Казахский национальный университет имени аль-Фараби

УДК 004.056:336.7(043)

На правах рукописи

ШАЙЗАТ МЕДЕТ ЖАНБОЛАТҰЛЫ

Разработка методов и моделей машинного обучения для киберкриминалистического анализа Bitcoin-транзакций

8D06301 – Системы информационной безопасности

Диссертация на соискание степени доктора философии (PhD)

Отечественный научный консультант:
Мусиралиева Ш. Ж.,
кандидат физико-математических
наук, профессор,
Алматы, Казахстан

Зарубежный научный консультант:
Терейковский И. А.,
доктор технических наук, профессор,
Киев, Украина

Республика Казахстан
Алматы, 2026

СОДЕРЖАНИЕ

НОРМАТИВНЫЕ ССЫЛКИ 3
ОПРЕДЕЛЕНИЯ 4
ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ 6
ВВЕДЕНИЕ 7
1 ОСНОВЫ КИБЕРКРИМИНАЛИСТИЧЕСКОГО АНАЛИЗА BITCOIN-ТРАНЗАКЦИЙ 14
1.1 Bitcoin-транзакции как объект киберкриминалистического анализа 14
1.2 Типологии незаконной активности в сети Bitcoin 17
1.3 Методы киберкриминалистического анализа Bitcoin-транзакций 20
1.4 Наборы данных для анализа Bitcoin-транзакций 23
1.5 Научная проблема и границы исследования 24
1.6 Выводы по разделу 1 25
2 ОТБОР ПРИЗНАКОВ И СРАВНИТЕЛЬНАЯ ОЦЕНКА МОДЕЛЕЙ ВЫЯВЛЕНИЯ НЕЛЕГАЛЬНЫХ BITCOIN-ТРАНЗАКЦИЙ 26
2.1 Наборы данных Elliptic и Elliptic++ 26
2.2 Постановка задачи и экспериментальный протокол 28
2.3 Отбор признаков на основе генетического алгоритма 32
2.4 Результаты экспериментов 37
2.5 Интерпретация результатов и ограничения исследования 43
2.6 Выводы по разделу 2 45
3 РАЗРАБОТКА КРИМИНАЛИСТИЧЕСКИ ИНТЕРПРЕТИРУЕМЫХ ПРИЗНАКОВ И МОДЕЛИ ВЫЯВЛЕНИЯ НЕЛЕГАЛЬНЫХ BITCOIN-ТРАНЗАКЦИЙ 46
3.1 Формирование интерпретируемого набора данных 46
3.2 Базовые и структурно-графовые признаки Bitcoin-транзакций 49
3.3 Анализ перемещения средств в сети Bitcoin по материалам расследований 55
3.4 Формализация криминалистически интерпретируемых признаков .. 58
3.5 Результаты экспериментов 76
3.6 Предложенная модель и интерпретация результатов 83
3.7 Выводы по разделу 3 87
4 ГИБРИДНАЯ СИСТЕМА КИБЕРКРИМИНАЛИСТИЧЕСКОГО АНАЛИЗА BITCOIN-ТРАНЗАКЦИЙ 89
4.1 Архитектура гибридной системы анализа Bitcoin-транзакций 89
4.2 Хранилище данных об адресах Bitcoin и проверка источников 90
4.3 Поведенческие индикаторы, анализ локального окружения и объединение результатов 92
4.4 Разработка программной системы 96
4.5 Выводы по разделу 4 103
ЗАКЛЮЧЕНИЕ 104
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 106

НОРМАТИВНЫЕ ССЫЛКИ

В настоящей диссертации использованы ссылки на следующие нормативные правовые акты и стандарты:

Приказ Министра науки и высшего образования Республики Казахстан от 20 июля 2022 года № 2 «Об утверждении государственных общеобязательных стандартов высшего и послевузовского образования».

Приказ Министра образования и науки Республики Казахстан от 31 марта 2011 года № 127 «Об утверждении Правил присуждения степеней».

ГОСТ 7.32–2017 Система стандартов по информации, библиотечному и издательскому делу. Отчет о научно-исследовательской работе. Структура и правила оформления.

ГОСТ 7.1–2003 Система стандартов по информации, библиотечному и издательскому делу. Библиографическая запись. Библиографическое описание. Общие требования и правила составления.

ОПРЕДЕЛЕНИЯ

В настоящей диссертации используются следующие термины и определения.

Термин	Определение
Bitcoin-адрес	Идентификатор, используемый для получения средств и задания условий их последующего расходования. Один пользователь или кошелек может управлять несколькими адресами.
Bitcoin-кошелек	Средство управления ключами и адресами для формирования и подписания транзакций.
Bitcoin-транзакция	Операция, расходующая ранее созданные непотраченные выходы и формирующая новые выходы.
CoinJoin	Способ совместного формирования Bitcoin-транзакции несколькими участниками с множеством входов и выходов, затрудняющий установление соответствия между отправителями и получателями средств.
illicit	Метка транзакции, отнесенной в наборе данных к классу, связанному с нелегальной активностью. Не является правовой оценкой.
licit	Метка транзакции, отнесенной в наборе данных к классу, связанному с легальной активностью. Не является правовой оценкой.
Proof-of-Work	Механизм консенсуса, основанный на выполнении вычислительной работы и используемый для формирования и добавления новых блоков в блокчейн Bitcoin.
UTXO (Unspent Transaction Output)	Непотраченный выход Bitcoin-транзакции, который может быть использован в качестве входа новой транзакции.
Атрибуция	Установление предполагаемой принадлежности объекта или его связи с конкретным лицом, организацией, сервисом либо иной сущностью.
Адресная кластеризация	Объединение адресов, предположительно принадлежащих одной сущности, на основе эвристик и внешних данных.
Вход транзакции	Элемент транзакции, ссылающийся на ранее созданный непотраченный выход и обеспечивающий его расходование.
Выход транзакции	Создаваемая транзакцией сумма с установленными условиями последующего расходования.

Выход сдачи	Выход транзакции, возвращающий остаток средств на адрес, контролируемый отправителем.
Высота блока	Порядковое положение блока в блокчейне.
Графовый сигнал	Обнаружение в локальном окружении подтвержденного адресного совпадения.
Комиссия транзакции	Разность между общей суммой входов и выходов транзакции.
Консолидация UTXO	Объединение нескольких непотраченных выходов во входах одной транзакции с формированием меньшего числа новых выходов.
Майнер	Участник сети, формирующий блоки и включающий в них проверенные транзакции.
Миксер	Сервис, смешивающий и перераспределяющий средства для затруднения их прослеживания.
Ончейн-данные	Данные, записанные в блокчейне: входы, выходы, суммы, комиссии, время и связи между транзакциями.
Псевдонимность	Свойство сети, при котором транзакции публичны, но личность владельца адреса непосредственно не раскрывается.
Реактивация адреса	Возобновление операций после длительного периода неактивности.
Транзакционный граф	Направленный граф, в котором вершины обозначают транзакции, а ребра отражают расходование выходов одной транзакции во входах другой.
Трассировка движения средств	Восстановление последовательности движения средств между связанными адресами и транзакциями.

