DOI 10.36622/1682-7813.2024.27.2.011
УДК 004.056

ИНФОРМАЦИОННОЕ КАРТОГРАФИРОВАНИЕ BLOCKCHAIN-ТРАНЗАКЦИЙ КИБЕРПРЕСТУПНИКОВ В ЭКОСИСТЕМЕ TON

А.Л. Сердечный, А.О. Абрамов, Е.А. Москалева

Целью работы является разработка методических и инструментальных средств анализа транзакций в блокчейне TON (The Open Network) для выявления признаков, демаскирующих деятельность киберпреступных сообществ. Для этого в настоящей работе использован метод информационного картографирования, позволяющий представить большой объём данных о транзакциях TON в виде информационной карты, с помощью которой эксперт в области расследования компьютерных преступлений может обнаружить скрытые взаимосвязи, указывающие на наличие киберпреступной деятельности. В рамках проведения исследования рассмотрены структурные особенности инфраструктурных компонентов на базе TON, предложен алгоритм их обнаружения на карте транзакций. Разработано средство сбора и интеграции сведений о крпитокошельках TON, являющееся информационно-картографической системой, которая предоставляет возможности интерактивного анализа карт транзакций и автоматизации расследования компьютерных преступлений. Также в работе предложены меры противодействия такой деятельности. Результаты, полученные в ходе проведенного исследования, позволяют выявить мошеннические транзакции, а разработанная методика – создать эффективные средства для обнаружения и предотвращения киберпреступных действий в сети TON, что может быть полезным для криптовалютных бирж, финансовых организаций и государственных учреждений.

Ключевые слова: информационная картография, TON, Blockchain, смарт-контракты, ущерб.

Введение

Сегодня развитие информационных технологий осуществляется по различным направлениям, в том числе, по направлению борьбы с киберпреступностью. Технология Blockchain является основой децентрализованного устройства системы цифровых денег, которые обеспечивают независимою от традиционных финансовых инструментов деятельность в киберпространстве. Данная технология активно используется различными видами киберпреступников: мошенничествами, кибервымогателями, кибертеррористами. Их деятельность наносит серьёзный ущерб государствам, частным компаниям, некоммерческим организациям и обычным гражданам. С помощью технологии Blockchain преступники анонимно легализуют незаконный доход, продают нелегальные товары и осуществляют поддержку терроризма [1].

Настоящая работа является продолжением исследований, направленных на противодействие киберпреступности за счёт анализа криптовалютных транзакций, проводимых на кафедре систем информационной безопасности Воронежского государственного технического университета [2]. Предложенный в [2] поход информационного картографирования блокчейн-транзакций был применён для анализа инфраструктуры, построенной на базе технологии TON (The Open Network, изначально расшифровывалось как Telegram Open Network [3-5]).

В настоящей работе представлены результаты разработки методических и инструментальных средств анализа транзакций в блокчейне TON, на базе которой в настоящее время сформирована целая экосистема из множества проектов [3].

Экосистема TON активно развивается благодаря усилиям сообщества, организованного разработчиками мессенджера Telegram. Её популярность стремительно растёт в международном масштабе по мере появления новых

функциональных возможностей. Это достигается за счёт архитектуры, обеспечивающей высокую скорость транзакций при достаточно низкой комиссии. Также значительную роль играет глубокая интеграция экосистемы с указанным мессенджером. Однако направленность на массового потребителя, децентрализация и элементы анонимности делает данную экосистему также привлекательной и для киберпреступников.

В связи с изложенным исследование рисков использования криптовалюты TON становится крайне актуальным и важным для обеспечения информационной безопасности. При этом для адекватной оценки рисков требуется понимание процессов, происходящих в экосистеме TON, что сопровождается необходимостью обработки большого объёма сведений, в том числе о транзакциях, приводящихся в рассматриваемом блокчейне [6-11]. Ежедневно количество таких транзакций может достигать сотен тысяч. В связи с этим основным методом исследования был использован метод информационного картографирования, который ранее успешно использовался для решения аналогичных задач в рамках анализа блокчейнов Bitcoin и Etherium [2].

Таким образом, основная **цель** исследования заключается в противодействии злоумышленникам, которые пользуются криптовалютой для финансирования своих действий в киберпространстве, за счет разработки программного средства сбора данных о TON-транзакциях, использования технологии построения, исследования карт криптовалют, а также оценки рисков от деятельности киберпреступников.

Для того, чтобы достичь указанной цели решены следующие **задачи**:

- проанализированы научные работы, касающиеся исследований действий киберпреступников связанных с использованием криптовалют, а также проанализированы риски указанных действий и исследования Blockchain TON, в том числе, с использованием методов информационной картографии;
- разработано средство сбора и интеграции сведений криптовалюты TON для системы картографирования в области защиты информации;
- создан алгоритм исследования информационной карты транзакций блокчейн сети TON;
- выявлены основные структурные особенности экосистемы TON, определено их представление на информационной карте;
- разработаны меры противодействия деятельности киберпреступных сообществ, учитывающие специфику использования ими экосистемы TON.

Существующие исследования [6-11], схожие с нашим подходом, посвящены различным методам укладки и визуализации графа транзакций пользователей в Blockchain-сетях. Однако в этих работах построенный граф не рассматривается как полноценная информационная карта [12]. Авторы используют стандартные функции визуализации графов, предусмотренные программными средствами, но обоснование эффективности и полезности этого метода отсутствует.

При этом ни в одной из работ не применяется технология создания и исследования карты Blockchain-транзакций и смарт-контрактов TON. Эта технология облегчает моделирование и отображение пространственного расположения, сочетания и взаимосвязи объектов и явлений, происходящих в Blockchain.

Для проведения исследований в рамках работ по созданию киберполигона на кафедре систем информационной безопасности Воронежского государственного технического университета было разработано средство сбора и интеграции сведений криптовалюты TON для системы картографирования рисков в области защиты информации [13]. По сравнению с аналогами [14] разработанное средство является информационно-картографической системой [15], которая в полном объёме реализует возможности метода информационного картографирования [12].

Ключевых аспектов технологии TON

Технология TON, или Telegram Open Network [4, 5], была разработана командой

Telegram и впервые представлена в 2017 году как решение для создания децентрализованных приложений и смарт-контрактов. Telegram Open Network представляет собой сложную ногоуровневую систему, включающую различные типы Blockchain, каждый из которых выполняет уникальные функции в рамках общей экосистемы. В центре всей системы находится главный Blockchain (Master Blockchain), который играет ключевую роль в координации и управлении всей сетью TON. Главный Blockchain содержит информацию о состоянии всей системы, включая актуальный реестр валидаторов и конфигурационные данные. Общая схема работы сети изображена на рис. 1.

