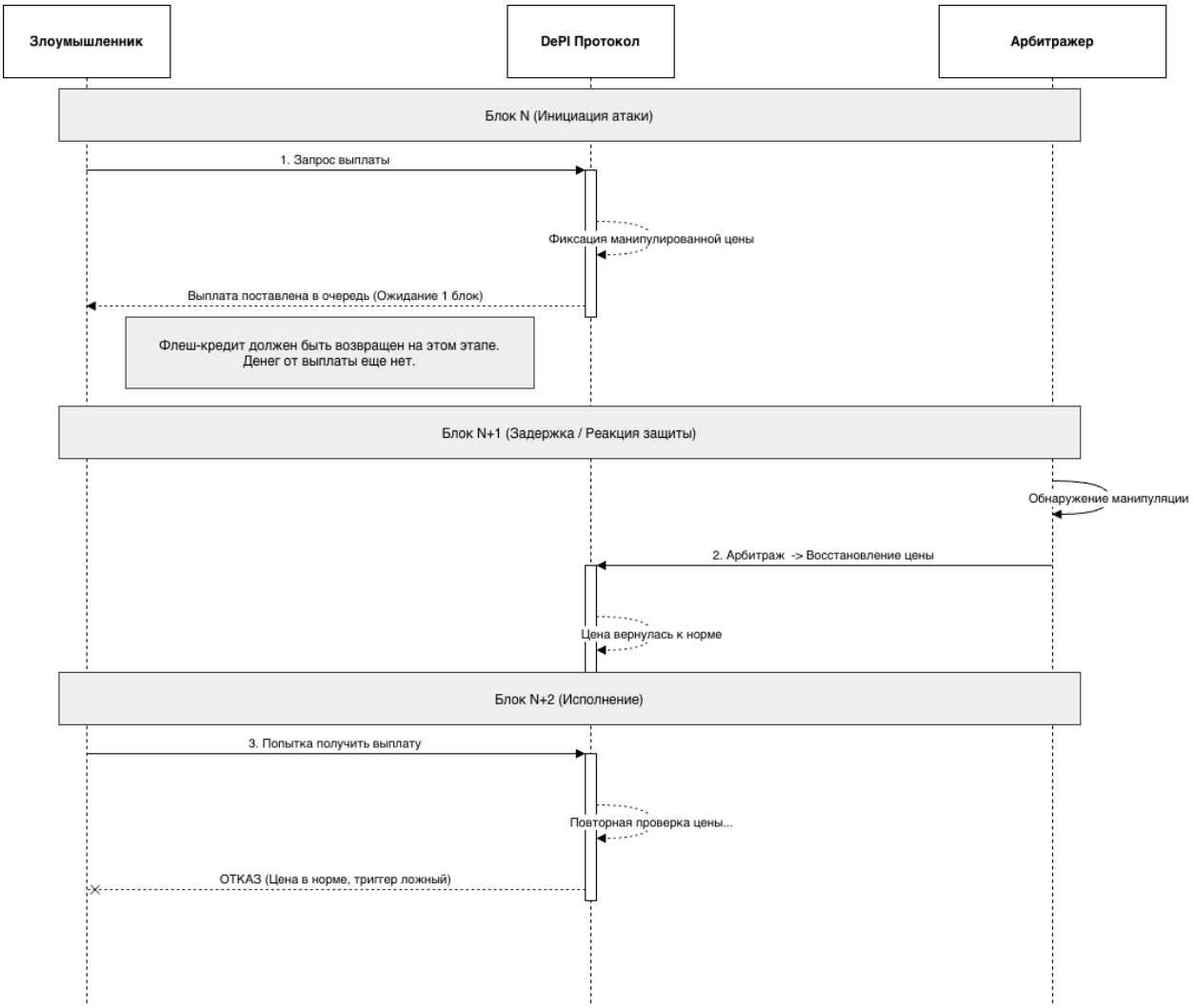

Рис. 5. - Нарушение атомарности атаки при внедрении механизма временной блокировки

Таким образом, внедрение минимальной задержки $\Delta_t = 1$ блок трансформирует «SC-Guard» из вероятностной превентивной защиты в детерминированную систему гарантированного реагирования, устойчивую к любым методам сокрытия транзакций.