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

API – Application Programming Interface
ANOVA – Analysis of Variance
APPNP – Approximate Personalized Propagation of Neural Predictions
BABD – Bitcoin Address Behavior Dataset
BTC – Bitcoin
CatBoost – Categorical Boosting
DGI – Deep Graph Infomax
FATF – Financial Action Task Force
FN – False Negative
FP – False Positive
GA – Genetic Algorithm
GAR – Graph Autoregressive Lineage
GAT – Graph Attention Network
GCN – Graph Convolutional Network
GCNII – Graph Convolutional Network with Initial Residual and Identity Mapping
GGNN – Gated Graph Neural Network
GIN – Graph Isomorphism Network
GNN – Graph Neural Network
GraphMAE – Graph Masked Autoencoder
GraphSAGE – Graph Sample and Aggregate
H2GCN – Higher-order and Heterophily-aware Graph Convolutional Network
HITS – Hyperlink-Induced Topic Search
JK-Net – Jumping Knowledge Network
LightGBM – Light Gradient Boosting Machine
MAD – Median Absolute Deviation
MLP – Multilayer Perceptron
PNA – Principal Neighbourhood Aggregation
PR – PageRank
PR-AUC – Area Under the Precision–Recall Curve
REST API – Representational State Transfer Application Programming Interface
RF – Random Forest
RPGE – Reachability-Preserving Graph Embedding
SDN List – Specially Designated Nationals and Blocked Persons List
SGC – Simple Graph Convolution
SGFormer – Simplified Graph Transformer
SHAP – SHapley Additive exPlanations
SkipGCN – Graph Convolutional Network with Skip Connections
TN – True Negative
TP – True Positive
txid – Transaction Identifier
UTXO – Unspent Transaction Output
XGBoost – eXtreme Gradient Boosting

ВВЕДЕНИЕ

Актуальность темы исследования. Анализ транзакций цифровых активов имеет значение для правового регулирования, финансового мониторинга и цифровой криминалистики. Для Республики Казахстан эта проблематика особенно актуальна, поскольку обращение цифровых активов включено в национальную систему правового регулирования Законом Республики Казахстан «О цифровых активах в Республике Казахстан». Наличие специального правового регулирования формирует практическую потребность в инструментах контроля и анализа операций с цифровыми активами, в том числе при осуществлении финансового мониторинга и расследовании связанных с ними правонарушений [1].

Значимость этой проблематики подтверждается международной практикой. В обновлении 2025 года FATF отмечает, что имплементация стандартов в отношении виртуальных активов и поставщиков соответствующих услуг остается неполной и неоднородной. Сохраняются проблемы, связанные с оценкой рисков, надзором за деятельностью поставщиков услуг и практическим применением Travel Rule [2]. Эти проблемы не могут быть устранены только технологическими средствами, однако они усиливают потребность в аналитических инструментах, поддерживающих транзакционный мониторинг, оценку рисков и надзорную деятельность.

Актуальность исследования также определяется масштаб незаконной активности в криптовалютной среде. По оценке Chainalysis, в 2025 году адреса, связанные с незаконной активностью, получили не менее 154 млрд долл. США, хотя доля таких операций в общем объеме атрибутированных криптотранзакций остается сравнительно низкой. Это означает, что даже при небольшой относительной доле таких операций их абсолютный объем остается значительным и требует развития методов выявления, анализа и документирования соответствующих потоков [3].

Выбор Bitcoin в качестве объекта исследования обусловлен особенностями ее публичной архитектуры. Она позволяет проводить формализованный анализ транзакционного графа, прослеживать движение средств и исследовать поведенческие закономерности при сохранении псевдонимности участников [4].

Сочетание публичности и псевдонимности делает Bitcoin сложным объектом киберкриминалистического анализа. Доступность данных блокчейна не гарантирует их однозначной и обоснованной интерпретации. Исследования в области криминалистического анализа блокчейна показывают, что результаты существующих методов зависят от полноты разметки данных и используемых процедур атрибуции. Это затрудняет проверку и сопоставление полученных результатов и повышает риск ошибочных выводов [5].

Таким образом, данные о Bitcoin-транзакциях доступны, однако существующие подходы не всегда позволяют получить на их основе понятные выводы. 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 криминалистически интерпретируемых признаков Bitcoin-транзакций. При ее разработке учитывались повторяющиеся схемы движения средств, выявленные при анализе практических кейсов и формализованные в виде вычисляемых количественных дескрипторов. Система включает три группы признаков, характеризующие локальное отклонение транзакции от графового окружения, динамику последующего расходования ее выходов и отклонение текущих характеристик транзакции от значений, характерных для ее предшествующей истории. Расширение базового набора из 26 транзакционных и структурно-графовых признаков за счет добавления 61 разработанного дескриптора повысило значения PR-AUC и F1-score у всех проверенных моделей: средний прирост PR-AUC составил 3.97 п. п., а F1-score – 4.26 п. п.

Разработана модель выявления нелегальных Bitcoin-транзакций на основе CatBoost, обученная на специализированном наборе данных с открытой семантикой признаков. Для формирования набора данных восстановлены идентификаторы Bitcoin-транзакций и сформировано признаковое пространство из 87 характеристик: 26 транзакционных и структурно-графовых признаков и 61 криминалистически интерпретируемого дескриптора, рассчитываемого по формально определенным правилам. В отличие от моделей, использующих 166 анонимизированных признаков Elliptic, входные характеристики разработанной модели могут быть получены на основе данных анализируемой Bitcoin-транзакции и ее графового контекста. На сформированном наборе модель показала лучшие результаты среди проверенных моделей, достигнув средних значений PR-AUC 90.27 %, F1-score 83.90 % и Recall 81.11 %.