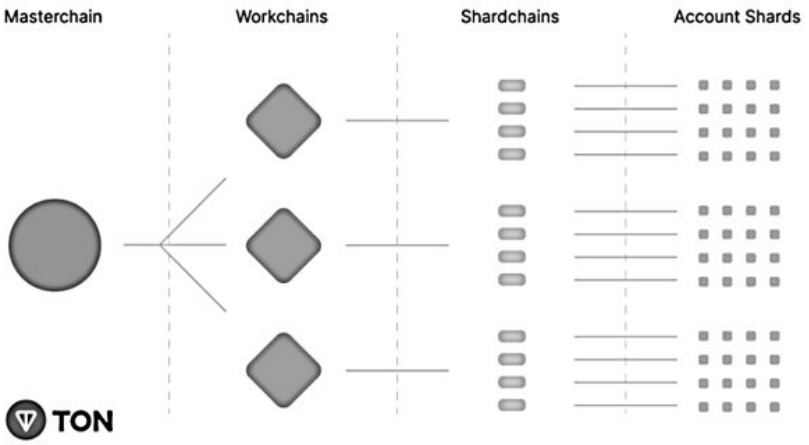

Рис. 1. Структура блокчейна TON

В дополнение к основному Blockchain, в TON имеются рабочие Blockchain (workchains), которые представляют собой самостоятельные Blockchain с уникальными характеристиками и правилами. Эти рабочие Blockchain придают системе гибкость, позволяя обрабатывать различные типы транзакций и поддерживать множество криптовалют и смарт-контрактов.

На сегодняшний день в Blockchain TON работают только главная цепь (masterchain, workchain_id=-1) и, иногда, базовая цепь (basic workchain, workchain_id=0). Оба они имеют 256-битные адреса, поэтому предполагается, что workchain_id равен либо 0, либо -1, а адрес в рабочем Blockchain составляет 256 бит.

Для улучшения масштабируемости и обработки транзакций TON использует технологию шардинга (shardchain), которая включает разделение рабочих Blockchain на более мелкие сегменты, называемые шардами. Этот процесс позволяет параллельно обрабатывать транзакции в разных частях сети, значительно увеличивая пропускную способность и эффективность всей системы. Шардинг обеспечивает высокую скорость транзакций и позволяет сети эффективно масштабироваться в соответствии с растущими требованиями пользователей и приложений. Итак, каждый shardchain отвечает за транзакции тех аккаунтов, которые находятся в shardchain, каждый workchain отвечает за свой shardchain и наконец masterchain за все workchain.

Одной из главных особенностей TON является использование модифицированного алгоритма Proof-of-Stake (PoS) для процесса консенсуса. Это отличает его от более традиционных и энергоемких систем, таких как Proof-of-Work, используемых в других Blockchain. Валидаторы в сети TON играют ключевую роль в поддержании целостности сети, участвуя в создании новых блоков и подтверждении транзакций, при этом система спроектирована так, чтобы минимизировать риски, связанные с двойной тратой и атаками TON использует сложные криптографические алгоритмы для защиты данных и транзакций. Это включает в себя:

- шифрование: все данные в сети TON, включая транзакции и смарт-контракты, зашифрованы, что обеспечивает их

конфиденциальность и защиту от несанкционированного доступа;

- цифровые подписи: каждая транзакция в сети TON подписывается цифровой подписью отправителя, что гарантирует ее подлинность и помогает предотвратить подделку;

- хеширование: использование криптографических хеш-функций для создания уникального отпечатка каждого блока и транзакции, что позволяет легко проверять их целостность и подлинность.

Адресация в TON. Особенности адресации имеют важное значение при проведении информационного картографирования транзакций, так как адреса обеспечивают идентификацию узлов такого графа. Чтобы избежать дублирования узлов и фрагментов такого графа необходимо учитывать различные типы адресов, которые в экосистеме TON применяются на практике. Кроме того, адреса криптокошельков могут содержать дополнительную информацию, которая будет полезной при выявлении роли соответствующего узла в ходе информационно-картографического анализа.

В экосистеме TON используются несколько типов адресов:

- Raw addresses («сырые» адреса);

- User-friendly addresses (упрощённые адреса);

- человекочитаемые адреса.

Raw addresses – стандартные адреса кошельков в Blockchain, представляющие собой длинную последовательность из букв и цифр. Эти адреса генерируются на основе криптографических ключей и обычно очень сложны для восприятия человеком, что приводит к увеличению риска ошибок при ручном вводе.

Raw addresses состоят из ID рабочей цепи (workchain_id) и ID аккаунта (account_id) (пример адреса –1:fcb91a3a3816d0f7b8c2c76108b8a9bc5a6b7a55bd79f8ab101c52db29232260). Все ID аккаунтов в TON состоят из 256-битных адресов в «главной цепи» и «базовой цепи» (Basechain). ID аккаунта (account_id) определяется как хеш-функции для объектов смарт-контрактов (SHA-256).

User-friendly addresses имеют более короткое представление, могут содержать понятные слова или имена, характеризующие какие-либо признаки владельца адреса (например, название децентрализованной торговой площадки EQBYTuYbLf8INxFtD8tQeNk5ZLy-nAX9ahQbG_yl1qQ-**GEMS**). Упрощённый адрес состоит из 36 байт, включающих флаги, ID рабочей цепи и ID аккаунта.

Также в TON имеется возможность использования *человекочитаемого адреса* вида ivan.ton или ivan@crypto, что обеспечивается службой TON DNS, которая реализована на базе смарт-контрактов самого блокчейна. Эти адреса часто используют более привычные форматы, подобные электронной почте или веб-доменам. Они упрощают процесс передачи и запоминания адресов кошельков, делая использование криптовалют более доступным для широкой аудитории. Однако для получения такого адреса требуется внести определённую сумму в криптовалюте TON на специальные кошельки.

Смарт-контракты являются фундаментальной концепцией в блокчейне TON. Каждый кошелек в блокчейне связан с компьютерной программой, которая определяет его работу. Эта программа позволяет автоматизировать проверку выполнения условий соглашений между сторонами, устраняя необходимость в доверии к третьей стороне. Благодаря смарт-контрактам можно создать децентрализованные криптовалютные биржи (DEX), которые автоматически выполняют функции обычных бирж и торговых площадок.

Выполнение смарт-контрактов осуществляется в TVM (TON Virtual Machine. TVM). Виртуальная машина спроектирована так, чтобы обеспечить высокую эффективность и безопасность выполнения контрактов. TVM обеспечивает поддержку всех операций, необходимых для анализа входящих сообщений и постоянных данных, а также для создания новых сообщений и изменения постоянных данных. В настоящее время TVM используется для исполнения кода смарт-контрактов как в главной цепи

(masterchain, -1 workchain), так и в базовой цепи (basechain, 0 workchain). Другие рабочие цепи могут использовать иные виртуальные машины наряду с TVM или вместо нее. Смарт-контракты могут быть написаны языках программирования, таких как Fift и FunC.

Fifth – это специализированный высокоуровневый язык для разработки скриптов, позволяющих выполнять операции по взаимодействию с TON Blockchain. Fift был разработан для повышения читаемости и скорости разработки смарт-контрактов. TVM также предоставляет разнообразные примитивы для работы с базовыми типами данных Blockchain TON, такими как TVM Cells. Более подробная информация о структуре и принципах работы TVM содержится в оригинальном документе [4].

В TON существует своя среда разработки для написания, тестирования и развертывания смарт-контрактов под названием «Blueprint».

