АННОТАЦИЯ

к диссертации Шайзата Медета Жанболатұлы
на соискание степени доктора философии (PhD)
по образовательной программе
«8D06301 – Системы информационной безопасности»
на тему «Разработка методов и моделей машинного обучения для киберкриминалистического анализа Bitcoin-транзакций»

Актуальность темы исследования. Анализ транзакций цифровых активов имеет значение для правового регулирования, финансового мониторинга и цифровой криминалистики. Для Республики Казахстан эта проблематика особенно актуальна в связи с действием Закона Республики Казахстан «О цифровых активах в Республике Казахстан», формирующего практическую потребность в инструментах контроля и анализа соответствующих операций, в том числе при финансовом мониторинге и расследовании правонарушений.

Международная значимость проблемы подтверждается тем, что имплементация стандартов FATF в отношении виртуальных активов и поставщиков соответствующих услуг остается неполной и неоднородной. Сохраняются трудности оценки рисков, надзора и применения Travel Rule, что усиливает потребность в аналитических инструментах транзакционного мониторинга.

Актуальность исследования также определяется масштабом незаконной активности в криптовалютной среде. По оценке Chainalysis, в 2025 году адреса, связанные с незаконной активностью, получили не менее 154 млрд долл. США. Несмотря на сравнительно небольшую долю таких операций в общем объеме атрибутированных криптотранзакций, их абсолютный объем остается значительным и требует развития методов выявления, анализа и документирования соответствующих потоков.

Выбор Bitcoin обусловлен публичной архитектурой сети, позволяющей анализировать транзакционный граф, прослеживать движение средств и исследовать поведенческие закономерности при сохранении псевдонимности участников. Однако доступность блокчейн-данных не гарантирует их однозначной интерпретации. Результаты существующих методов зависят от полноты разметки и процедур атрибуции, что затрудняет их проверку и сопоставление и повышает риск ошибочных выводов.

Таким образом, научная проблема состоит в недостаточной разработанности методов, позволяющих выявлять Bitcoin-транзакции с признаками нелегальной активности и объяснять результаты анализа с учетом транзакционного, временного и графового контекста.

Связь темы исследования с научно-исследовательскими программами: Диссертационная работа выполнена в рамках грантового финансирования молодых ученых «Жас ғалым» на 2025–2027 годы по проекту AP25793719 «Разработка системы анализа нелегальных криптовалютных

транзакций», реализуемому по приоритетному направлению «Национальная безопасность и оборона, биологическая безопасность» и специализированному направлению «Обеспечение информационной безопасности».

Цель исследования. Целью диссертационного исследования является разработка методов формирования интерпретируемых признаков и моделей машинного обучения для киберкриминалистического анализа Bitcoin-транзакций.

Задачи исследования. Для достижения поставленной цели в диссертационной работе решаются следующие задачи:

1. Проанализировать существующие подходы к киберкриминалистическому анализу Bitcoin-транзакций, основанные на машинном обучении и графовом анализе.
2. Исследовать существующие наборы данных Bitcoin-транзакций и способы построения транзакционных графов, определить их основные ограничения.
3. Разработать метод отбора признаков на основе генетического алгоритма для анонимизированных наборов данных Elliptic и Elliptic++.
4. Провести сравнительную оценку табличных и графовых моделей выявления нелегальных Bitcoin-транзакций.
5. Сформировать специализированный набор данных Bitcoin-транзакций с семантически открытыми признаками на основе данных публичного блокчейна Bitcoin.
6. Разработать систему криминалистически интерпретируемых признаков, включающую признаки локального отклонения от окружения, временные признаки последующего расходования средств и признаки предшествующей транзакционной истории.
7. Разработать и оценить модели машинного обучения на сформированном наборе данных, определить вклад разработанных признаков и интерпретировать результаты классификации.
8. Разработать программную систему киберкриминалистического анализа Bitcoin-транзакций, объединяющую классификацию транзакций, адресный, поведенческий и графовый анализ.

Объект исследования: процесс киберкриминалистического анализа Bitcoin-транзакций.