Предложен оберточный метод отбора признаков для блокчейн-наборов данных с анонимизированными признаками, содержательный смысл которых не раскрыт, что исключает их экспертный отбор на основе предметной интерпретации. Метод использует генетический поиск подмножеств признаков, представленных бинарными масками. Каждое подмножество оценивается моделью Random Forest по F1-score класса illicit. В отличие от фильтрационных методов, таких как SelectKBest, которые оценивают признаки по отдельности, предложенный метод учитывает их совместное влияние на результат классификации. Число отбираемых признаков заранее не задается и определяется в ходе оптимизации. Отбор выполняется только в пределах обучающих временных срезов, при этом более поздние тестовые срезы исключаются из генетического поиска, что предотвращает утечку информации из тестовой выборки. Применение метода к набору Elliptic позволило сформировать подмножество из 53 признаков вместо исходных 166 и получить значения Precision 99.37 %, Recall 73.13 % и F1-score 84.26 %, которые превышают опубликованные показатели модели RF+GCN исходного бенчмарка

Elliptic на 2.3, 5.6 и 4.7 п. п. соответственно. В рамках эксперимента F1-score превысил результат Random Forest на полном наборе признаков на 1.36 п. п., а результат SelectKBest при том же количестве признаков – на 5.49 п. п. Дополнительная проверка на наборе Elliptic++ привела к отбору 85 признаков из 183 и повышению F1-score на 1.57 п. п. по сравнению с полным набором и на 3.42 п. п. по сравнению с SelectKBest. Полученные результаты показывают, что предложенный метод сокращает анонимизированное признаковое пространство, повышает F1-score выявления транзакций класса illicit и может применяться к наборам данных, для которых содержательная интерпретация и экспертный отбор признаков невозможны.

Теоретическая значимость исследования заключается в развитии подходов к интерпретируемому анализу Bitcoin-транзакций. Предложенные признаки описывают отклонение транзакции от локального окружения, особенности последующего расходования ее выходов и отличие текущих параметров от значений, характерных для предшествующей транзакционной истории. Они дополняют транзакционные и структурно-графовые характеристики и позволяют учитывать свойства транзакции, ее положение в графе и предшествующую историю. Все признаки формируются на основе данных блокчейна и имеют понятный содержательный смысл.

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, представленные в диссертационной работе, неоднократно заслушивались и обсуждались на научных семинарах факультета информационных технологий и искусственного интеллекта Казахского национального университета имени аль-Фараби, кафедры кибербезопасности и криптологии, а также были представлены на Международной научной конференции студентов и молодых ученых «Фараби әлемі» в докладе «Биткоин желісіндегі ауытқуларды анықтау әдісі» (Алматы, Казахстан, 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

Диссертационная работа состоит из введения, четырех разделов, заключения и списка использованных источников.

Во введении обосновывается актуальность темы исследования, формулируются научная проблема, цель и задачи исследования, определяются объект, предмет и методы исследования, раскрываются научная новизна, теоретическая и практическая значимость работы, приводятся положения, выносимые на защиту, сведения о публикациях и личном вкладе автора.

В первом разделе рассматриваются теоретические и методические основы киберкриминалистического анализа Bitcoin-транзакций. Анализируются особенности транзакционной и графовой структуры сети Bitcoin, типологии незаконной активности, методы машинного обучения и графового анализа, открытые наборы данных, а также ограничения существующих подходов.

Во втором разделе разрабатывается метод отбора анонимизированных признаков на основе генетического алгоритма для наборов данных Elliptic и Elliptic++. Сравниваются полный и сокращенный наборы признаков, табличные модели и графовые нейронные сети, а также анализируются полученные результаты и ограничения их интерпретации.

В третьем разделе формируется набор данных Bitcoin-транзакций с семантически открытыми и воспроизводимыми признаками. Разрабатываются транзакционные и структурно-графовые признаки, признаки локального отклонения от окружения, временные признаки последующего расходования и признаки предшествующей транзакционной истории. Проводится сравнительная оценка моделей машинного обучения, анализируется вклад отдельных групп признаков и интерпретируются результаты классификации.

В четвертом разделе предлагается гибридная архитектура киберкриминалистического анализа Bitcoin-транзакций. Она объединяет классификацию транзакций, проверку адресов, анализ поведенческих индикаторов и локального графового окружения. Описываются порядок объединения результатов и реализация подхода в виде веб-приложения.

В заключении обобщаются основные результаты исследования, оценивается полнота решения поставленных задач, приводятся рекомендации по применению разработанных методов и программного инструментария, рассматриваются вычислительная эффективность и научный уровень выполненной работы.

Общий объем диссертации составляет 114 страниц компьютерного текста, включая 41 рисунок, 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.

1 ОСНОВЫ КИБЕРКРИМИНАЛИСТИЧЕСКОГО АНАЛИЗА BITCOIN-ТРАНЗАКЦИЙ

В первой главе рассматриваются теоретические и методические основы киберкриминалистического анализа Bitcoin-транзакций. Описываются технические характеристики транзакций, UTXO-модель и графовое представление сети, типологии незаконной активности и методы машинного обучения. Особое внимание уделяется открытым наборам данных Elliptic и Elliptic++, а также ограничениям, связанным с анонимизацией признаков, построением графа и временным разделением данных. На основе проведенного анализа формулируется научная проблема.

1.1 Bitcoin-транзакции как объект киберкриминалистического анализа

В отличие от традиционных платежных систем, где значительная часть информации находится у операторов и недоступна исследователю напрямую, подтвержденные Bitcoin-транзакции сохраняются в открытом распределенном реестре [6]. За время существования сети Bitcoin в распределенном реестре накоплен значительный объем данных, которые можно повторно извлекать, сопоставлять и анализировать в рамках блокчейн-анализа и киберкриминалистических исследований [7]. При этом сеть Bitcoin псевдонимна: по данным реестра можно определить адреса, входы и выходы транзакций, суммы переводов, комиссии и связи между операциями [6], но нельзя установить лиц, контролирующих эти адреса [8].

Эти особенности определяют специфику киберкриминалистического анализа Bitcoin-транзакций, который сочетает методы блокчейн-аналитики и цифровой криминалистики. Извлечение транзакций, построение графов и прослеживание движения средств относятся к задачам блокчейн-аналитики [9]. Используемые для этого инструменты должны обеспечивать полноту, целостность и конфиденциальность получаемой информации [10]. Цифровая криминалистика, в свою очередь, устанавливает требования к достоверности результатов, документированию этапов анализа и воспроизводимости проведенного исследования [5].

Одной из основных форм представления транзакционных данных служит граф, позволяющий исследовать связи и движение средств между объектами сети. Согласно обзору J. Wu и соавт., исследования в этой области охватывают моделирование транзакционной сети, изучение поведения ее участников по доступным адресным и транзакционным данным, а также выявление нетипичных или вызывающих подозрение схем перевода средств [9].