Наличие смарт-контрактов даёт исследователю дополнительные средства анализа. В первую очередь – это типизация различных смарт-контрактов по их функциональности. Можно выделить следующие типы TON-кошельков:

- кошельки управления сетью TON, которые связаны с уникальными смарт-контрактами, обеспечивающими работу Blockchain TON, такими как Config Contract, Ector Contract, DNS Contract, а также смарт-контрактами валидаторов, номинаторов и их пулов, и смарт-контрактами для сжигания и блокировки токенов;
- кошельки с базовой функциональностью (связаны со смарт-контрактами, которые реализуют базовые функции, такие как «регистрация смарт-контракта», «изменение смарт-контракта», «выполнение транзакций», «обработка ошибок» и т.п., в блокчейне используются разные версии базовых кошельков, например, Wallet v2, Wallet v3, Wallet v4 и др.);
- кошельки с плагинами (могут управляться из внешних приложений, например, ботов мессенджера Telegram);
- кошельки токенов (смарт-контракты взаимозаменяемых токенов, называемых жетонами – Jetton Wallet, невзаимозаменяемых токенов – NFT Wallet, NFT Collection);
- кошельки децентрализованных бирж и маркетплейсов (смарт-контракты для обмена и перемещения токенов в зависимости от выполнения определённых условий, таких как Swap и Router) и др.

Необходимо отметить, что экосистема TON динамично развивается и периодически появляются новые типы смарт-контрактов, а также изменяются существующие смарт-контракты.

Типы смарт-контрактов играют существенную роль в информационно-картографическом анализе, так как сигнатуры соответствующих кошельков проявляются на информационной карте транзакций в виде особых структур (которые будут подробно рассмотрены в соответствующем разделе) и влияют на её ландшафт. При этом необходимо отметить, что функции смарт-контрактов предполагают замену их кода, что делает возможным изменение роли кошельков.

Особенности использования технологии Blockchain киберпреступным сообществом

Выявление подозрительных финансовых операций, ассоциированных с противозаконной практикой, проанализировано в исследованиях [6, 7]. В рамках этих исследований предложены разнообразные методики вычисления транзакций преступных группировок. Тем не менее, авторам удалось лишь теоретически обосновать эффективность своих методов, не подтверждая их практическим применением, что вызывает сомнения в надежности предложенных подходов. Более того, эти исследования проводились до широкого распространения смарт-контрактов и не учитывают их современные возможности и практическое применение.

В работе [6] описана методика анализа киберпреступлений с использованием криптовалюты Bitcoin. Этот подход включает сбор данных о транзакциях в Blockchain за определенный период, кластеризацию

адресов, построение графа транзакций и его анализ для выявления случаев кражи Bitcoin.

В статье [8] рассматриваются различные стратегии, которые киберпреступники применяют на криптовалютных биржах для вывода средств. Также проводится анализ технологий выявления таких преступников и подчеркиваются проблемы, связанные с неэффективным законодательством. Хотя это детальное исследование узкой темы, оно не включает в себя исчерпывающее использование картографических методов.

На основании проанализированных работ сформировано представление об особенностях использования киберпреступниками технологии Blockchain для осуществления своей незаконной деятельности. Установлено, что для задачи расследования компьютерных преступлений важно проследить цепочку транзакций злоумышленника от кошелька, через которые он получает криптовалюту от жертвы или заказчика до кошелька, через который осуществляется перевод цифровых активов в реальные.

Злоумышленник стремиться скрыть эту цепочку (особенно кошелёк, через который выводятся средства). Для этого используются различные механизмы, среди которых:

- традиционные миксеры;
- цепочки децентрализованных бирж и торговых площадок;
- кошельки легитимных пользователей.

Традиционные миксеры обеспечивают запутывание следов за счёт включения в состав миксера множества кошельков, между которыми непрерывно проводится большое число транзакций. С помощью миксера злоумышленник смешивает монеты со своего криптокошелька и монеты кошельков миксера. Все его средства, которые были направлены в миксер (за вычетом стоимости услуг миксера), выводятся на вновь созданные кошельки в течение нескольких циклов транзакций внутри миксера. Владение новыми кошельками передается потребителю услуг миксера.

Ограничением использования традиционного миксера являются высокие расходы на выполнение смешивающих транзакций. В блокчейнах с высокой комиссией поддержание работы миксеров оправдано лишь при наличии большого числа клиентов. Кроме того, цепочка транзакций до миксера однозначно компрометирует владельца такого кошелька. Традиционные миксеры впервые появились в блокчейне Bitcoin, являясь на тот момент единственным средством сокрытия транзакций.

Цепочки децентрализованных бирж и торговых площадок позволяют преодолеть указанные ограничения традиционных миксеров. Способ сокрытия следов заключается в следующем. С помощью децентрализованных бирж и торговых площадок осуществляется обмен криптовалюты TON (или его производных в виде различных жетонов) на токены других блокчейнов. В других блокчейнах злоумышленник может воспользоваться аналогичным механизмом перехода из блокчейна в блокчейн. Восстановить полную цепочку таких переходов затруднительно без мониторинга множества транзакций сразу во всех распространённых реестрах. Кроме того, для восстановления цепочки также требуется внутренняя информация децентрализованных бирж о связи кошельков и токенов разных блокчейнов, на которые выводились средства. При этом, некоторые блокчейны (такие как Monero), по сути, сами являются одним большим миксером, из которого невозможно получить такую информацию о связях транзакций злоумышленники.

Ещё одним механизмом сокрытия цепочки операций злоумышленника является *использование им кошельков легальных пользователей*. В первую очередь это связано с возможностью получения несанкционированного доступа к их кошелькам для использования с целью маскировки своих транзакций. Другим вариантом вовлечения легитимных пользователей в процесс сокрытия транзакций нарушителей является создание услуг в «серой зоне» (услуг, которые слабо регулируются законодательством). Например, злоумышленники могут организовать продажу легальных товаров за криптовалюту со скидкой, провоцируя легальных пользователей осуществлять

криптовалютные транзакции со своими торговыми площадками, через которые также могут продаваться товары или услуги, запрещённые в какой-либо стране. В этом случае потоки легальных пользователей смешиваются с нелегальными, что может ввести в заблуждение правоохранительные органы.

Метод информационного картографирования позволяет обнаруживать такого рода схемы маскирования транзакций, что позволяет повысить осведомлённость о текущем уровне использования киберпреступниками механизмов блокчейна, а также повысить эффективность расследования за счёт повышения уровня организации экспертного анализа транзакций.

Разработка инструментального и методического обеспечения для анализа транзакций блокчейна TON

Существование множества возможностей для сокрытия транзакций киберпреступников создаёт насущную потребность в автоматизации транзакций. В известных [6-8] средствах автоматизации реализованы методы теория графов, математической статистики и теория вероятности. Также внимание уделяется возможностям визуализации графов транзакций.

В исследовании [7] определяется характер поведения участников на основании анализа размера комиссии для совершаемых ими транзакций Bitcoin. Для этого обрабатываются данные, полученные с помощью blockexplorer.com – веб-инструмента, имеющего открытый исходный код, и позволяющего визуализировать информацию о блоках и транзакциях в Blockchain.

В статьях [6, 8] идет речь о кластерном анализе Bitcoin-транзакций. Авторами использовались инструменты bitcointools и BitIodine, с помощью которых осуществлялась ручная разметка связанных групп адресов криптокошельков.

