DOI 10.36622/1682-7813.2025.28.1.001
УДК 349:004.056

МЕТОДИКА ИНФОРМАЦИОННОГО КАРТОГРАФИРОВАНИЯ И АНАЛИЗА РИСКОВ КИБЕРПРЕСТУПНОЙ ДЕЯТЕЛЬНОСТИ, ОСУЩЕСТВЛЯЕМОЙ С ИСПОЛЬЗОВАНИЕМ КРОСЧЕЙН-СЕТЕЙ

А.Л. Сердечный, А.А. Пыхов, А.О. Абрамов, И.Л. Батаронов, В.М. Питолин

Целью работы является разработка инструментов и подходов для анализа кроссчейн-транзакций в блокчейнах Ethereum, Bitcoin и Binance. Основная цель – выявить признаки, которые могут указывать на деятельность маскирующихся киберпреступников в блокчейн сетях. Для этого в исследовании будет использован метод информационного картографирования, который позволяет представить огромные объемы данных о транзакциях в виде наглядных карт. Такие карты помогают специалистам, занимающимся расследованием преступлений в цифровой сфере, находить замаскированные связи и распознавать подозрительные действия. В ходе исследования были изучены особенности работы блокчейнов Ethereum, Bitcoin и Binance. На основе этого анализа был разработан алгоритм, который помогает отображать ключевые элементы их инфраструктуры на информационных картах транзакций. Для реализации этого подхода было использовано специальное программное обеспечение, которое собирает данные о криптокошельках и интегрирует их в общую базу данных. В работе также представлены конкретные шаги для борьбы с преступной деятельностью в блокчейне с использованием кроссчейн сетей. Полученные результаты показывают, что предложенный подход позволяет эффективно выявлять киберпреступные кроссчейн-транзакции. Благодаря этой методике можно распознавать и предотвращать возможные киберпреступные дейтсвия с использованием кроссчейн сетей. Такие инструменты будут полезны для разработки средств противодействия преступных действий в отношении криптовалютных бирж, финансовых организаций и государственных структур, в цифровой среде.

Ключевые слова: Ethereum, Bitcoin, Binance, кроссчейн-сеть, кроссчейн-транзакции, картографирование, киберпреступники.

Введение

В реалиях активного развития цифровых технологий важную роль играет борьба с киберпреступностью, которая используют передовые технологии маскировки своих незаконных действий. Технология Blockchain, лежащая в основе децентрализованных систем, позволяет скрытно совершать финансовые операции, что способствует широкому распространению таких преступлений, как мошенничество, отмывание денег, финансирование терроризма и незаконная торговля.

В зоне особого внимания киберпреступников находятся кросчейн-сети, которые дают возможность взаимодействия между различными блокчейнами и значительно усложняют процесс расследования киберпреступлений.

Кроссчейн-транзакции позволяют киберпреступникам скрывать свои действия, используя сложные схемы перевода активов между различными сетями, что требует применения инновационных методов и технологий для их выявления.

Метод информационного картографирования даёт возможность визуализировать сложные транзакционные цепочки, выделяя скрытые взаимосвязи, а также помогая при анализе выявлять незаконную деятельность.

Представленный труд посвящен разработке методических и инструментальных средств анализа рисков, связанных с использованием кросчейн-сетей для киберпреступной деятельности. Логически он продолжает исследования, направленные на противодействие киберпреступной деятельности посредством анализа криптовалютных кроссчейн-транзакций. Разработанные ранее подходы информационного картографирования блокчейн-транзакций, успешно применённые на данных Bitcoin и Ethereum, показали свою эффективность в рамках изучения структур и

схем, используемых преступниками. В данном исследовании методика информационного картографирования значительно расширена и адаптирована для анализа кросчейн-сетей, включая Binance Smart Chain.

Данные сети играют ключевую роль в формировании кросчейн-транзакций, которые активно используются как легальными участниками цифрового рынка, так и киберпреступниками. Взаимодействие между различными блокчейнами вызывает сложность для анализа, создавая серьезные проблемы у специалистов в области информационной безопасности. Популярность кросчейн-сетей повышается благодаря высокой скорости транзакций, низким комиссиям и возможности перемещения активов между блокчейнами, а это делает их особенно привлекательными для массовых пользователей. И эти же особенности влияют на то, что кросчейн-сети становятся привлекательным инструментом для осуществления и сокрытия киберпреступной деятельности.

Таким образом, исследование рисков использования кросчейн-сетей в киберпреступных целях приобретает особую актуальность. Для оценки данных рисков необходимо понимание сути процессов, происходящих в блокчейнах Bitcoin, Ethereum и Binance Smart Chain, а также разработка эффективных методик обработки большого количества данных о транзакциях, которые ежедневно исчисляются сотнями тысяч. Основным методом исследования, использованным в данной работе, является метод информационного картографирования, который зарекомендовал себя при анализе криптовалютных транзакций, а также позволил выявить аномалии и рисковые схемы в экосистемах цифровых активов [1].

Настоящее исследование представляет собой результаты разработки методических и инструментальных средств анализа транзакций в кросчейн-сетях. Эти средства направлены на значительное повышение эффективности противодействия киберпреступной деятельности, включая выявление киберпреступных действий.

Таким образом, основная **цель** исследования заключается в противодействии киберпреступности за счет анализа киберпреступных транзакций в блокчейн-системах, с использованием методов информационного картографирования для оценки и регулирования рисков киберпреступных действий, совершаемых с помошью кроссчейн сетей.

Для достижения указанной цели решены следующие **задачи**:

- осуществлен сбор данных из открытых интернет-источников, а также суммаризация сведений, касающихся кроссчейн-транзакций, совершаемых киберпреступниками в отношении защищаемых распределённых компьютерных систем;

- выполнена кластеризация и разметка собранного и суммаризированного набора данных с использованием метода информационного картографирования для идентификации транзакций, относящихся к киберпреступной деятельности;

- создан алгоритм исследования информационной карты транзакций блокчейн сетей.

- сформированы политики и регламенты реагирования, направленные на предотвращение и ликвидацию последствий множественных киберпреступных транзакций, обнаруженных в транзитных узлах распределённых компьютерных систем.