В диссертации предлагается трехуровневая схема интерпретации результата анализа, включающая модельный результат, криминалистическую гипотезу и правовую оценку. Модель только присваивает транзакции определенный класс. На основе этого результата с учетом признаков, графового

контекста и доступных данных может быть сформулирована криминалистическая гипотеза. Правовую оценку дает уполномоченный специалист на основе всех данных. Результата модели машинного обучения самого по себе для этого недостаточно.

Технические характеристики Bitcoin-транзакций

Сеть Bitcoin основана на распределенном реестре, поддерживаемом одноранговой сетью и механизмом консенсуса Proof-of-Work [6]. В работе подробно не рассматриваются криптографические алгоритмы, механизм консенсуса и взаимодействие узлов сети. Основное внимание уделяется данным о транзакции, которые сохраняются в блокчейне и затем используются для анализа. После формирования транзакция передается в сеть и проверяется узлами. До включения в блок она может находиться в пуле неподтвержденных транзакций, после чего майнер может добавить ее в новый блок. На этом этапе уже доступны идентификатор транзакции, ее входы и выходы, а также комиссия. После включения транзакции в блок становятся известны высота и хеш блока, а также время включения. Количество подтверждений затем увеличивается по мере добавления последующих блоков [11]. Создание транзакции, ее появление в пуле неподтвержденных транзакций (mempool), включение в блок и получение последующих подтверждений представляют собой разные временные события. До добавления в блок скорость обработки зависит от распространения транзакции по сети, размера комиссии и политики отдельных узлов. Жизненный цикл Bitcoin-транзакции показан на рисунке 1.1.



Рисунок 1.1 – Жизненный цикл Bitcoin-транзакции

В основе связей между Bitcoin-транзакциями лежит UTXO-модель. Каждая новая транзакция расходует выходы, созданные ранее, и формирует новые, которые впоследствии могут использоваться в следующих транзакциях [11]. Благодаря этому движение средств можно прослеживать по цепочке операций, как показано на рисунке 1.2. Комиссия, размер, сумма, число входов и выходов характеризуют структуру транзакции. Большое число входов может указывать на объединение UTXO, а наличие нескольких выходов может быть связано с переводом средств разным получателям и возвратом оставшейся суммы отправителю**.** Однако ни один из этих признаков сам по себе не позволяет определить характер транзакции: высокая комиссия или большое число выходов встречаются и в обычных переводах [12]. Поэтому при определении характера транзакции эти признаки анализируются вместе с ее связями с предшествующими и последующими операциями, а также временем их совершения [13].



Рисунок 1.2 – UTXO-модель транзакций в сети Bitcoin: связь между входами, выходами и непотраченными выходами

В зависимости от задачи граф Bitcoin-сети может строиться на уровне транзакций, адресов или сущностей. На транзакционном уровне вершинами графа выступают Bitcoin-транзакции, а ребра отражают расходование ранее сформированных выходов [7]. Для представления транзакций с несколькими входами и выходами может использоваться гиперграф [14]. На адресном уровне рассматриваются адреса, используемые для получения и расходования средств, при этом один кошелек может управлять несколькими адресами и ключами. На сущностном уровне адреса с помощью эвристик кластеризации объединяются в группы, предположительно принадлежащие одному участнику сети [15]. Для

уточнения таких групп и выявления адресов сдачи могут использоваться внешние данные и методы обучения с учителем [16].

В практическом расследовании обычно анализируется не весь граф, а локальный маршрут средств, начинающийся с известной транзакции или адреса. Для его построения применяются модели отслеживания средств, основанные на определенных правилах их распределения между последующими транзакциями. Полученный маршрут зависит от выбранного правила, доступного графового контекста и условий завершения анализа [17].

Помимо структуры связей учитывается время совершения транзакций. Без временных данных нельзя определить, как быстро средства переводились дальше, какие интервалы были между транзакциями и повторялись ли такие последовательности [13]. Взаимосвязь транзакционного, адресного и сущностного уровней, а также место локального маршрута в графовом анализе показана на рисунке 1.3.



Рисунок 1.3 – Переход от отдельной транзакции к локальному графовому контексту

Поскольку основной единицей анализа является Bitcoin-транзакция, в экспериментальной части используется транзакционный граф. Адресный и сущностный уровни рассматриваются как дополнительные источники информации.

1.2 Типологии незаконной активности в сети Bitcoin

По структуре связей нельзя однозначно определить, связана ли Bitcoin-транзакция с незаконной активностью. Похожие связи между транзакциями могут возникать при агрегации платежей сервисом, биржевом клиринге, микшировании, выводе похищенных средств или обычной консолидации UTXO [12].

В литературе рассматриваются платежи программ-вымогателей, операции даркнет-маркетов, мошенничество, кражи и отмывание средств. Для усложнения отслеживания могут применяться миксеры, CoinJoin, цепочки поэтапного вывода и перевод средств в активы с повышенной приватностью.

Группа разработки финансовых мер борьбы с отмыванием денег (FATF) отмечает, что необычные транзакционные паттерны, размер и частота транзакций, профиль отправителя или получателя, источник средств и технологии анонимизации могут быть индикаторами нелегальной активности, но требуют проверки в контексте [12].

При анализе платежей программ-вымогателей особенно важно сопоставление транзакционного графа с внешними данными об известных адресах и первоначальных платежах, а также со сведениями, полученными от потерпевших [18]. Для идентификации сервисов микширования анализируются локальные графовые структуры и различия транзакционных паттернов [19]. Даркнет-маркеты исследуются на основе транзакционных сетей, связанных с уже известными площадками, и взаимодействий между их участниками. Такой анализ позволяет рассматривать структуру входящих и исходящих потоков, связи между рынками, покупателями и продавцами [20].

При анализе мошеннических схем и краж устанавливают источник поступления средств и прослеживают их дальнейшее движение [12]. Также учитываются скорость перемещения средств, дробление суммы между несколькими адресами, ее последующее объединение и использование миксеров [12]. Эти признаки оцениваются по всей цепочке транзакций, пример которой приведен на рисунке 1.4.