Среди возможных направлений анализа Blockchain также можно отметить работу [11], в которой описывается инструмент для извлечения метаданных bitcoin-транзакций под названием BitcoinOpReturn. Данный инструмент специализируется на анализе инструкции OP_RETURN, позволяющей встраивать сообщения в Blockchain. В случае подтверждения майнингом транзакции с полем OP_RETURN, ее содержимое внедряется в блок, при этом сохраняясь бессрочно в Blockchain. При этом предоставляются удобные средства для изучения уязвимостей Bitcoin с использованием визуализации цепочки блоков.

Также существуют инструменты для извлечения данных из Blockchain Ethereum. Ethereum ETL (Ethereum Extract, Transform, Load) – это инструмент, предназначенный для извлечения, преобразования и загрузки данных из Blockchain Ethereum в удобном для анализа формате данных. После сбора данных инструмент позволяет проводить их преобразование для удобства анализа, например, сохранение в CSV-файла для последующего импорта в базу данных SQL является бесполезным шагом. В статье [10] был описан экстрактор данных Ethereum. Этот инструмент извлекает данные из структуры «Go Ethereum» и сохраняет их в базе данных PostgreSQL. После извлечения и сохранения проводится анализ безопасность смарт-контрактов.

В целом, для всех средств имеются следующие методические ограничения:

- отсутствуют или недостаточно полно формализована процедура анализа демаскирующих признаков цепочки транзакций киберпреступников;
- способы визуального анализа графов транзакций применяются лишь к их фрагментам (как правило, небольшого размера) и не используют метод информационного картографирования, позволяющего учесть контекст, в котором такой фрагмент располагается;
- не учитывается специфика транзакций и смарт-контрактов экосистемы TON.

С целью преодоления ограничений известных инструментов в рамках настоящей работы:

- разработано средство сбора и интеграции сведений криптовалюты TON для

системы картографирования в области защиты информации [13];

- создан алгоритм исследования информационной карты транзакций блокчейна сети TON.

Средство сбора данных о TON-транзакциях разработано на языке программирования Python. Данным средством осуществляется сбор сведений о транзакциях с использованием API сервиса toncenter.com, которые сохраняются в графовую систему управления базами данных (СУБД) Neo4j (рис. 2). Допустимо расширять возможности средства за счёт включения дополнительных функций обогащения сведений о транзакциях и криптокошельках данными из других информационных ресурсов. Примером такого обогащения является сбор сведений о пулах ликвидности, предоставляемых платформой децентрализованной биржи STON.fi через её API (api.ston.fi).

Средство интеграции сведений криптовалюты TON реализовано на базе анализатора графов Gephi и геоинформационной системы QGIS, с помощью которых осуществляется построение и анализ ландшафта информационной карты на основе сведений о транзакциях, записанных в СУБД Neo4j.

Построение и анализ информационной карты осуществляется в соответствии с алгоритмом, представленном на рис. 3.

В соответствии с алгоритмом осуществляются следующие этапы:

а) построение информационной карты:

- загрузка сведений о транзакциях в СУБД Neo4j;
- формирование ландшафта информационной карты;

б) анализ информационной карты:

- ситуационный анализ с использованием информационной карты;
- анализ рисков реализации угроз, связанных с киберпреступными сообществами.

Рассмотрим реализацию алгоритма на примере анализа блокчейн-транзакций экосистемы TON 22 марта 2024 года.

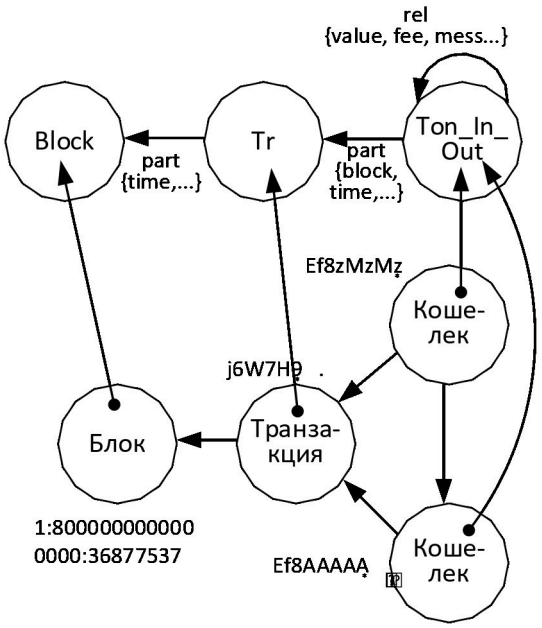

Рис. 2. Модель и пример данных о транзакциях в блокчейне TON, сохраняемых в СУБД Neo4j

Рис. 3. Алгоритм исследования информационной карты транзакций блокчейн сети TON

Построение информационной карты транзакций блокчейна TON

С помощью средства сбора в СУБД Neo4j загружены данные о 2 936 382 транзакциях из 21 516 блока сети TON (с 36856022 по) -36877537). Далее на основе загруженных данных в программе Gephi построен граф, который уложен в двухмерном пространстве с помощью

алгоритма ForceAtlas2. Выполнена его кластеризация с помощью лейденского алгоритма, осуществлена раскраска узлов. Рассчитаны метрики центральности: степень, взвешенная степень, показатель PageRank.

На основе полученного графа в программе QGIS сформирован ландшафт информационной карты. Для этого были выполнены следующие операций:

- определения контуров значимых областей информационной карты;
- экспертной разметки значимых областей информационной карты.

На рис. 4 и 5 показана информационная карта TON-транзакций, проводимых 22.03.2024 с нанесённой разметкой основных зон (рис. 4) и конкретных криптокошельков (рис. 5).