Существующие исследования, посвящённые методам укладки и визуализации графов транзакций в Blockchain-сетях, схожи с предложенным подходом. Однако в них построенные графы, как правило, не рассматриваются как полноценные информационные карты, пригодные для анализа рисков кроссчейн транзакций, а применены на конкретные блокчейн сети. Авторы данных исследований используют стандартные функции визуализации графов, предусмотренные популярными инструментами [2,3].

В рамках данного исследования разработаны и применены методы информационного картографирования для анализа транзакций в кроссчейн-сетях (Bitcoin, Ethereum, Binance Smart Chain). Использование этих методов позволяет моделировать и визуализировать пространственное расположение, взаимосвязи и особенности транзакционных процессов в данных экосистемах.

Разработанные подходы, облегчают выявление схем и инструментов, используемых киберпреступниками, и повышают эффективность противодействия их деятельности в

рамках защищаемых распределённых компьютерных систем.

Ключевые механизмы использования кроссчейн технологии киберпреступниками в блокчейнах Ethereum, Bitcoin, Binance

В 2015 году была представлена первая версия Ethereum, которая стала новинкой в сфере блокчейна. В 2016 произошло резонансное событие, связанное со взломом системы, созданной на базе Ethereum, что привело к раздвоению на: Ethereum и Ethereum Classic. Но не смотря на данный инцидент платформа Ethereum продолжила свою работу. Платформа систематически совершенствовалась вплоть до значимого перехода к системе Proof of Stake в 2022 году. Данное изменение повлекло за собой значительное улучшение в сфере безопасности блокчейнов. По состоянию на декабрь 2024 года Ethereum является одним из лидеров среди всех блокчейнов, применяемых для проведения децентрализованных транзакций. Ethereium представляет собой систему, которая отслеживает изменение состояний. Такой метод даёт входные данные и на основе этих данных переходит в совершенно иное состояние. В Ethereum всё начинается с того, что начальное состояние называется «первоначальным». Это положение можно назвать изначальной точкой, когда ещё ничего не произошло в системе. Когда поступающие транзакции начинают поступать и формироваться, система переходит из изначальной точки в текущее. При каждом последующем изменении система отображает все произошедшие с ней действия [4]. Общая схема работы сети изображена на рис.1

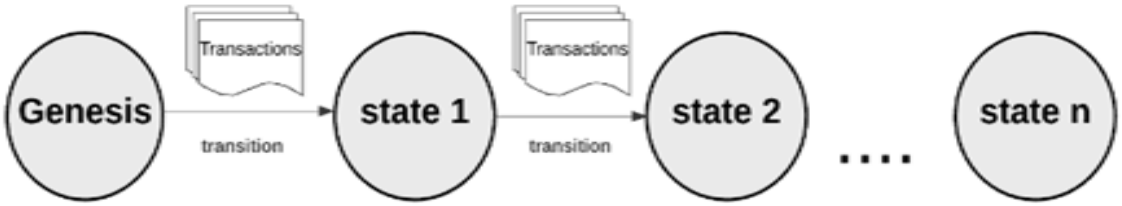

Рис. 1. Структура блокчейна ETHEREUM

Каждое состояние состоит из множества операций, которые, в свою очередь, формируют блоки. Каждый блок вбирает в себя транзакции и также связывается для проверки и уточнений с предыдущим блоком. Этот метод отображает порядок всех действий и демонстрирует единую структуру, которую формируют блоки. Эта структура и обеспечивает целостность и последовательность данных в сети. Кроссчейн-транзакции в Ethereum представляют собой процесс обмена данными или активами между Ethereum и другими блокчейнами, позволяют пользователям использовать свои активы в различных сетях, повышая их ликвидность и функциональность. Работа кроссчейн-транзакций основывается на нескольких ключевых механизмах:

Главный принцип работы кроссчейн-транзакций следующий:

- блокировка средств: Средства замораживаются в исходной сети (Ethereum),

- выпуск эквивалента: В целевой сети создаётся токенизированная версия этих средств,

- обратный процесс: при необходимости актив можно «развернуть» обратно в исходной сети.

Binance — это одна из крупнейших криптовалютных платформ, которая предоставляет множество услуг пользователям по всему миру. Она стала одним из центральных игроков в криптовалютной индустрии, благодаря своей платформе для торговли, а также целой экосистеме сервисов и продуктов, охватывающих разные аспекты работы с криптовалютами (рис.2).

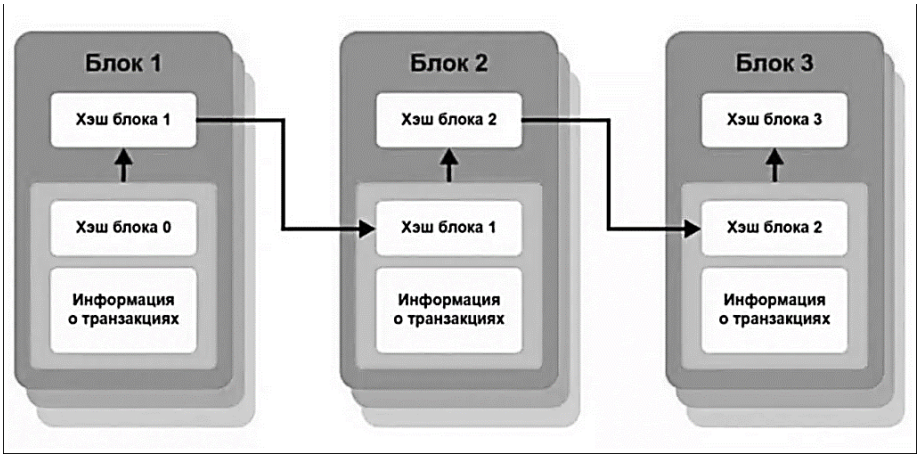

Рис. 2. Структура блокчейна BITCOIN

Bitcoin модель данных немного другая. Если в etherium в транзакции фигурирует два кошелька (From, To) и смакрт-контракт (программа-которая регулирует совершение транзакции), то в bitcoin на вход (in) транзакции одновременно может подаваться несколько кошельков, также, как и на выходе (out) быть тоже несколько. Адресация показана на рис.3.