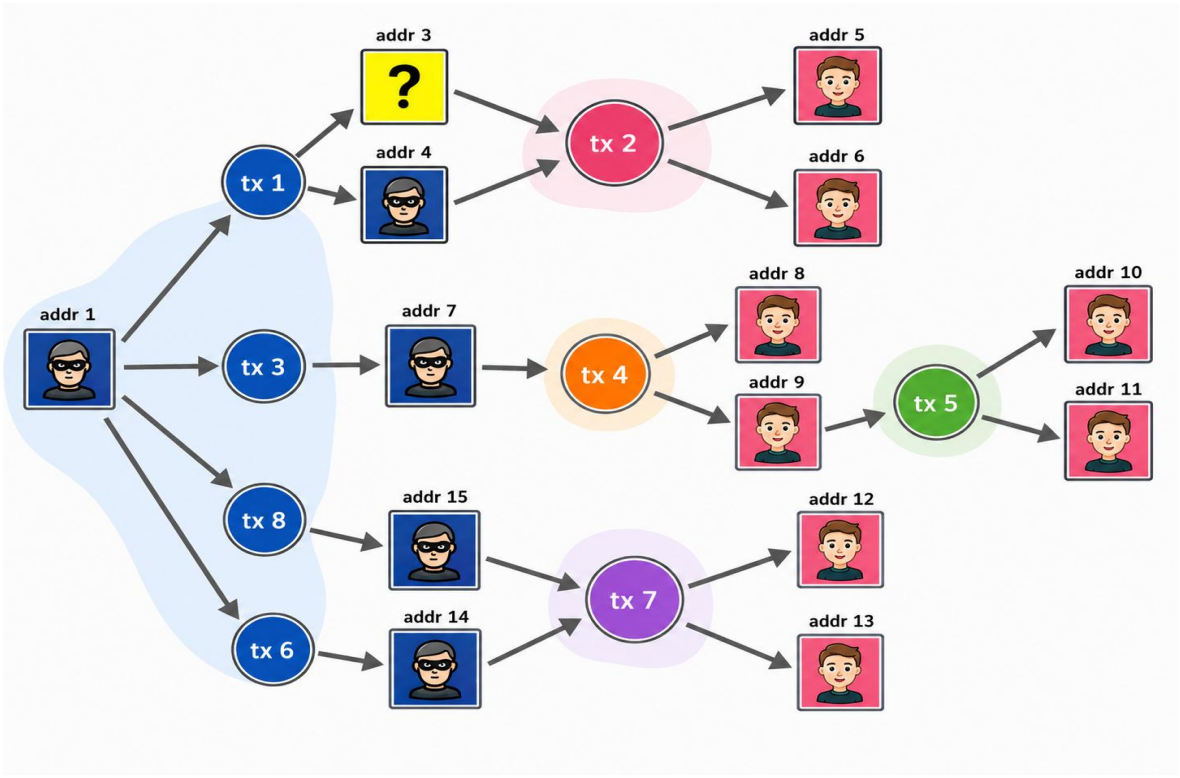


Рисунок 1.4 – Схематическое представление расщепления и последующего движения средств в локальном Bitcoin-графе [21]

В таблице 1.1 обобщены признаки, учитываемые при криминалистической интерпретации различных видов активности в сети Bitcoin.

Таблица 1.1 – Виды незаконной активности и особенности их криминалистической интерпретации

Типология	Уровень анализа	Что важно для интерпретации	Возможный источник ошибки
Программы-вымогатели	Адрес, транзакция, маршрут средств	Известные адреса, время вывода, последующая консолидация	Без внешних данных платеж трудно отличить от обычного перевода
Даркнет-маркеты	Поток средств, локальный подграф	Регулярные поступления, связи с сервисами, дальнейший вывод средств	Сходная структура встречается и у обычных сервисов
Мошеннические схемы	Подграф, временная динамика	Массовые поступления, перераспределение средств, повторяемость схемы	Без жалоб и внешних данных назначение переводов остается неясным
Кражи	Исходное событие и маршрут вывода	Быстрое дробление средств, миксеры, промежуточные адреса	Принадлежность промежуточных адресов трудно установить

Индикаторы риска, транзакционные паттерны и аномалии

Наличие подозрительного признака или отклонение от обычного поведения еще не означает, что Bitcoin-транзакция связана с незаконной деятельностью. FATF рассматривает такие индикаторы как основание для дополнительной проверки, но не как доказательство отмывания денег или финансирования терроризма [12]. Такими индикаторами могут быть повторяющиеся переводы крупных сумм, объединение множества небольших поступлений, быстрое распределение средств между несколькими адресами и взаимодействие с сервисами микширования [12]. Конкретный набор признаков зависит от анализируемой схемы. Например, при выявлении финансовых пирамид учитываются массовые поступления и последующее перераспределение средств [22], а при анализе платежей программ-вымогателей учитываются связи с известными адресами и дальнейшее движение средств [18].

Если несколько признаков образуют устойчивую конфигурацию связей или повторяющуюся последовательность переводов, такую структуру рассматривают как транзакционный паттерн. Аномалией считается заметное отклонение характеристик транзакции, адреса или последовательности переводов от обычных значений. Chandola, Banerjee и Kumar выделяют точечные, контекстные и коллективные аномалии [23]. Точечная аномалия относится к отдельной транзакции или адресу, контекстная определяется с

учетом условий наблюдения, а коллективная проявляется в группе связанных событий. Поэтому отдельные транзакции могут не выделяться, тогда как вся последовательность переводов образует нетипичную схему. В графовых данных аномалии могут обнаруживаться на уровне вершин, ребер, подграфов и временных последовательностей [24]. Методы обнаружения аномалий позволяют выделять транзакции и фрагменты графа, требующие дополнительной проверки [25]. Последовательность перехода от наблюдаемого признака к криминалистической гипотезе показана на рисунке 1.5.



Рисунок 1.5 – Переход от наблюдаемого признака к криминалистической гипотезе

1.3 Методы киберкриминалистического анализа Bitcoin-транзакций

С ростом объема данных и усложнением схем перемещения средств ручной анализ Bitcoin-транзакций стал затруднительным. Поэтому для обработки большого числа признаков начали применять машинное обучение, а для изучения связей между транзакциями и их положения в сети – графовые методы. Наряду с адресными эвристиками и ручным анализом графов получили развитие методы обучения с учителем (supervised learning), без учителя (unsupervised learning) и с частичной разметкой (semi-supervised learning), а также графовые нейронные сети (GNN).

Одним из наиболее часто используемых подходов является обучение с учителем. Для обучения таких моделей нужны размеченные датасеты с признаками транзакций. В качестве признаков могут использоваться параметры входов и выходов, характеристики локального окружения, центральности и интервалы между событиями. Для классификации часто применяются ансамблевые модели на основе решающих деревьев, прежде всего Random Forest и бустинговые методы [26, 27]. Они подходят для работы с разными типами признаков, учитывают нелинейные зависимости и позволяют оценить вклад отдельных характеристик в прогноз.