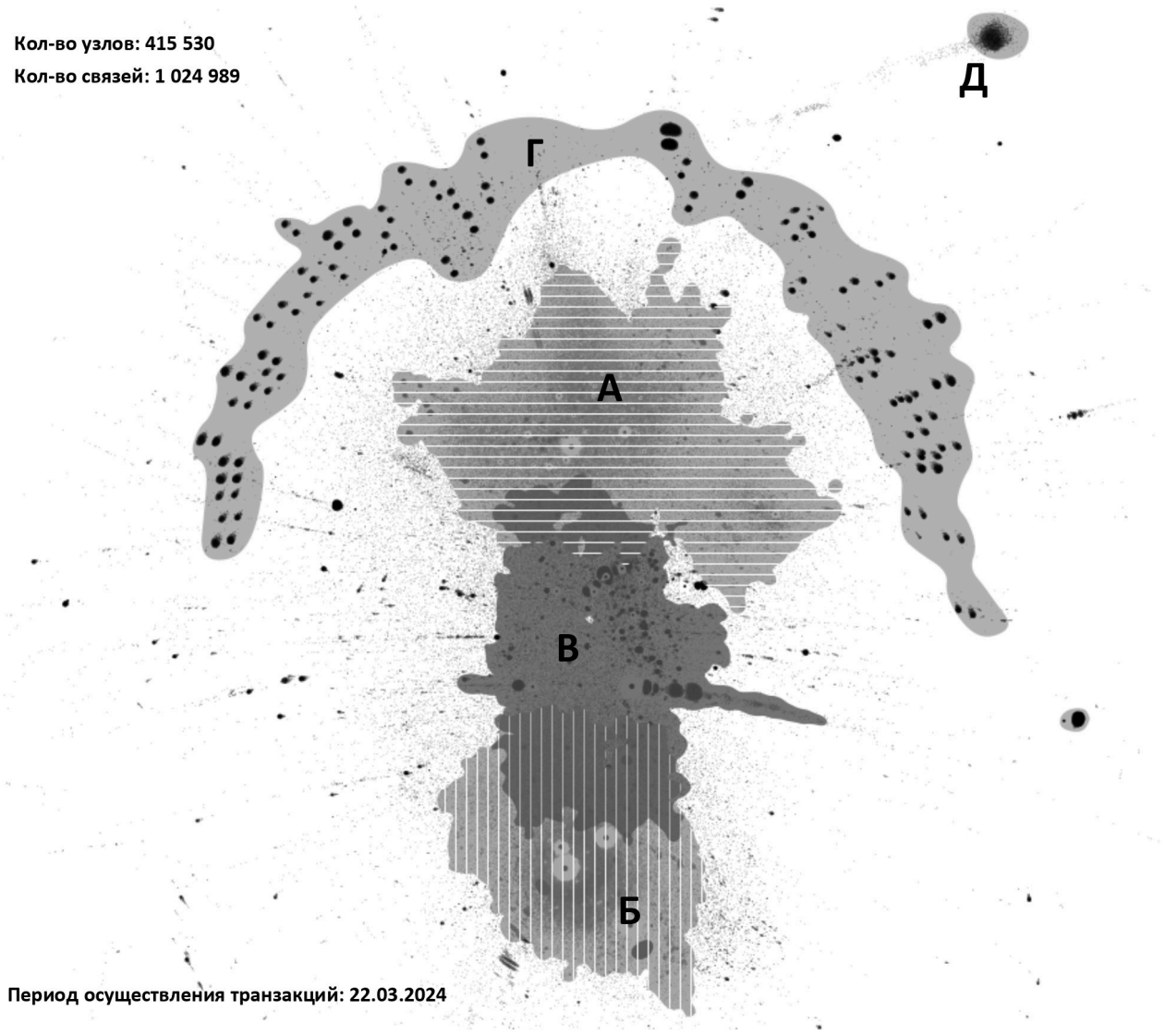

Рис. 4. Информационная карта TON-транзакций, проводимых 22.03.2024, на которой отмечены следующие наиболее крупные зоны: А – зона операций с жетонами (взаимозаменяемыми токенами), Б – зона операций с NFT (невзаимозаменяемыми токенами), В – зона операций на криптовалютных рынках (маректплейсах), Г – зона жетонов, Д – предполагаемый миксер

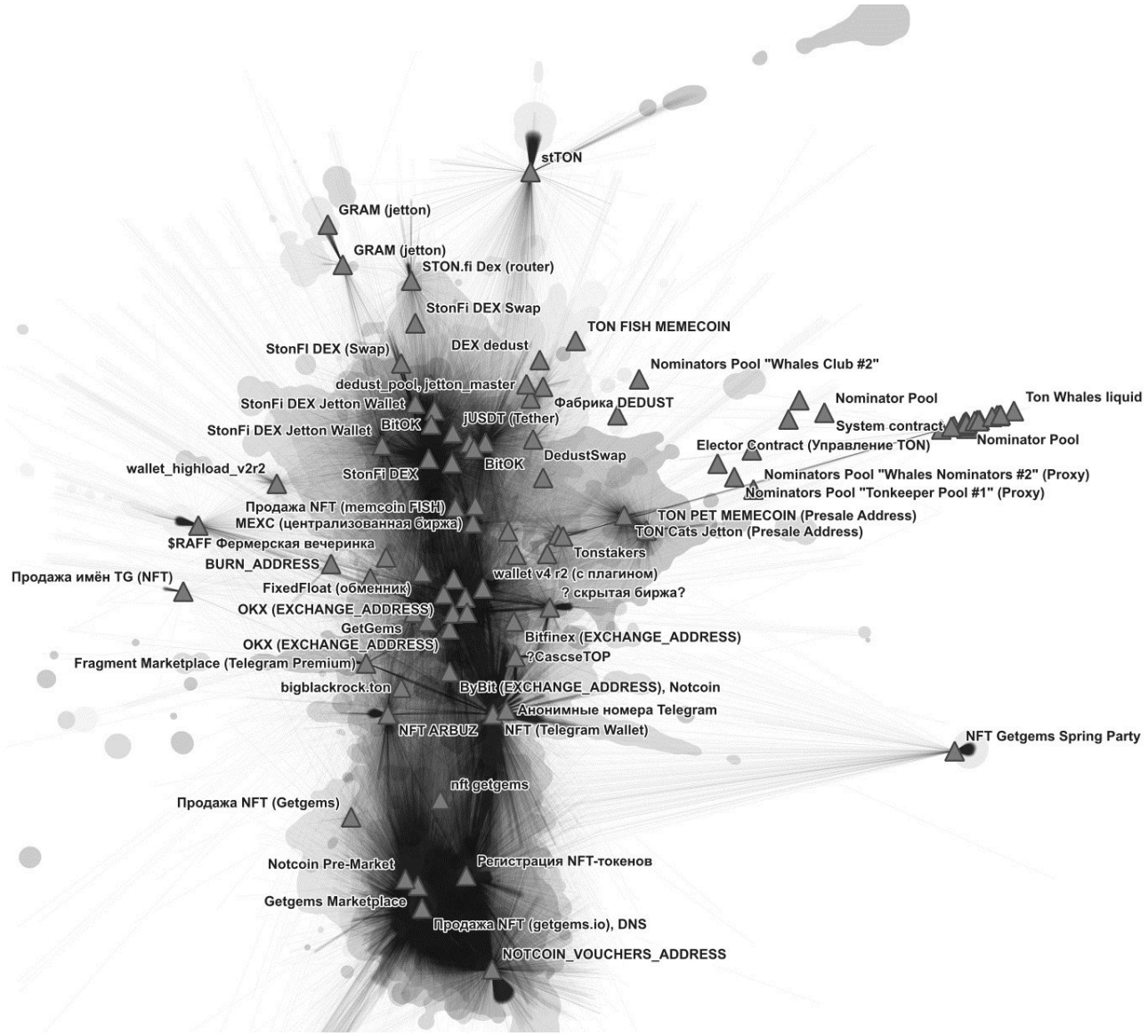

Рис. 5. Информационная карта TON-транзакций, проводимых 22.03.2024, на которой некоторые криптокошельки отмечены символом «треугольник»

Карту условно можно разбить на несколько крупных зон:

- зоны жетонов Г и операций с ними А (рис. 4);
- зона NFT – Б (рис. 4);
- зона операций на криптовалютных рынках В (рис. 4);
- зона кошельков Д, предположительно связанных с миксером (рис. 4).