Предмет исследования: методы формирования и отбора признаков, а также модели машинного обучения для киберкриминалистического анализа Bitcoin-транзакций.

Методы исследования. В работе использованы системный и сравнительный анализ, генетический алгоритм, методы анализа данных, машинного обучения и интерпретации моделей**.**

Научная новизна исследования

Предложена система из 61 криминалистически интерпретируемого дескриптора Bitcoin-транзакций, формализующих выявленные при анализе

практических кейсов паттерны движения средств. Признаки характеризуют локальное отклонение от графового окружения, динамику последующего расходования выходов и отклонение текущих характеристик от значений, ожидаемых по предшествующей транзакционной истории. Их добавление к 26 базовым признакам повысило качество всех проверенных моделей: средний прирост PR-AUC составил 3.97 п. п., а F1-score – 4.26 п. п. Абляционный анализ подтвердил вклад всех трёх групп признаков.

Разработана модель выявления нелегальных Bitcoin-транзакций на основе CatBoost, использующая сформированный набор данных с раскрытой семантикой 87 признаков вместо анонимизированных характеристик Elliptic. Сохранены графовая структура, временные срезы и разметка Elliptic, восстановлены публичные идентификаторы транзакций, а порядок вычисления признаков формально определён. Модель достигла средних значений PR-AUC 90.27 %, F1-score 83.90 % и Recall 81.11 %.

Предложен обёрточный метод отбора анонимизированных признаков на основе генетического поиска и оценки подмножеств моделью Random Forest по F1-score нелегального класса. Отбор выполняется только на обучающих временных срезах. На наборе Elliptic метод сократил признаковое пространство со 166 до 53 признаков и обеспечил Precision 99.37 %, Recall 73.13 % и F1-score 84.26 %, превысив опубликованные показатели RF+GCN на 2.3, 5.6 и 4.7 п. п. соответственно. На Elliptic++ отобрано 85 из 183 признаков, а F1-score превысил результат полного набора на 1.57 п. п.

Теоретическая значимость исследования состоит в развитии теоретико-методических основ интерпретируемого киберкриминалистического анализа Bitcoin-транзакций за счет формализации признаков локального отклонения от окружения, временных признаков последующего расходования и признаков предшествующей транзакционной истории. Предложенная система объединяет эти признаки с транзакционными и структурно-графовыми характеристиками, что позволяет учитывать параметры транзакции, ее положение в графе, отклонение от локального окружения, динамику последующего расходования и отклонение от ожидаемых значений, рассчитанных по предшествующей транзакционной истории. Разработанные признаки вычисляются непосредственно по данным блокчейна и имеют содержательную интерпретацию.

Практическая значимость исследования состоит в возможности применения разработанного программно-аналитического инструментария для подготовки данных о Bitcoin-транзакциях, их анализа и классификации, интерпретации результатов модели и представления полученных выводов для экспертной проверки. Разработанный инструментарий может применяться подразделениями финансового мониторинга, правоохранительными органами, криптовалютными биржами и организациями, осуществляющими противодействие отмыванию доходов и расследование преступлений с использованием криптовалют.

Положения, выносимые на защиту:

1. Система криминалистически интерпретируемых признаков Bitcoin-транзакций, формализующая криминалистические гипотезы, повышает качество выявления нелегальных транзакций: ее включение в базовое признаковое представление обеспечило прирост PR-AUC и F1-score для всех проверенных моделей, при этом максимальные приросты составили 5.19 п. п. по PR-AUC и 7.46 п. п. по F1-score.
2. Модель выявления нелегальных Bitcoin-транзакций на основе алгоритма CatBoost отличается тем, что обучена на сформированном наборе данных с семантически открытыми транзакционными, структурно-графовыми и криминалистически интерпретируемыми признаками и не использует анонимизированные признаки Elliptic, что позволяет применять ее для первичного анализа реальных Bitcoin-транзакций, достигнутые значения PR-AUC, F1-score и Recall составили 90.27 %, 83.90 % и 81.11 % соответственно.
3. Метод отбора признаков для блокчейн-наборов данных с анонимизированными признаками, основанный на генетическом поиске подмножеств признаков и их оберточной оценке моделью Random Forest по F1-score нелегального класса, при применении к набору данных Elliptic позволил сформировать подмножество из 53 признаков вместо исходных 166, при этом значения Precision, Recall и F1-score модели Random Forest на отобранном подмножестве превысили опубликованные показатели модели RF+GCN исходного бенчмарка Elliptic на 2.3, 5.6 и 4.7 п. п. соответственно.