Когда признаков много, некоторые из них могут дублировать друг друга, слабо влиять на результат или вносить шум. В таких случаях проводят отбор признаков, чтобы сократить избыточность, снизить вычислительную нагрузку и улучшить качество модели [28]. Если смысл признаков известен, некоторые из

них можно исключить или оставить с учетом предметной области. Но когда признаки анонимизированы, такой подход неприменим, поэтому используют статистические и информационные методы, включая корреляционный анализ, анализ различий между классами и оценку взаимной информации. Из датасета могут удаляться дублирующие и сильно коррелирующие признаки [28].

Полностью размеченные наборы Bitcoin-транзакций встречаются редко, из-за этого обучение с учителем подходит не всегда. Поэтому при отсутствии меток применяются кластеризация и методы обнаружения аномалий. В работе [29] алгоритмы k-means и trimmed k-means использовались для группирования транзакций по сходству их характеристик. Isolation Forest выделяет наблюдения, которые быстро отделяются от основной массы данных при последовательных случайных разбиениях [30]. Одноклассовые модели определяют область пространства признаков, в которой сосредоточена основная часть наблюдений [31]. Автоэнкодеры выявляют аномалии по величине ошибки восстановления исходных данных [32]. Результатом кластеризации становится отнесение транзакции к определенной группе, тогда как методы обнаружения аномалий формируют аномальный балл. Ни принадлежность к кластеру, ни высокий аномальный балл сами по себе не подтверждают связь транзакции с незаконной деятельностью.

Методы с частичной разметкой используют одновременно размеченные и неразмеченные данные. В методах распространения меток информация о классах размеченных объектов используется для оценки связанных с ними неразмеченных объектов [33]. В других подходах модель присваивает предполагаемые классы транзакциям, для которых прогноз получен с высокой уверенностью, и использует их при дальнейшем обучении [34]. Такой подход позволяет расширить обучающую выборку, но ошибки на этапе присвоения меток могут повлиять на последующие результаты. При самоконтролируемом обучении метки классов на первом этапе не нужны. Модель сначала учится выделять полезные характеристики из признаков и связей между узлами, а затем использует их для классификации транзакции по размеченной части данных [35, 36].

Граф в таких исследованиях может использоваться по-разному. В ранних работах по графу преимущественно рассчитывали степени узлов, показатели центральности и характеристики окружения. Затем появились методы, которые извлекают из структуры векторное представление узла, или эмбеддинг, а итоговую классификацию выполняет отдельная модель. В Inspection-L модуль Deep Graph Infomax с энкодером на основе GIN формирует эмбеддинги узлов, которые затем используются моделью Random Forest для классификации транзакций [35]. В RPGE, предложенном в работе [37], применяется другой способ: эмбеддинги строятся по сети достижимости транзакций, что сокращает объем ручного формирования признаков. В сквозной графовой нейронной сети эти этапы объединены: представление узла и классификатор обучаются совместно [38].

Архитектуры GNN различаются тем, как собирают сведения о соседях. GCN агрегирует признаки соседних узлов с учетом нормализации структуры

графа [38]. GAT использует механизм внимания, позволяющий присваивать разные веса соседним узлам [39]. GIN предназначена для различения локальных графовых структур [40]. На качество классификации также влияют способ построения графа [35, 37] и выбор временной границы доступного подграфа [13]. Рассмотренные методы и связанные с ними ограничения сопоставлены в таблице 1.2.

Таблица 1.2 – Сопоставление методов машинного обучения и графового анализа Bitcoin-транзакций

Группа методов	Используемая информация	Принцип анализа	Основное ограничение
Признаковые модели с обучением с учителем	Признаки транзакции и ее графового окружения	Обучение классификатора на размеченных данных	Зависимость от качества меток и состава признаков
Методы без учителя	Числовые признаки без разметки	Поиск операций, отличающихся от основной массы данных	Отклонение не подтверждает принадлежность к классу illicit
Обучение с частичной разметкой	Размеченные и неразмеченные узлы графа	Распространение меток и использование псевдометок	Риск накопления ошибок в псевдометках
Самоконтролируемое обучение	Признаки и структура графа без меток на этапе предобучения	Предобучение представлений с последующей классификацией по размеченным данным	Зависимость от предтекстовой задачи и качества представлений
Графовые признаки и векторные представления	Связи, свойства соседей и положение узла в графе	Расчет признаков или эмбеддингов для отдельного классификатора	Зависимость от построения графа и способа представления
Графовые нейронные сети	Признаки узлов и структура связей	Совместное формирование представления узла и прогноза	Сложность интерпретации и зависимость от способа построения графа.

Возможности интерпретации зависят от типа модели. В моделях, использующих табличные признаки, вклад отдельных переменных оценивают по показателям важности и значениям SHAP [41]. Для графовых нейронных сетей интерпретация немного сложнее, поскольку прогноз определяется не

только признаками анализируемого узла, но и его окружением, включая соседние узлы и связи между ними. GNNExplainer и другие методы позволяют выделить подграф и признаки, наиболее значимые для конкретного решения модели [42].

1.4 Наборы данных для анализа Bitcoin-транзакций

В исследованиях Bitcoin-транзакций качество данных не менее важно, чем выбор алгоритма. От полноты, корректности и согласованности данных зависят результаты анализа и последующая интерпретация полученных выводов. Работа с открытыми блокчейн-данными начинается с подготовки набора. Записи о Bitcoin-транзакциях надо извлечь, очистить, привести к единому формату и построить граф [7]. На этом же этапе определяются объект анализа, временные границы и правила разметки. При этом метки обычно охватывают только часть графа и могут быть получены из разных источников [9]. Поэтому результаты разных датасетов следует сопоставлять с учетом того, что именно классифицируется, как построен граф и по какому протоколу проводилась оценка.

В данной работе в качестве основных наборов данных для анализа Bitcoin-транзакций используются Elliptic Dataset и его расширенная версия Elliptic++. Elliptic содержит 203 769 Bitcoin-транзакций, 234 355 направленных связей, 166 признаков и 49 временных срезов и представляет Bitcoin-транзакции в виде временного транзакционного графа с метками licit, illicit и unknown [26]. Значительная часть транзакций не имеет меток, то есть отнесена к классу unknown, а признаки анонимизированы, что не позволяет определить, какие характеристики транзакций повлияли на результат модели [26]. Elliptic++ дополняет эту структуру адресным, двудольным и сущностным уровнями, что позволяет исследовать различные объекты и типы связей блокчейна [21].