В зоне жетонов Г (рис. 4) расположены преимущественно кошельки с взаимозаменяемыми токенами. Жетоны рассматриваются в качестве криптовалюты, производной от TON. Они обладают определённой ликвидностью, могут использоваться в качестве:

- эквивалента криптовалюты других блокчейнов, позволяющего обменивать её на криптовалюту TON с помощью децентрализованных бирж;
- игровой криптовалюты в децентрализованных приложений экосистемы TON;
- «мемкоинов», используемых в качестве спекулятивного актива;
- внутренней учётной единицей стоимости товара на торговых площадках, ведущих незаконную деятельность.

Примеры структур транзакций кошельков с жетонами показан на рис. 6.

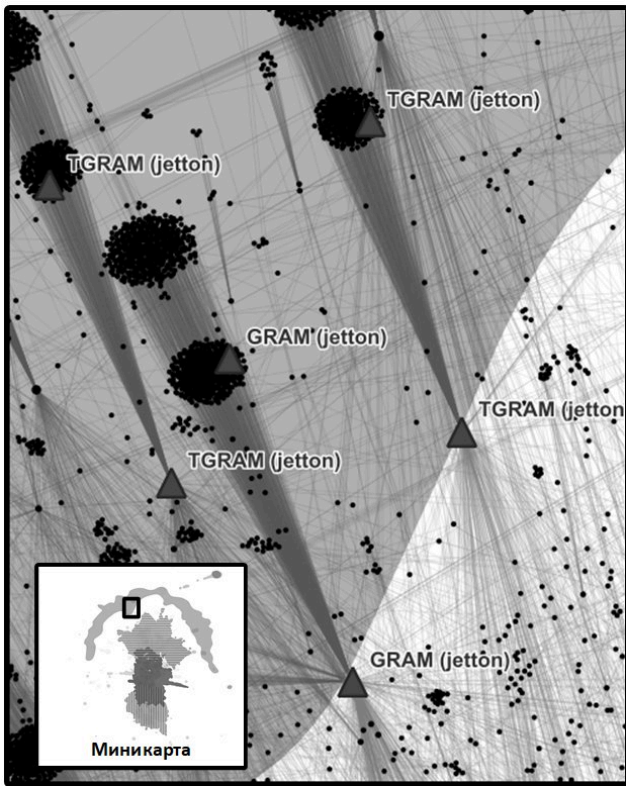

Рис. 6. Примеры структур транзакций жетонов (GRAM, TGRAM)

В зоне операций с жетонами A (рис. 4) располагаются преимущественно криптокошельки, обеспечивающие деятельно децентрализованных бирж (например, Ston.fi или DeDust.io) площадок. Инфраструктура таких объектов располагается охватывает достаточно большую область карты (рис. 7). На них осуществляется обмен таких жетонов на криптовалюту TON за счёт наличия соответствующих пулов ликвидности, работа которых регулируются особыми смарт-контрактами.

Для расследования киберпреступлений наибольший интерес представляют криптовалютные кошельки бирж, которые обеспечивают перевод цифровых активов в реальные. Пример такого кошелька показан на рис. 8. Кошелек расположен в центральной части карты, а транзакции от него (к нему) ведут в разные зоны карты. При этом необходимо отметить, что транзакций ведут как криптокошелькам обычных пользователей, так и другим биржам.

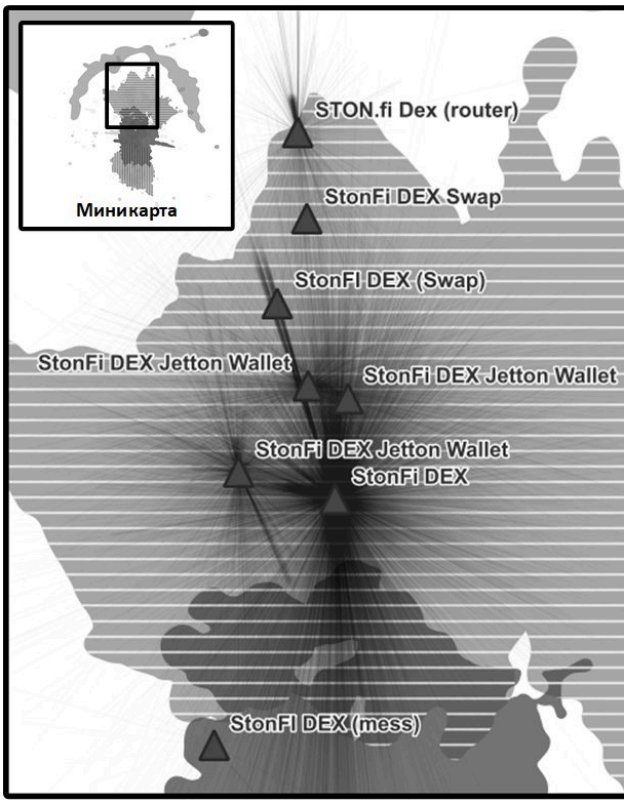

Рис. 7. Пример фрагмента структуры децентрализованной биржи (StonFi DEX)

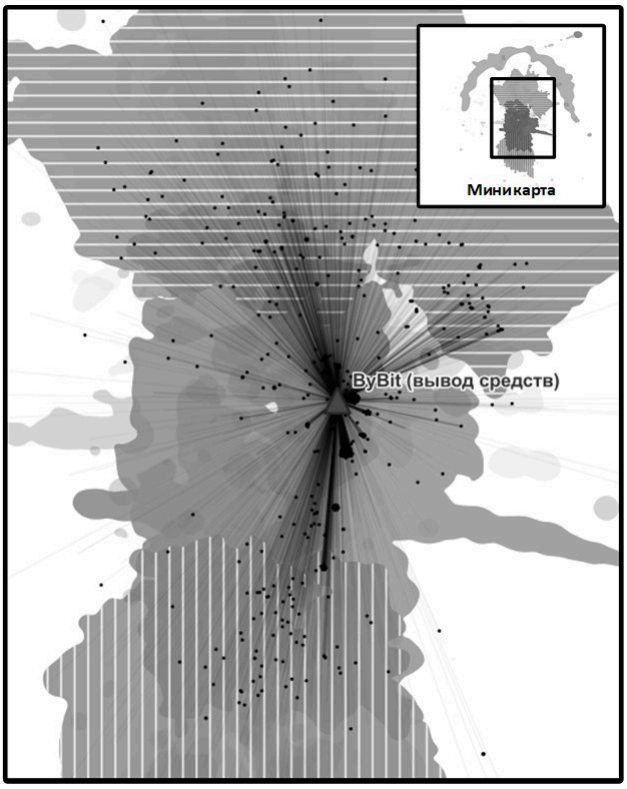

Рис. 8. Пример транзакций кошелька, используемого для перевода цифровых активов в реальные (криптовалютная биржа ByBit)

Особое внимание необходимо обращать на кошельки, расположенные за пределами основной зоны и связанные с инфраструктурой, которая может быть использована для маскирования цепочек транзакций. Например, на рис. 9 показаны таки подозрительные транзакции.