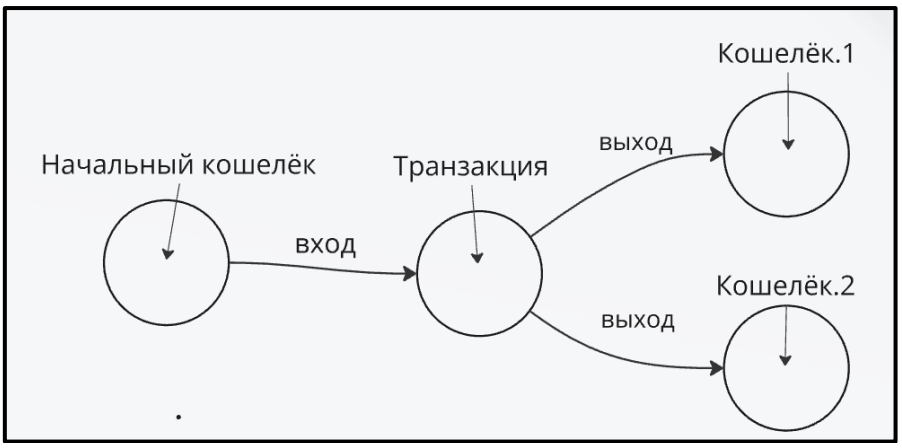

Рис. 3. Адресация в BITCOIN

Особенность адресов в Binance Smart Chain заключается в их использовании в кроссчейн-транзакциях. Например, если пользователь хочет перевести активы из Binance Smart Chain в Ethereum, создаётся получателя в другой, создавая уникальные связи для каждой транзакции [5-8].

Особенности использования кроссчейн-транзакций в технологии Blockchain киберпреступным сообществом

В рамках исследования [9] было рассмотрено руководство по межсетевой блокчейн безопасности, с использованием кроссчейна. Однако в работе были просто описаны свойства кроссчейн-транзакций и признаков, которые помогают их выявлять. Авторы статьи теоретически обосновали эффективность предложенных методов по поиску подозрительных кроссчейн транзакций и без конкретных действий по устранению проблем с подозрительными транзакциями.

В рамках исследования [6] был применён способ для анализа киберпреступных с блокчейн сетью Bitcoin. В работе была проведена разработка, а также использование средства сбора данных по транзакциям с помощью открытого API и его применения для постройки графа за конкретный рассматриваемый период. В отличии от рассмотренного аналога уникальностью настоящего исследования является общий сбор данных с использованием

нескольких блокчейн сетей. Построение информационных карт для поиска киберпреступных кластеров, участники которого действовали в одинаковый период времени, а также поиск и обнаружения связей на основе общих признаков, показывающих структурно схожие подходы к применению кроссчейна для отмывки и маскировки похищенных средств.

В исследовании [10-13] приводится множество стратегий, которые киберпресутпники могут применять в ходе сокрытия и запутывания своих действий с целью вывода денежных средств с криптобирж, а также сравнивают эффективность и методы применяемых технологий для выявления киберпреступников, ключевым аспектом выделяют отсутствие регулирование децентрализованных систем на законодательном уровне. Это исследование показало эффективный анализ существующих методов поиска и выявления киберпреступников, но не использует конкретики действий злоумышленников и недостаточно использует картографические методы. А также не делает акцент на специфике кроссчейн трназакций.

Анализ с использованием информационной карты включает в себя несколько ключевых этапов после выполнения которых можно исследовать полученный объём данных. Для начала собираются данные о транзакциях и взаимодействиях. Это можно сделать через открытые блокчейновые API, которые есть у таких блокчейн сетей как Ethereum или Binance. После строится граф сети, который отражает структуру взаимодействий. С помощью инструментов информационной карты можно вычислить метрики, такие как центральность узлов, которые покажут через какие узлы совершалось наибольшее количество транзакций. В настоящем исследовании это поможет понять, какие узлы являются наиболее привлекательными для киберпреступников и где могут возникнуть риски. Применение информационной карты, также помогает выявлять потенциальные уязвимости. Например, анализ может показать, что большая часть транзакций в сети зависит от одной или нескольких бирж участвующих в системы, что в свою очередь может привести к уязвимости выхода из строя данных адресов, и в свою очередь приведёт к неминуемому уменьшенью потоков транзакций.

Такой подход помогает в исследовании взаимодействий и поиску возможных рисков использования определённых мостов или бирж, а также строить надёжные системы взаимодействия с блокчейнами.

Подобный метод анализа был использован в статье [6], где основной упор был сделан на использование услуг миксера, зачастую связанных с незаконной деятельностью. Где с помощью информационного картографирования определялось ядро миксера, который состоит из большого количества кошельков. Информационная карта являлась ключевым аспектом в работе и позволял выявлять и оценивать риск, что в свою очередь позволяет разработать стратегии по защите и снижению потенциального ущерба.

Разработка и применение алгоритма сбора и интеграции сведений о киберпреступных транзакциях в кроссчейн сетях

В процессе сбора информации о транзакциях можно воспользоваться различными ресурсами, такими как базы данных, веб-сайты или файлы, с утечками, которые постоянно публикуются на закрытых форумах. Для сбора данных доступны разнообразные инструменты. Например, есть созданные специально парсеры для извлечения нужной информации из выбранных источников на основе открытых данных. А также для применения извлечения данных с веб ресурсов есть специализированные приложения API, которые предоставляются самими сайтами и могут быть использованы ПО для извлечения данных из нужных ресурсов.

В данной выпускной квалификационной работе будет применён технический инструмент, созданный с использованием языка Python. Этот инструмент используется для автоматического сбора и анализа данных, доступных на веб-ресурсах для разных блокчейн-сетей, с целью формирования обширной базы информации о сделках, блоках транзакций и кошельках пользователей сети. В начале данная программа, написанная на Python, применяет библиотеку requests для отправки запроса на веб-сайт. Затем, она автоматически извлекает необходимую инфор-

мацию с этого сайта для дальнейшего использования. Далее, на этапе загрузки данных в базу данных Neo4j, программа использует библиотеку neo4j для записи данных в указанную базу данных Neo4j. Пример данных с сайта etherscan.io изображен на рис. 4. Данный сайт позволяет получить детальную информацию по транзакциям, связанным с ним.