Вместе с тем, несмотря на доказанную эффективность архитектуры «SC-Guard» и механизма временной блокировки, существует ряд

направлений для дальнейшего развития и оптимизации предложенной модели:

- Защита от каскадных атак. Текущая модель рассматривает взаимодействие «один протокол — один оракул». Будущие исследования должны быть направлены на масштабирование модели системы «SC-Guard» для защиты от системных рисков, где манипуляция ценой в одном пуле вызывает цепную реакцию ликвидаций в смежных протоколах;
- Интеграция моделей машинного обучения (ML). Эвристический анализ мемпула может быть дополнен вероятностными моделями [15]. Внедрение легковесных ML-моделей непосредственно в смарт-контракты позволит выявлять новые, ранее неизвестные паттерны атак [16];

Заключение

Экономические атаки, такие как манипуляции оракулами с помощью флеш-кредитов, не могут быть полностью решены только криптографическими или пассивными методами. Они требуют экономически обоснованных решений, как это предлагается в работах по формальным методам и теории игр. В данной статье автор формализовал такую атаку как теоретико-игровую задачу и математически определили "окно уязвимости".

Автором статьи была предложена и экспериментально опробована система "SC-Guard", которая переходит от пассивной обороны к превентивному сдерживанию. Предлагаемая система создает "экономический иммунный ответ", динамически субсидируя MEV-botf для нейтрализации угрозы. Если мы сделаем любую атаку невыгодной по экономическим причинам, ликвидируется стимул к ее проведению. Будущие исследования могут расширить эту модель для защиты от более сложных,

многопротокольных каскадных атак и оптимизировать эффективность механизмов мониторинга [4], с точки зрения затрат на транзакции.

Литература

1. Chainlink Labs. Chainlink 2.0: Next Steps in the Evolution of Decentralized Oracle Networks: Whitepaper. New York. Chainlink Labs. 2021. 136 p.

2. Тищенко, Б. А., Катасонов, А. С. Анализ методов поиска уязвимостей в смарт-контрактах. Вестник УрФО. Безопасность в информационной сфере. 2023. № 2 (48). С. 67–78.

3. Wang, D., Wu, S., Lin, Z., Wu, L., Yuan, X. DeFiRanger: Detecting Price Manipulation Attacks on DeFi Applications. IEEE Transactions on Information Forensics and Security. 2023. Vol. 18. Pp. 2432–2445.

4. Zhou, L., Qin, K., Cully, A., Livshits, B., Gervais, A. On the Just-In-Time Discovery of Profit-Generating Transactions in DeFi Protocols. IEEE Symposium on Security and Privacy (SP). San Francisco. IEEE. 2021. Pp. 919–936.

5. Kulkarni, S., Diamandis, S., Chatzigiannis, P. Towards a Game-Theoretic View of MEV in Decentralized Finance. Financial Cryptography and Data Security. Willemstad. Springer. 2024. Pp. 345–360.

6. Capponi, A., Jia, R., Wang, Y. The Allocative Efficiency of Decentralized Exchange. Journal of Financial Economics. 2024. Vol. 155. P. 103819.

7. Bigi, G., Bracciali, A., Meola, G., Tuosto, E. Validation of Decentralised Smart Contracts Through Game Theory and Formal Methods. Programming Languages with Applications to Biology and Security. Cham. Springer. 2015. Pp. 142–161.

8. Daian, P., Goldfeder, S., Kellmann, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L., Juels, A. Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges. arXiv preprint. 2019. 20 p.

9. Zhang, Y., Ma, J., Li, Y. Flash-Loan-Based Attacks in DeFi: Taxonomy, Detection, and Mitigation. IEEE Transactions on Dependable and Secure Computing. 2024. Vol. 21. No. 2. Pp. 1134–1149.

10. Chen, T., Li, Z., Zhang, Y., Zhang, X. EtherScope: A Real-Time Detection System for Malicious Smart Contracts. ACM Transactions on Software Engineering and Methodology. 2023. Vol. 32. No. 3. Pp. 68:1–68:35.

11. Wu, L., Cheng, Y., Wang, D. Real-Time Detection of Flash Loan Attacks in DeFi using Graph Learning. IEEE International Conference on Blockchain. Bali. IEEE. 2023. Pp. 332–339.

12. Gupta, A., Sward, J., Cappos, J. MEV on Layer 2: A Survey of the State of the Art. arXiv preprint. 2024. 18 p.

13. Петренко, С. А. Модель квантовых и алгоритмических угроз безопасности для национальных блокчейн-экосистем. Вопросы кибербезопасности. 2022. № 1 (47). С. 53–63.