Другие открытые корпуса используются в литературе для смежных постановок. Elliptic2 рассматривает не отдельные транзакции, а подграфы, выделенные из крупного фонового графа Bitcoin [43]. BitcoinHeist содержит данные о платежах программ-вымогателей и поэтому охватывает более узкую задачу [44]. BABD используется для анализа поведения Bitcoin-адресов [45]. ORBITAAL предназначен для анализа временных связей между предполагаемыми сущностями Bitcoin [15]. Крупномасштабные транзакционные графы позволяют исследовать структуру сети и масштабируемость графовых методов [7]. Сравнительная характеристика указанных открытых наборов данных приведена в таблице 1.3.

Таблица 1.3 – Открытые Bitcoin-датасеты и их значение для задач криминалистического анализа

Датасет	Объект и тип задачи	Сильная сторона	Ограничение

Elliptic Dataset	Транзакции, классификация licit / illicit / unknown	Наличие графовой и временной структуры	Анонимизация признаков
Elliptic++	Транзакции, адреса, сущности, многоуровневый графовый анализ	Несколько представлений графа	Более сложная интерпретация уровней анализа
BitcoinHeist	Адреса, связанные с ransomware, выявление платежей программ-вымогателей	Фокус на конкретной типологии незаконной активности	Не охватывает другие виды незаконной активности
BABD	Bitcoin-адреса, поведенческий анализ адресов	Адресный уровень признаков	Не предназначен для прямой классификации отдельных транзакций
Elliptic2	Подграфы, классификация структур внутри фонового графа Bitcoin	Переход от отдельных транзакций к анализу подграфов	Результаты нельзя напрямую сопоставлять с классификацией отдельных транзакций
ORBITAAL	Сущности и временные связи, масштабируемый графовый анализ	Подходит для анализа динамики и отношений уровня сущностей	Не содержит меток licit/illicit для прямой классификации отдельных транзакций

Остальные перечисленные наборы данных важны для понимания границ существующих подходов, однако в экспериментальной части диссертации не используются, поскольку исследование основано на Elliptic и Elliptic++.

1.5 Научная проблема и границы исследования

Модели, обученные на Elliptic, позволяют классифицировать Bitcoin-транзакции по классам licit и illicit, но анонимизация признаков затрудняет объяснение полученного результата и перенос модели на новые данные [26]. Для реальной транзакции нельзя воспроизвести исходные признаки и установить, какие ее характеристики повлияли на прогноз.

Научная проблема исследования состоит в противоречии между возможностью классифицировать Bitcoin-транзакции на основе открытых блокчейн-данных и недостаточной пригодностью существующих наборов признаков и моделей для криминалистически интерпретируемого, воспроизводимого и переносимого анализа реальных транзакций. Это связано с

анонимизацией исходных признаков и зависимостью результатов от способа построения графа.

Сформулированная проблема решается в два этапа. На первом этапе на наборах данных Elliptic и Elliptic++ проводится отбор анонимизированных признаков и сравниваются табличные и графовые модели. На втором этапе создается набор данных Bitcoin-транзакций с семантически открытыми и воспроизводимыми признаками, что позволяет преодолеть ограничения исходных наборов. Эти признаки рассчитываются по данным транзакции, ее локальному графовому окружению, временной последовательности переводов и предшествующей транзакционной истории. На основе сформированного набора признаков разрабатывается модель классификации Bitcoin-транзакций.

Исследование ограничено сетью Bitcoin. Основным объектом выступает отдельная транзакция и ее графовое окружение. В работе анализируются только подтвержденные транзакции. Обозначения licit и illicit используются как метки классов в наборах данных и не являются правовой оценкой.

1.6 Выводы по разделу 1

Проведенный анализ показал, что открытые данные Bitcoin позволяют классифицировать транзакции, однако анонимизация признаков ограничивает применение существующих моделей при анализе реальных транзакций. Результат классификации и выявленные индикаторы требуют проверки с учетом характеристик транзакции, ее графового окружения, последовательности переводов и доступных внешних данных.

Во второй главе оцениваются возможности анонимизированных признаков: проводится отбор признаков с использованием генетического алгоритма и сравниваются табличные и графовые модели на наборах данных Elliptic и Elliptic++. На следующем этапе на основе этих результатов разрабатываются признаки с понятным содержанием и воспроизводимым расчетом.

2 ОТБОР ПРИЗНАКОВ И СРАВНИТЕЛЬНАЯ ОЦЕНКА МОДЕЛЕЙ ВЫЯВЛЕНИЯ НЕЛЕГАЛЬНЫХ BITCOIN-ТРАНЗАКЦИЙ

В главе рассматривается классификация Bitcoin-транзакций на данных Elliptic с учетом временной структуры, дисбаланса классов и частичной разметки. Elliptic++ используется для дополнительной проверки предложенного метода. Основное внимание уделено разработке метода отбора анонимизированных признаков на основе GA+Random Forest, в котором выбор подмножества формализован как оберточная оптимизация по F1-score класса illicit. Описываются состав наборов данных, схема кодирования меток и временное разделение на обучающую и тестовую части. Результаты предложенного метода сопоставляются с графовыми нейронными сетями и ранее опубликованными исследованиями. В завершение рассматриваются ошибки модели и ограничения, связанные с отсутствием содержательной интерпретации признаков.

2.1 Наборы данных Elliptic и Elliptic++

Набор данных Elliptic широко используется в исследованиях анализа Bitcoin-транзакций. Транзакции в нем представлены в виде графа, как показано на рисунке 2.1: вершины обозначают отдельные транзакции, а ребра показывают движения средств от одной транзакции к другой [26].