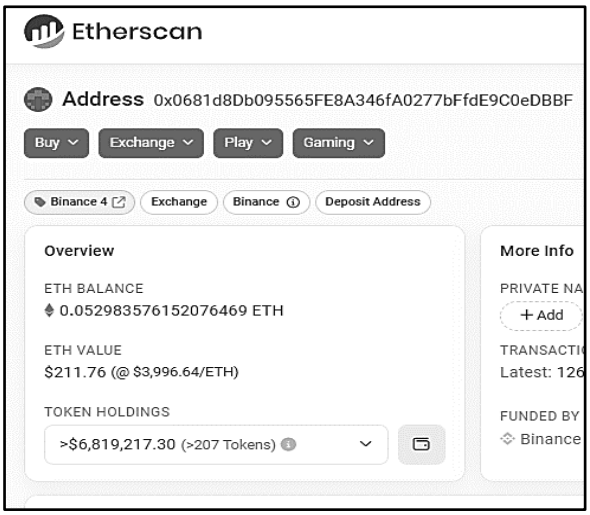

Рис. 4. Данные по кошельку

Интеграция полученных данных с выбранного веб-ресурса позволяет загрузить их для построения и проведения интерактивного анализа карт. Далее, полученная информация о транзакциях переносится в графовую базу данных Neo4j для анализа и визуализации данных. На этапе загрузки данных в базу данных Neo4j, программа использует библиотеку для записи данных в указанную базу данных. Пример запроса и графовое представление показано на рис. 5 и 6.

```
1  match (a:Eth_Addr)-[n]→(b:Eth_Addr)
2  return distinct a.hash as Source, b.hash as Target
3
```

Рис. 5. Запрос для формирования таблицы данных

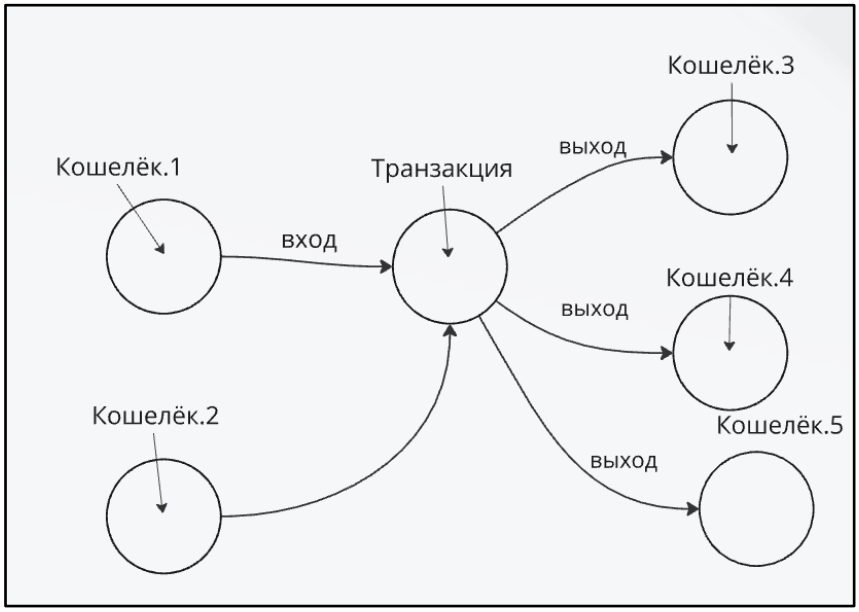

Рис. 6. Пример графа связей

После сформированных запросов и записи данных необходимо с помощью запроса сформировать таблицу для выгрузки данных из Neo4j и их графического представления. Neo4j формирует файл CSV (рис. 7), содержащий узлы и отношения, что позволяет визуализировать граф транзакций с помощью программного средства визуализации графов Gephi. Source - отправитель, target – получатель.

Source	Target
0x9aa99c23f67c81701c772b106b4f83f6e858dd2e	0xc5102fe9359fd9a28f877a67e36b0f050d81a3cc
0x4fb8bbbdc0da1b607ceb337bb70dd33a97f65aca	0xc5102fe9359fd9a28f877a67e36b0f050d81a3cc
0x659f7f3b6bb9f2cd8665b387a0ca6296d2ede467	0x46a8dbd372c288ab2b3526111ca70d79d4ba5c56

Рис.7. Пример файла csv, содержащий узлы и отношения

Современные методы анализа и обнаружения киберпреступных транзакций в кроссчейн-сетях используют различные подходы, статистический анализ и блокчейн-аналитические инструменты. В данном разделе будет предложен алгоритм, направленный на выявление киберпреступных транзакций с использованием кроссчейн-сетей. Для наглядности методика будет разбита на этапы.

На первом этапе определяется исходное множество транзакций и формируется база данных (рис. 8). Использование утечки базы данных форума по продаже и обмену утечек данных, включая перечень транзакций, которыми пользователи, используя внутреннюю валюту оплачивали услуги на покупку утечек (утечка данных с которого датируется началом 2023 и охватывает транзакции с весны 2022-го по дату утечки). Breach Forum связан с киберпреступностью по многим признакам. Многие форумы выкладывают украденные данные пользователей и их транзакций. Это могут быть инструкции по взлому, вредоносное ПО, украденные данные, поддельные документы или способы обхода систем безопасности. На платформе могут предлагаться киберпреступные услуги такие как DDoS-атаки, взломы, торговля эксплойтами и хакерскими инструментами. Оплата чаще всего принимается в криптовалюте, чтобы сохранить анонимность. Такие форумы часто функционируют в Darknet через Tor и используют сложные методы шифрования, чтобы скрыть свою активность от правоохранительных органов. Breach Forum постоянно упоминаются в отчетах правоохранительных органов или компаний по кибербезопасности как платформа, где обсуждаются или ко-координируются нелегальные действия.

	A	B	C	D	E	F
1	crypto_ty	status	object_ty	market	address_t	address
2	btc	COMPLETI	god	coinbase	ethereum	0xa7a4e0ca
3	btc	COMPLETI	god	coinbase	usdc	0xa7a4e0ca
4	btc	COMPLETI	god	coinbase	dai	0xa7a4e0ca
5	btc	COMPLETI	god	coinbase	bitcoincas	qpput2fnn
6	btc	COMPLETI	god	coinbase	dogecoin	DUNvKsaqi

Рис.8. Сформированная база данных

С помощью средства сбора в СУБД NEO4J были загружены данные о транзакциях блокчейнов BITCOIN, ETHEREUM BINANCE. Для визуализации полученных данных было использовано программное обеспечение Gephi. Gephi — это программное обеспечение с открытым исходным кодом для визуализации и анализа сложных сетей. Оно предоставляет мощные инструменты для исследования взаимосвязей в данные и создания красочных и информативных графиков.