14. Positive Technologies. Уязвимости и угрозы в Web3: Аналитический отчет. Москва. Positive Technologies Research. 2024. 46 с.

15. Zhou, Y., Kumar, D., Bakshi, S., Mason, J., Miller, A., Reiter, M. K. An Empirical Study of DeFi Attacks. ACM Conference on Computer and Communications Security (CCS). Copenhagen. ACM. 2023. Pp. 2826–2840.

16. Choi, J., Kim, D., Kim, S. Smart Contract Vulnerability Detection using Graph Neural Networks. IJCAI International Joint Conference on Artificial Intelligence. Macao. IJCAI. 2023. Pp. 354–362.

References

1. Chainlink Labs. Chainlink 2.0: Next Steps in the Evolution of Decentralized Oracle Networks: Whitepaper. New York. Chainlink Labs. 2021. 136 p.

2. Tishhenko, B. A., Katasonov, A. S. Vestnik UrFO. Bezopasnost' v informacionnoj sfere. 2023. № 2 (48). pp. 67–78.

3. Wang, D., Wu, S., Lin, Z., Wu, L., Yuan, X. DeFiRanger: Detecting Price Manipulation Attacks on DeFi Applications. IEEE Transactions on Information Forensics and Security. 2023. Vol. 18. Pp. 2432–2445.

4. Zhou, L., Qin, K., Cully, A., Livshits, B., Gervais, A. On the Just-In-Time Discovery of Profit-Generating Transactions in DeFi Protocols. IEEE Symposium on Security and Privacy (SP). San Francisco. IEEE. 2021. Pp. 919–936.

5. Kulkarni, S., Diamandis, S., Chatzigiannis, P. Towards a Game-Theoretic View of MEV in Decentralized Finance. Financial Cryptography and Data Security. Willemstad. Springer. 2024. Pp. 345–360.

6. Capponi, A., Jia, R., Wang, Y. The Allocative Efficiency of Decentralized Exchange. Journal of Financial Economics. 2024. Vol. 155. P. 103819.

7. Bigi, G., Bracciali, A., Meola, G., Tuosto, E. Validation of Decentralised Smart Contracts Through Game Theory and Formal Methods. Programming Languages with Applications to Biology and Security. Cham. Springer. 2015. Pp. 142–161.

8. Daian, P., Goldfeder, S., Kellmann, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L., Juels, A. Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges. arXiv preprint. 2019. 20 p.

9. Zhang, Y., Ma, J., Li, Y. Flash-Loan-Based Attacks in DeFi: Taxonomy, Detection, and Mitigation. IEEE Transactions on Dependable and Secure Computing. 2024. Vol. 21. No. 2. Pp. 1134–1149.

10. Chen, T., Li, Z., Zhang, Y., Zhang, X. EtherScope: A Real-Time Detection System for Malicious Smart Contracts. ACM Transactions on Software Engineering and Methodology. 2023. Vol. 32. No. 3. Pp. 68:1–68:35.

11. Wu, L., Cheng, Y., Wang, D. Real-Time Detection of Flash Loan Attacks in DeFi using Graph Learning. IEEE International Conference on Blockchain. Bali. IEEE. 2023. Pp. 332–339.

12. Gupta, A., Sward, J., Cappos, J. MEV on Layer 2: A Survey of the State of the Art. arXiv preprint. 2024. 18 p.

13. Petrenko, S. A. Voprosy' kiberbezopasnosti. 2022. № 1 (47). pp. 53–63.

14. Positive Technologies. Uyazvimosti i ugrozy' v Web3: Analiticheskij otchet. [Vulnerabilities and threats in Web3: Analytical report]. Moskva Positive Technologies Research. 2024. 46 p.

15. Zhou, Y., Kumar, D., Bakshi, S., Mason, J., Miller, A., Reiter, M. K. An Empirical Study of DeFi Attacks. ACM Conference on Computer and Communications Security (CCS). Copenhagen. ACM. 2023. Pp. 2826–2840.

16. Choi, J., Kim, D., Kim, S. Smart Contract Vulnerability Detection using Graph Neural Networks. IJCAI International Joint Conference on Artificial Intelligence. Macao. IJCAI. 2023. Pp. 354–362.

Автор согласен на обработку и хранение персональных данных.

Дата поступления: 14.11.2025

Дата публикации: 25.12.2025