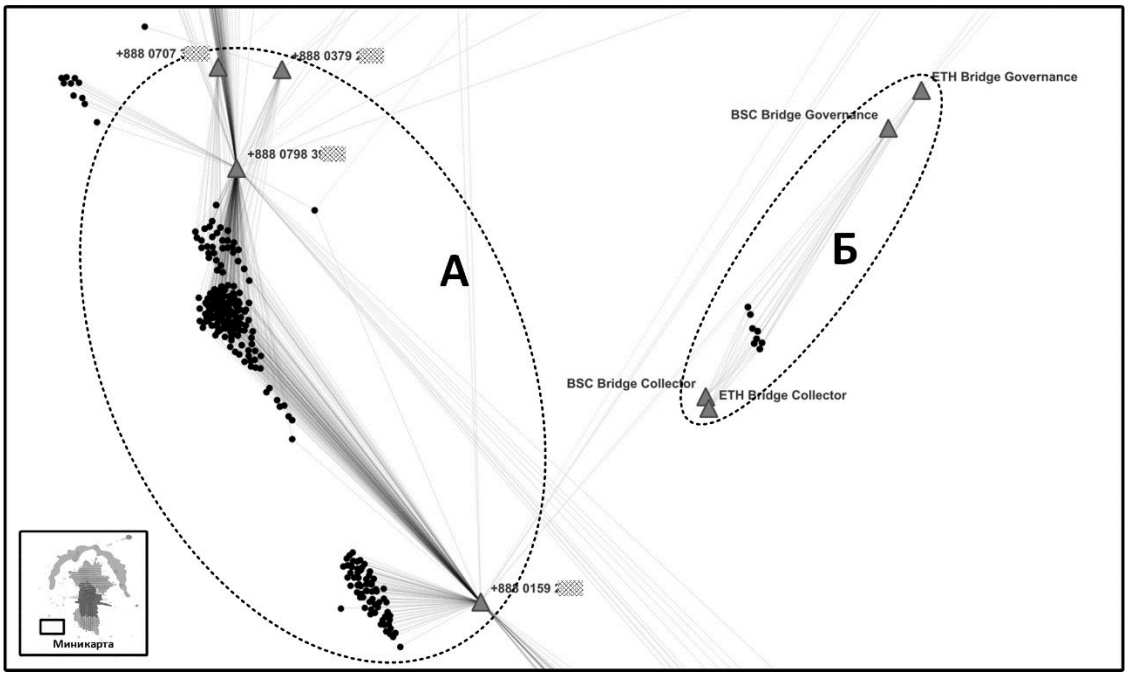

Рис. 9. Пример подозрительных транзакций, связанных с инфраструктурой, которую можно использовать для маскировки активности киберпреступников

На рис. 9 показаны транзакции А, связанные с анонимными номерами, на которые и с которых приходят суммы фиксированного размера (около 101 TON). Транзакции Б – проходящие между мостами блокчейнов Etherium и BNB Chain. Такие мосты могут использоваться в цепочках децентрализованных бирж для сокрытия киберпреступных транзакций.

Правее от зоны А расположены пулы *номинаторов*. Номинаторы делятся своей криптовалютой с валидаторами, чтобы те могли обеспечить выполнение требований для участия в процессе валидации. В свою очередь, валидаторы направляют номинаторам часть вознаграждения за участие в подтверждении криптовалютных транзакций. Логика такого сотрудничества задаётся смарт-контрактом кошелька «Пул номинаторов» (Nominator Pool).

Узлы кошельков номинаторов, которые не принимают участие в других операциях, располагаются за границами центральной зоны и образуют собственный кластер номинаторов. При этом часть узлов, которые связаны транзакциями с центральной частью, расположены левее от такого кластера. Чем дальше они расположены, тем менее связаны с центральным кластером.

В нижней части карты расположена зона операций с невзаимозаменяемыми токенами Б (рис. 4). Концепция NFT (non-fungible token) появилась в 2012 году для обеспечения возможности создания и обмена цифровыми активами, для которых обеспечивается их уникальность. Предполагается, что их использование, должно обеспечить подтверждение авторства над информационным ресурсом владельца такого невзаимозаменяемого токена.

На данный момент большинство NFT в сети TON связаны с игровыми активами, которые предоставляют их владельцам какие-либо преимущества в соответствующих играх. Однако имеются и уникальные NFT для информационных ресурсов, которые относятся к важным компонентам экосистемы TON. Такими NFT являются:

- номера телефонов, которые позволяют анонимно регистрироваться в мессенджере Telegram;
- имена пользователей и каналов мессенджера Telegram;
- имена в доменной зоне .ton, которые могут быть использованы как в качестве идентификаторов сайтов, так и кошельков в экосистеме TON.

В данной зоне значительное место занимают кошельки со смарт-контрактами NFT-платформы Getgems. Данная платформа является первой платформой в блокчейне TON, которая реализовала возможность создания, торговли и коллекционирования цифровых активов различных форматов (изображения, видео, аудио и др.).

Между зонами операций с жетонами и NFT расположена центральная область карты (рис. 4), в которой значительное влияние на ландшафт информационной карты оказывают кошельки маректплейсов, торгующих как жетонами, так и NFT. Среди таких торговых площадок можно отметить Fragment Marketplays, которая относится к инфраструктуре TON и обеспечивает возможность продажи Telegram Premium за криптовалюту TON.

Удалённость от центрально части карты может свидетельствовать об обособленности процессов, в рамках которых проводятся соответствующие транзакции. Это может являться признаком наличия незаконной или нерегулируемой деятельности. Так, например, в зоне, показанной на рис. 4 расположены кошельки предполагаемого миксера – зона Д. Структура его транзакций изображена на рис. 10.

Использование услуг миксера, зачастую, связано с незаконной деятельностью. С помощью метода информационного картографирования можно определить состав всех кошельков миксера. Ядро миксера, пример которого показан на рис. 10, состоит из 2001 кошелка. Между ними ежечасно проводится большое количество транзакций. При этом необходимо отметить, что если известен состав кошельков миксера, то можно отследить все взаимодействия с ними. Таким образом, можно фиксировать объём поступающих транзакций. Характеристики рассмотренного миксера приведены в табл. 1.

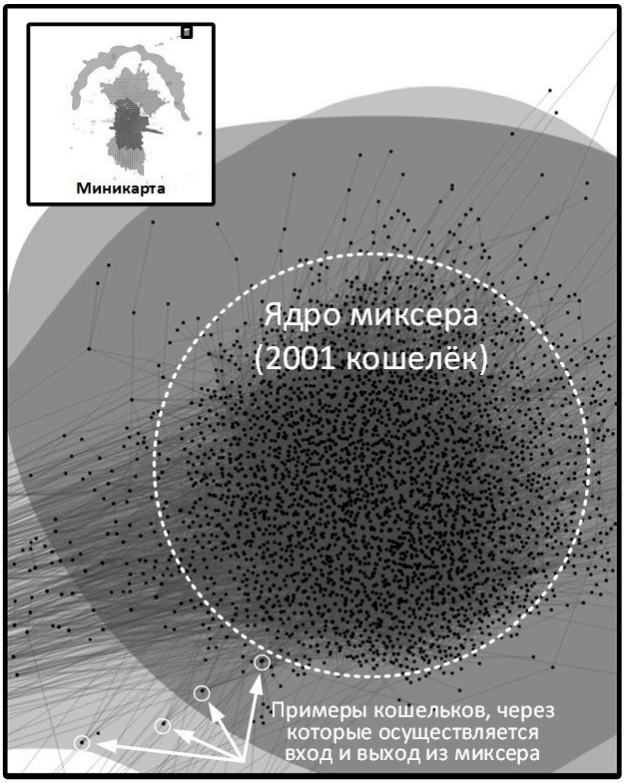

Рис. 10. Пример структуры традиционного миксера, состоящего из 2001 кошелька

Таблица 1

Пример характеристики миксера

Название параметра	Значение параметра
Тип миксера	традиционный
Кол-во узлов в ядре	2001
Кол-во ежедневных внутренних транзакций	~10 000
Ежедневная комиссия за внутренние транзакции	~6.5 TON
Ежедневно число клиентов	~500
Средняя величина транзакции, для которой осуществляется запутывание цепочки	310 TON