После загрузки CSV файла необходимо сделать силовую укладку графа (рис. 9).

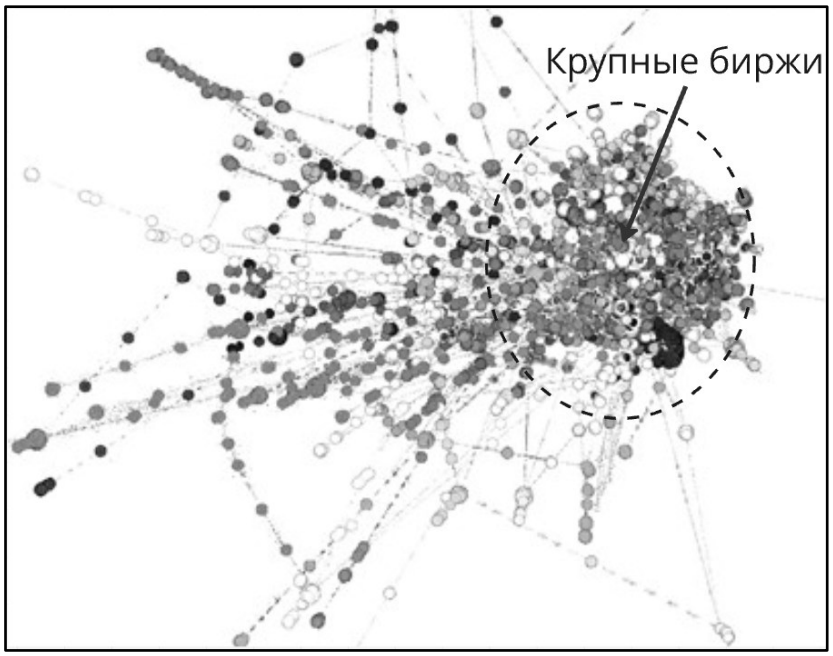

Рис. 9. Граф транзакций

Для этого был использован алгоритм ForceAtlas2. Алгоритм ForceAtlas — это метод визуализации сетевых структур, который имитирует систему для пространственной визуализации. Подобранные силы отталкивания и притяжения между узлами сети позволяют добиться равномерного распределения вершин, предотвращая слишком близкое расположение и подчеркивая взаимосвязи. Для построения и анализа графа было собрано более 2000000 транзакций по каждому из блокчейнов. Далее используем PageRank для задания размеров узлов, а также проведем кластеризацию графа с помощью алгоритма Leiden для покраски кластеров.

На следующем этапе проводится отделение потенциальных киберпреступников от обычных пользователей или представителей спецслужб. Необходимо определить подозрительные группы на основе структурных характеристик и совпадений с адресами из утечки и провести картографический анализ для выявления аномальных взаимодействий.

На рис. 10 представлен граф Bitcoin-транзакций со сформированными связями, а на рис. 11 – граф Ethereum-транзакций.

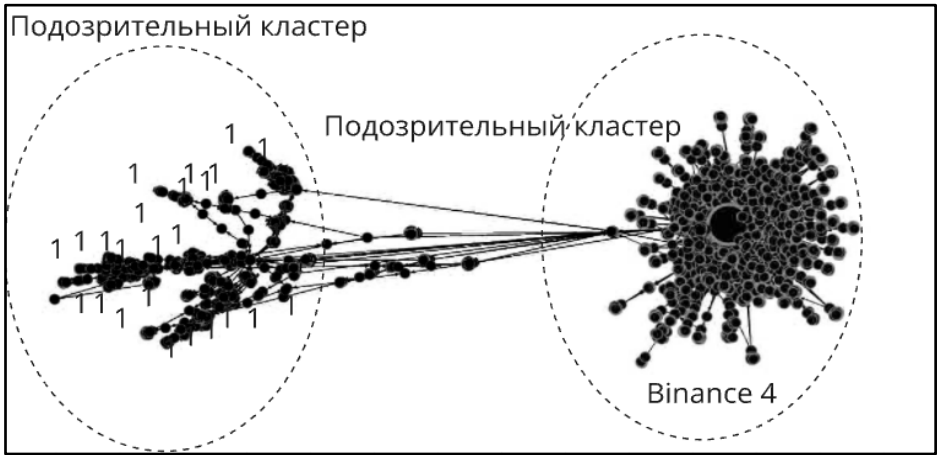

Рис. 10. Граф Bitcoin-транзакций, соединённый с транзакциями из утечки (отмеченные 1)

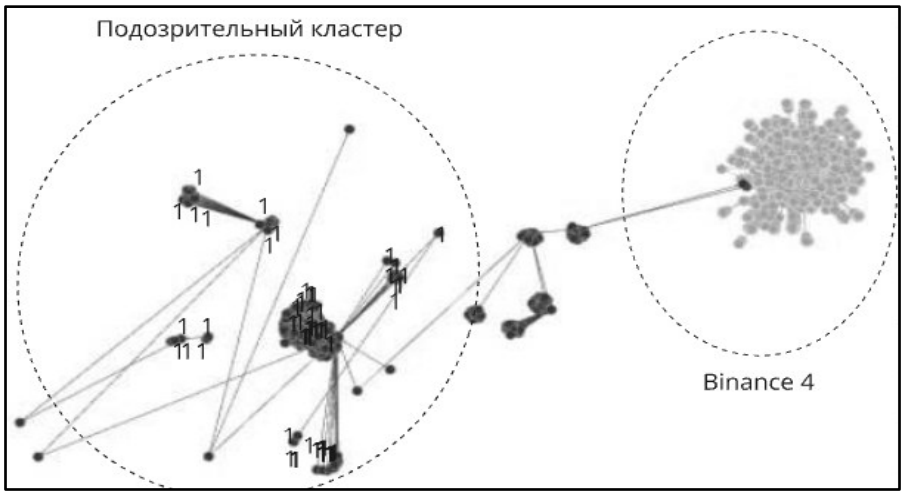

Рис. 11. Граф Ethereum-транзакций, соединённый с транзакциями из утечки (отмеченные 1)

Был произведен анализ данных, выделены кластеры, связанные с кошельками из утечки. Кластеры со множеством совпадений с базой данных утечки были помечены для проверки в других блокчейнах. Эти кластеры выглядели структурно похожими. Несоответствующие критериям кластеры были отфильтрованы. Период транзакций подозрительного кластера Bitcoin совпадает с периодом подозрительного кластера Ethereum и периодом утечки (рис. 12,13). Оба кластера выводили деньги через биржу Binance. Что ещё больше подтверждает факт кроссчейна.