Апробация результатов диссертационной работы. Результаты исследования обсуждены на научных семинарах факультета информационных технологий и искусственного интеллекта и кафедры кибербезопасности и криптологии КазНУ имени аль-Фараби, а также представлены на конференции «Фараби әлемі» в докладе «Биткоин желісіндегі ауытқуларды анықтау әдісі» (Алматы, 2022).

Публикации диссертационной работы: Результаты диссертационного исследования опубликованы в 5 научных работах, из них 2 статьи – в журналах, индексируемых в базе данных Scopus, 2 статьи – в изданиях, рекомендованных Комитетом по обеспечению качества в сфере науки и высшего образования Министерства науки и высшего образования Республики Казахстан, и 1 работа – в материалах международной научной конференции:

Научные статьи, опубликованные в журналах, индексируемых в базе данных Scopus:

1. Shaizat M., Mussiraliyeva S., Tereikovskyi I. Forensically Interpretable Graph Descriptors for Improved Illicit Bitcoin Transaction Detection // International Journal of Computer Network and Information Security. – 2026. – Vol. 18, No. 3. – P. 63–84. Процентиль журнала по данным Scopus – 72.
2. Shaizat M., Mussiraliyeva S. Enhanced Identification of Illicit Bitcoin Transactions Through Genetic Algorithm-Based Feature Selection // Eastern-

European Journal of Enterprise Technologies. – 2025. – Vol. 4, No. 9 (136). – P. 34–42. Процентиль журнала по данным Scopus – 57.

Научные статьи, опубликованные в изданиях, рекомендованных КОКСНВО:

3. Мусиралиева Ш. Ж., Шайзат М. Ж., Бекетова А. К., Абайұлы Е., Манасова А. Б. О методе идентификации подозрительных транзакций в Биткоин сети / Identification of Suspicious Transactions in the Bitcoin Network // Известия Национальной академии наук Республики Казахстан. Серия физико-математическая. – 2023. – № 1 (345). – С. 154–169.
4. Мусиралиева Ш. Ж., Шайзат М. Ж., Бекетова А. К., Манасова А. Б. Биткоин желісінде күдікті транзакцияларды анықтау: талдау, белгілер және машиналық оқыту алгоритмдері // Вестник Национальной инженерной академии Республики Казахстан. – 2023. – № 3 (89).

Научные работы, опубликованные в материалах международных конференций:

5. Елтай Ж., Шайзат М., Бекетова А. Биткоин желісіндегі ауытқуларды анықтау әдісі // Материалы Международной научной конференции студентов и молодых ученых «Фараби әлемі». – Алматы, Казахстан, 2022. – С. 42.

Объем и структура диссертации

Диссертация состоит из введения, четырёх разделов, заключения и списка использованных источников. В первом разделе рассмотрены основы киберкриминалистического анализа Bitcoin-транзакций, существующие методы и наборы данных. Во втором разделе разработан метод отбора анонимизированных признаков на основе генетического алгоритма и сопоставлены табличные и графовые модели. В третьем разделе сформирован набор данных с семантически открытыми признаками, разработаны интерпретируемые дескрипторы и оценены модели машинного обучения. В четвёртом разделе разработана гибридная архитектура киберкриминалистического анализа Bitcoin-транзакций и описана её реализация в виде веб-приложения. Общий объём работы составляет 114 страниц, включая 41 рисунок и 20 таблиц. Список использованных источников включает 104 наименования.

Личный вклад автора

Личный вклад автора заключается в анализе научной литературы, разработке методов формирования и отбора признаков, подготовке набора данных, построении моделей машинного обучения, программной реализации предложенного подхода и интерпретации полученных результатов. Автором также подготовлены научные публикации по теме диссертации.