Меры противодействия деятельности киберпреступников, использующих криптовалюту TON

Для противодействия киберпреступным сообществам, использующим криптовалюту TON, предлагаются следующие меры защиты:

- ежедневный мониторинг обстановки в блокчейне с использованием метода информационного картографирования для своевременного выявления инфраструктуры, используемые злоумышленниками для осуществления киберпреступной деятельности;

- внедрение интеллектуальных средств обнаружения признаков атак, использующих криптовалюту TON. Эти инструменты должны быть нацелены на обнаружение скрытых угроз, таких как смешивание транзакций («миксование»);

- отслеживание транзакций, связанных с инфраструктурой киберпреступников с целью выявления новых киберпреступных сообществ, а также новых техник, использования экосистемы TON в преступной деятельности;

- использование системы автоматического и быстрого реагирования на обнаруженные угрозы, предполагающие установление протоколов действий при выявлении подозрительной активности, а также блокировку или замедление потенциально вредоносных операций;

- использование более строгого контроля над криптобиржами, предполагающего принятие жестких мер в отношении бирж, взаимодействующих с мошенниками и участвующих в процессе обналичивания незаконно полученных средств, а также внедрение систем, таких как система проверки личности (KYC) и система контроля легализации доходов (AML);

- применение сервисов и инструментов, подобных предложенным в исследовании, которые помогают эффективно расследовать преступления, а также рассчитывать риски для количественной оценки уровня опасности подобных угроз.

Заключение

В ходе исследования были определены возможные механизмы использования экосистемы TON, которые позволяют киберпреступникам маскировать цепочку своих транзакций (миксеры, цепочки децентрализованных бирж и торговых площадок, кошельки легитимных пользователей).

Представлены результаты разработки модуля сбора и интеграции сведений о криптовалютных транзакциях блокчейна TON для системы картографирования рисков в области защиты, в которой реализуются методы информационного картографирования. С помощью данного средства выявлены структурные особенности основных компонентов экосистемы TON, проявляемые на информационной карте (кластеры жетонов и NFT-токенов, децентрализованные криптовалютные биржи и торговые площадки, кошельки криптовалютных бирж, через которые массово осуществляется обмен цифровых активов на физические, стандартные криптокошельки пользователей экосистемы TON).

Разработанная методика представляет собой важный инструмент для улучшения процессов анализа и управления рисками в сфере Blockchain, которая способствует более глубокому и всестороннему пониманию динамики операций в данной области.

Результаты проведенной работы подчеркивают высокую эффективность разработанного программного инструмента. Его функционал не ограничивается лишь сбором данных, а предоставляет необходимую информацию, создавая возможности определения исходных данных для последующего риск-анализа киберпреступной деятельности.

Таким образом, проведенные исследования и разработанные методы и средства представляют важный вклад в область кибербезопасности, предостерегая от возможных угроз и обеспечивая более эффективные меры защиты информации от компьютерных атак киберпреступников, особенно с использованием технологии Blockchain TON.

Список литературы

1. РИА Новости нашло возможный криптокошелек-посредник в деле о «Крокусе» / РИА Новости. URL: https://ria.ru/20240330/koshelek-1936777283.html (дата обращения: 02.04.2024).

2. 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.

3. TON Ecosystem // URL: https://tonresear.ch/t/ton-ecosystem/505 (дата обращения: 02.04.2024).

4. Durov N. Telegram Open Network Virtual Machine // Open Netw., White Paper, Mar. 2020. P 172.

5. Telegram Open Network Virtual Machine // URL: https://ton.org/tvm.pdf (дата обращения: 02.04.2024).

6. 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.

7. Spagnuolo M. BitIodine: Extracting Intelligence from the Bitcoin Network / M. Spagnuolo, F. Maggi // Lecture Notes in Computer Science. 2014. V. 8437. P. 457-468.

8. Swan M. Blockchain: Blueprint for a New Economy / Melanie Swan // O'Reilly Media. 2015. 152 p.

9. Massimo Bartoletti A General Framework for Blockchain Analytics. Proceedings of the 1st Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers. URL: http: //blockchain.unica.it / projects / blockchain-analytics (дата обращения: 07.05.24).

10. Harrigan M. The Unreasonable Effectiveness of Address Clustering / M. Harrigan, C. Fretter // IEEE Internet of People, and Smart World Congress. 2016. P. 368 - 373.

11. Massimo B. An analysis of Bitcoin OP RETURN metadata. URL: https://arxiv.org/pdf/1702.01024.pdf (дата обращения: 07.05.2024).

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

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

15. 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 25.05.2024

Информация об авторах

Сердечный Алексей Леонидович – канд. техн. наук, начальник лаборатории, Государственный научно-исследовательский испытательный институт проблем технической защиты информации ФСТЭК России, e-mail: alex-voronezh@mail.ru

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

Москалева Екатерина Алексеевна – канд. техн. наук, доцент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

INFORMATION MAPPING OF BLOCKCHAIN TRANSACTIONS BY CYBERCRIMINALS IN THE TON ECOSYSTEM

A.L. Serdechnyy, A.O. Abramov, E.A. Moskaleva

The purpose of this paper is to develop methodological and instrumental tools for analyzing transactions in the TON (The Open Network) blockchain in order to identify features that unmask the activities of cybercriminal communities. For this purpose, this paper uses the method of information mapping, which allows presenting a large amount of data on TON transactions in the form of an information map, with the help of which an expert in the field of computer crime investigation can detect hidden relationships indicating the presence of cybercriminal activity. As part of the research, the structural features of TON-based infrastructure components are considered, and an algorithm for their detection on the transaction map is proposed. A means of collecting and integrating data on TON brickpurses has been developed, which is an information-mapping system that provides opportunities for interactive analysis of transaction maps and automation of computer crime investigation. Also, the paper proposed measures to counteract such activities. The results obtained in the course of the research allow to identify fraudulent transactions, and the developed methodology allows to create effective means to detect and prevent cybercriminal activities in the TON network, which can be useful for cryptocurrency exchanges, financial organizations and government agencies.

Keywords: information cartography, TON, Blockchain, smart contracts, damage.

Submitted 25.05.2024

Information about the authors

Alexey L. Serdechnyy – Cand. Sc. (Technical), Chief of Laboratory, State science research experimental institute of technical information protection problem of Federal service of technical an export control, e-mail: alex-voronezh@mail.ru

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

Ekaterina A. Moskaleva – Cand. Sc. (Technical), Associated Professor, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com