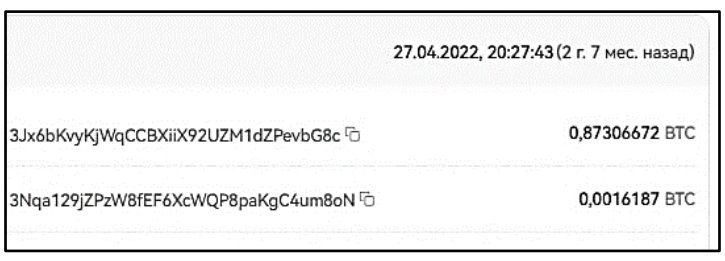

Рис. 12. Пример транзакций за 04.2022 подозрительного кластера ETH

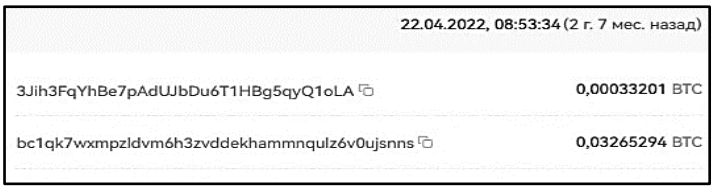

Рис. 13. Пример транзакций за 04.2022 подозрительного кластера Bitcoin

Период транзакций подозрительного кластера Bitcoin совпадал с периодом подозрительного кластера Ethereum. Оба кластера выводили деньги через биржу Binance. Что ещё больше подтверждает факт кроссчейна. Провели картографический анализ, определили кластеры, в которых превалируют кошельки с киберпреступного форума, посмотрели связи этого кластера с криптобиржами (проанализировав ландшафт информационной карты). Установили, что такой биржей, которой часто пользуются потенциальные киберпреступники являются Binance 4.

Если это киберпреступное сообщество, то оно все равно будет иметь некий кластер, где их транзакции используются для какой-либо деятельности. Чтобы выявить подобные кластеры мы и использовали помеченные кошельки, а вот далее среди полученного многообразия кошельков надо найти именно те, которые относятся к потенциальному кроссчейну. Очень похоже, что "Binance 4" в разных блокчейнах и выступает в роли подобного показан на рис. 14.

Рис. 14. Адрес биржи Binance 4 в Bitcoin

На заключительном этапе были выделены наиболее подозрительные адреса и транзакции, связанные с киберпреступными группировками (рис. 15).

	A	B	C	D	E	F	G	H	I
1	3KUv8T2dAGnigXDM2AxEiqVuQY7c39hr9a			0	1	1	1	2.343263311693 89E-5	8
2	3BS56doHnk2MktmgmT25JWVfE61ziFYdFQ			0	1	1	1	2.386161 4258433 842E-5	8
3	3CAZU81qoiudYE68wj18BT7W2aqQqwsg4J			0	1	1	1	1.791634 1008320 617E-5	8
4	3HKoG6LpU5pLB9FoK4LPvPbgwgG6mVQ4vY			0	1	1	1	2.585149 8434423 374E-5	8
5	3HFd2Z3sXNU91XntrhLAHhYrYYsrC4acTc			0	1	1	1	2.585149 8434423 374E-5	8
	3MjPHzgJJQeTBAK							2.513991	

Рис.15. Наиболее подозрительные адреса с суммами Bitcoin

А также после можно сформировать список с связями и суммами транзакций (табл.1).

Таблица 1

Связи и суммы транзакций

Отправитель	Получатель	Сумма транзакции
3BvQKsYBunF5sW7jZauzPKgVUJuW4BAdH1	33jogRsPVU8iTfdA9qCfnFn7CQ2dihProT	74087
147xtgfahTgMfiVuYzNXLoHLwwNUWmwK1E	37mkhX4UXzvkrGop22vvHVzA8MAKETEHJ1	75013
14RESEXqwPBA3zUypvR9MFj5NeSixWcyAx	3QEBt5UeLidRRnyQyLXWgKDxjZ9KXfuS8N	76278

Для подведения итогов данной методики можно кратко описать её.

– за основу взяты криптокошельки, связанные с операциями на киберпреступном форуме (Утечка данных с которого датируется началом 2023 и охватывает транзакции с весны 2022-го по дату утечки)

– собраны 2 уровня связей этих кошельков с другими по транзакциям, чтобы охватить как киберпреступные кластеры, так и

контекст (крупные криптобиржи) в котором они совершали сделки.

– для того, чтобы отобрать киберпреступные (т.к. в собранных данных могут содержаться и кошельки как обычных пользователей, так и представителей спецслужб) провели картографический анализ, определили кластеры, в которых превалируют кошельки с киберпреступного форума, посмотрели связи этого кластера с криптобиржами (проанализировав ландшафт информационной карты). Установили, что такой биржей-кроссчейном, которой часто пользуются киберпреступники являются Binance 4.

– среди нескольких киберпреступных кластеров (где превалируют помеченные кошельки) выбрали те, транзакции которых для Bitcoin, Etherium и BNB соответствуют периоду утечки и крайняя дата - начало 2023

В процессе анализа данных был использован предложенный метод, основанный на картографическом анализе. Этот метод помогает в более детальном изучении перемещения денежных средств и выявлении подозрительной активности, связанные с кроссчейн-транзакциями. В ходе работы удалось собрать и систематизировать обширную базу данных, которая содержит информацию о киберпреступных операциях с использованием кроссчейн сетей.

Особое внимание было уделено транзакциям, которые проходили через так называемые кроссчейн-мосты. Эти узлы представляли собой основные точки, через которые организаторы мошеннических схем направляли денежные потоки для сокрытия следов операций и затруднения их обнаружения. Использование картографического анализа дало возможность визуализировать маршруты подозрительных транзакций и выявить закономерности, которые повторяются в других блокчейн системах.

Результатом работы стало создание детализированной базы данных, включающей характеристики транзакций, таких как проведения операций, суммы, задействованные узлы. Эта база данных стала ключевым инструментом для дальнейшего расследования и разработки методов противодействия подобным преступлениям.

Рекомендации по защите от деятельности киберпреступников, использующих кроссчейн в блокчейн системах

Для противодействия киберпреступным группировкам, использующим кроссчейн-транзакции в блокчейн системах, предлагаются следующие меры защиты:

- обеспечить максимальную защиту активов. Для хранения большого количества активов можно использовать аппаратные кошельки. Их преимущество в изоляции ключей от доступа из интернета, что делает их практически недоступными для киберпреступников.

- использовать инструменты автоматизированного анализа блокчейнов, такие как Chainalysis или Elliptic. Эти сервисы помогают обнаруживать аномальные действия, например, внезапные крупные или автоматизированные переводы с использованием кроссчсейна.

- использовать мультиподпись — это механизм, который требует подтверждения транзакции от нескольких участников. Даже если один из ключей будет украден киберпреступником, он не сможет завершить перевод без подтверждения оставшихся участников транзакции.

- защита от отмывания средств через мосты, можно использовать технологии KYC (знай своего клиента) и AML (противодействие отмыванию денег).

- использование сервисов и инструментов, аналогичных описанным в исследовании, позволяет эффективно проводить расследования преступлений.

- разработанный алгоритм является одним из ключевых инструментов для улучшения анализа и управления рисками, связанных с деятельностью киберпреступников, использующих кроссчейн технологии в блокчейн-системах.

Эти инструменты особенно важны в контексте защиты блокчейн-систем. С помощью вышеуказанных мер можно сформировать таблицы защитных мер для федерального (рис. 16-18) и регионального уровней.

Законодательное регулирование и стандарты.		
Принятие законов о киберпреступлениях в блокчейн-среде	**Требования к прозрачности и мониторингу**	**Введение стандартов безопасности**
Введение строгих норм, регулирующих кроссчейн транзакции, с обязательной идентификацией участников.	Законы должны обязать операторов кроссчейн сетей предоставлять отчёты о подозрительных транзакциях в соответствующие органы.	Установление минимальных требований к шифрованию, проверке данных и авторизации транзакций между сетями.

Рис.16. Меры защиты для федерального уровня

Централизованное управление рисками	
Создание центра по мониторингу кроссчейн транзакций	**Обмен данными между федеральными агентствами**
отслеживать крупные объемы данных и выявлять подозрительные модели поведения.	Координация между финансовыми институтами и органами кибербезопасности для обмена информацией о подозрительных транзакциях.

Рис.17. Меры защиты для федерального уровня

Технологические меры	
Разработка государственной инфраструктуры для кроссчейн сетей	**Универсальная платформа проверки данных**
Внедрение государственных сетей с встроенными механизмами безопасности.	Создание платформы для проверки идентификаторов и источников транзакций.

Рис.18. Меры защиты для федерального уровня

На региональном уровне меры защиты можно сосредоточить на конкретных организациях, инфраструктуре. более адаптированные технологии и процессы (рис. 19,20)

Региональные центры кибербезопасности	
Локальные центры анализа транзакций	**Партнёрство с региональными предприятиями**
Создание центров мониторинга киберугроз для обработки транзакций, характерных для определённых регионов.	Установление связей с финансовыми институтами, банками и криптобиржами для выявления киберпреступных транзакций

Рис.19. Меры защиты для федерального уровня

Локальные технологические меры	
Мониторинг и аудит	**Локальная идентификация подозрительных пользователей**
Регулярная проверка локальных платформ на соответствие федеральным стандартам.	Использование региональных инструментов анализа для определения аномального поведения в рамках региона

Рис.20. Меры защиты для федерального уровня

Меры на федеральном уровне создают инфраструктуру, стандарты и законы для противодействия киберпреступности в блокчейне. Региональные меры адаптированы к особенностям именно локальных инфраструктур, что позволяет своевременно реагировать на угрозы. Предложенная в настоящем исследовании методика и двухуровневый подход способен повысить безопасность транзакций в кроссчейн сетях и минимизировать риск множественных киберпреступных действий.

В исследовании были предложены меры, которые способны в той или иной мере привести к снижению рисков реализации киберпреступных транзакций в защищаемых распределенных компьютерных системах. Но в силу того, что данные контрмеры напрямую подобраны под блокчейн транзакции, то они определенно должны оказать хотя бы минимальное положительное воздействие и привести к снижению величин рисков.

Заключение

В ходе исследования были определены возможные механизмы использования кроссчейн сетей в экосистеме блокчейнов, которые позволяют киберпреступникам маскировать цепочку своих транзакций

Представлены результаты методики по сбору и интеграции сведений о криптовалютных транзакциях блокчейна для системы информационного картографирования. С помощью данного средства выявлены структурные особенности основных компонентов экосистем, проявляемые на информационной карте (кластеры и кошельки, которые массово используются для переноса между блокчейн системами).

Разработанная методика представляет собой важный инструмент для улучшения процессов анализа и управления рисками в сфере Blockchain, которая способствует более глубокому и всестороннему пониманию динамики в контексте кроссчейн операций в данной области. Результаты проведенной работы показывают эффективность используемой методики.

Таким образом, проведенные исследования и разработанные методы представляют важный вклад в область кибербезопасности, предостерегая от возможных угроз и обеспечивая более эффективные меры защиты информации от киберпреступников.

Список литературы

1. Сердечный А.Л. Картографическое исследование blockchain-транзакций и смарт-контрактов киберпреступников, атакующих автоматизированные информационные системы, и оценка ущербов от реализации их атак / А.Л. Сердечный, Д.А. Скогорева, Е.П. Длинный, Т.Ч. Ле, Д.В. Чьеу // Информация и безопасность. 2021. Т. 24. Вып. 4. С. 471-500.

2. Остапенко А.Г. Картография защищаемого киберпространства / А.Г. Остапенко, А.Л. Сердечный, А.О. Калашников и др; Под ред. Академика РАН Д.А. Новикова М: Горячая линия – Телеком, 2023. 228с.:

3. Сердечный А.Л. Информационное картографирование Blockchain-транзакций киберпреступников в экосистеме TON / А.Л. Сердечный, А.О. Абрамов, Е.А. Москалева // Информация и безопасность. 2024. Т. 27. Вып. 2. - С. 257-272.

4. What are ETH Internal Transactions? / URL: https://www.geeksforgeeks.org/what-are-eth-internal-transactions/ (дата обращения: 13.04.2024)

5. Мир BNB: Инструкция по безопасной эксплуатации, или как правильно торговать на криптовалютном рынке / А. Криптонов. 2024. 193 с.

6. Chainalysis 2024 Crypto Crime Report Introduction. – Электрон. дан. – Режим доступа: https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/ (дата обращения: 28.12.2024).

7. PeckShield CoinHolmes. / URL: https://peckshield.com/#products_coinholmes (дата обращения: 28.12.2024).

8. Crypto Investment Scams. / URL: https://www.fool.com/research/crypto-investment-scams/ (дата обращения: 28.12.2024).

9. Chainalysis – Криптопреступность 2022. Часть 1 // Системы Информационной Безопасности / URL: https://is-systems.org/blog_article/11647251410 (дата обращения: 13.04.2024).

10. Zhao C. A graph-based investigation of bitcoin transactions / Y. Guan, C. Zhao // IFIP Advances in Information and Communication Technology. 2015. V. 462. P. 79-95.

11. Абрамов А.О. Киберполигон: программно-технические модули информационного картографирования для исследования Blockchain-транзакций и смарт-контрактов кибер-преступников, использующих криптовалюту TON. 2024. С. 102.

12. Остапенко А.Г. Картография защищаемого киберпространства / А.Г. Остапенко, А.Л. Сердечный, А.О. Калашников; [Под ред. чл.-корр. РАН Д.А. Новикова.Сер. Теория сетевых войн; Вып. 7.

13. Абрамов А.О. Средство сбора и интеграции сведений криптовалюты TON для системы картографирования рисков в области защиты информации / А.О. Абрамов, А.Л. Сердечный // Свидетельство регистрации на программное средство: № RU 2024611059 от 29.12.2023. Дата публикации: 17.01.2024. Язык программирования: Python. Объем: 4096 Б.

14. Сердечный А.Л. Информационно-картографические системы как инструментальная основа картографии защищаемого киберпространства // Системы управления и информационные технологии. 2021. № 4 (86). С. 41-46.

Государственный научно-исследовательский испытательный институт проблем технической защиты информации ФСТЭК России
State science research experimental institute of technical information protection problem of Federal service of technical an export control

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 14.01.25

Информация об авторах

Сердечный Алексей Леонидович – канд. техн. наук, зам. начальника отдела, Государственный научно-исследовательский испытательный институт проблем технической защиты информации ФСТЭК России; доцент, Воронежский государственный технический университет, e-mail: alex-voronezh@mail.ru

Пыхов Андрей Андреевич – студент, Воронежский государственный технический университет, e-mail: Andrey.pykhov@mail.ru

Абрамов Артем Олегович – студент, Воронежский государственный технический университет, e-mail: vozgrin96@mail.ru

Батаронов Игорь Леонидович – д-р физ.-мат наук, профессор, заведующий кафедрой высшей математики и физико-математического моделирования, Воронежский государственный технический университет, e-mail: vmfmm@mail.ru

Питолин Владимир Михайлович – д-р техн. наук, профессор, Воронежский государственный технический университет, e-mail: pitol@mail.ru

METHODOLOGY OF INFORMATION MAPPING AND RISK ANALYSIS OF CYBERCRIME ACTIVITIES CARRIED OUT USING CROSS-CHAIN NETWORKS

A.L Serdeshny, A.A Pykhov, A.O. Abramov, I.L. Bataronov, V.M. Pitolin

The aim of the work is to develop tools and approaches for analyzing cross-chain transactions in the blockchains of Ethereum, Bitcoin and Binance. The main goal is to identify signs that may indicate the activities of cybercriminals. For this purpose, the information mapping method is used, which allows you to present huge amounts of transaction data in the form of visual maps. Such cards help specialists involved in the investigation of digital crimes to find hidden connections and identify suspicious transactions. The study examined the features of the Ethereum, Bitcoin and Binance blockchains. Based on this analysis, an algorithm has been developed that helps display key elements of their infrastructure on transaction cards. To implement this approach, special software was used that collects data on crypto wallets and integrates them into a common system. This software not only visualizes the data, but also makes the analysis intuitive, allowing you to quickly find suspicious connections and simplify investigations. The paper also suggests specific steps to combat criminal activity on blockchains. The results show that the developed approach makes it possible to effectively identify fraudulent cross-chain transactions. Thanks to this, it is possible not only to detect, but also to prevent cybercrimes. Such tools will be useful for cryptocurrency exchanges, financial organizations, and government agencies that ensure security in the digital environment.

Keywords: Ethereum, Bitcoin, Binance, cross-chain network, cross-chain transactions, mapping, cybercriminals.

Submitted 14.01.25

Information about the authors

Alexey L. Serdechnyi – Cand. Sc. (Technical), Deputy Head of Department, State science research experimental institute of technical information protection problem of Federal service of technical an export control, Associated Professor, Voronezh State Technical University, e-mail: alex-voronezh@mail.ru

Andrey A. Pykhov – student, Voronezh State Technical University, e-mail: andrey.pykhov@mail.ru

Artem O. Abramov – student, Voronezh State Technical University, e-mail: vozgrin96@mail.ru

Igor L. Bataronov – Dr. Sc. (Phisical and Mathimatical), Professor, Head of Department of Higher Mathematics and Physical and Mathematical Modeling, Voronezh State Technical University, e-mail: vmfmm@mail.ru

Vladimir M. Pitolin – Dr. Sc. (Technical), Professor, Voronezh State Technical University, e-mail: pitol@mail.ru