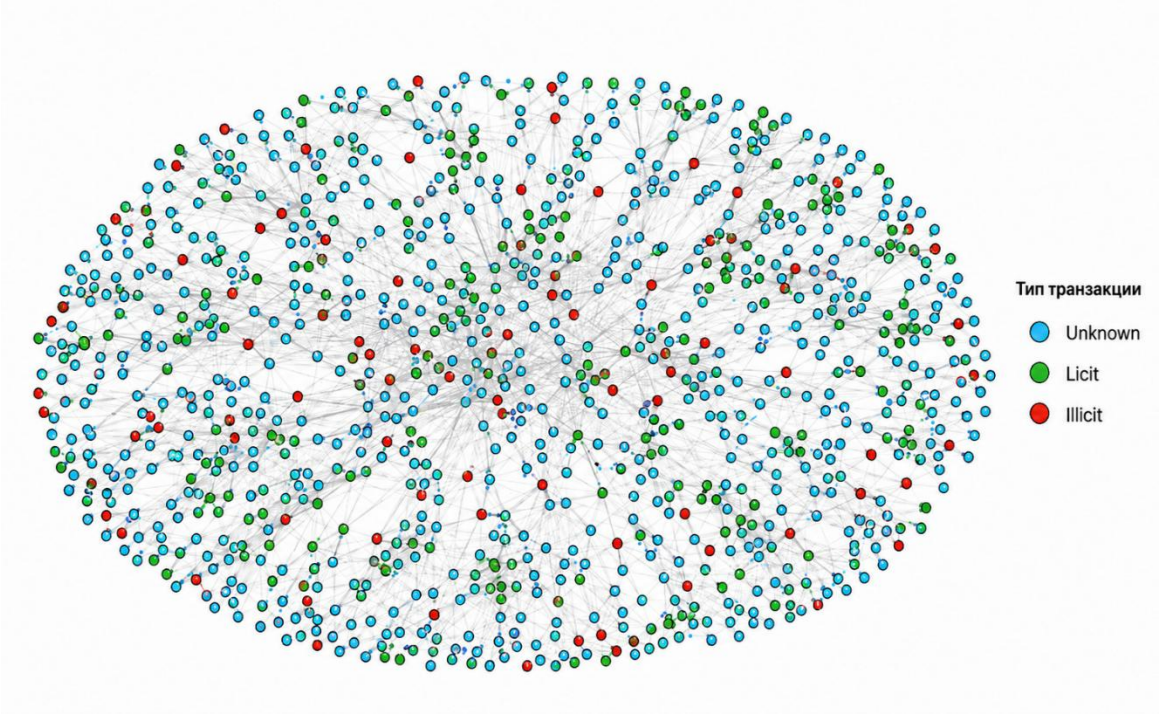


Рисунок 2.1 – Графовая структура Elliptic [46]

Датасет содержит 203 769 транзакций, 234 355 направленных ребер и 49 временных шагов, разделенных интервалами примерно в две недели. Каждый шаг включает связную компоненту транзакций, появившихся в блокчейне в

пределах менее трех часов. Связи между разными временными шагами отсутствуют [26]. Такая организация данных показана на рисунке 2.2.

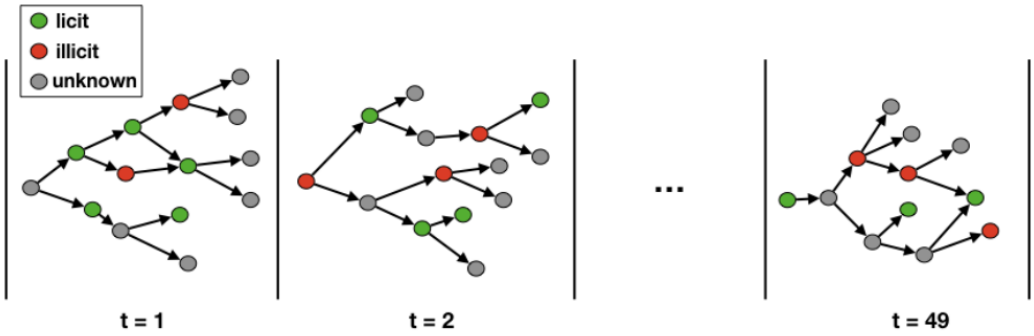


Рисунок 2.2 – Временная структура Elliptic [46]

Для каждой транзакции рассчитано 166 признаков. Из них 94 признака характеризуют саму транзакцию: ее размер, количество входов и выходов, комиссию и другие параметры. Остальные 72 содержат агрегированную статистику соседних транзакций [26]. За счет этого табличные модели получают не только сведения об отдельной транзакции, но и часть информации о ее графовом окружении.

В Elliptic размеченные транзакции относятся к двум классам: легальному (licit) и нелегальному (illicit). К классу illicit отнесены 4 545 транзакций, а к licit отнесены 42 019 транзакций. Остальные 157 205 транзакций не имеют метки. Размеченная часть составляет около 23% набора. На illicit приходится примерно 2% всех транзакций и 9,8% транзакций с известной меткой. Далее термин «нелегальные транзакции» используется как краткое обозначение транзакций, которым в наборе данных Elliptic присвоена метка illicit. Распределение классов показано на рисунке 2.3.

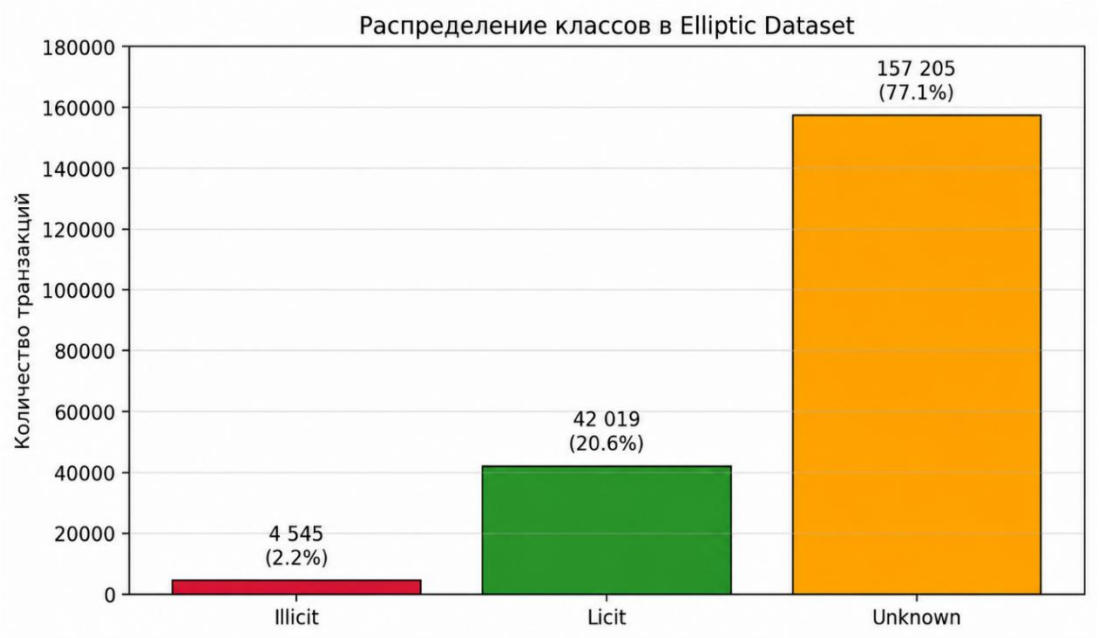


Рисунок 2.3 – Распределение классов в Elliptic Dataset

При подготовке данных учитывали дисбаланс классов и большое количество транзакций без метки. Такие транзакции нельзя автоматически относить к классу licit, поэтому их не использовали при обучении моделей с учителем и расчете метрик. В графовых моделях они сохранялись как вершины графа и поддерживали связи между размеченными транзакциями, но не получали целевую метку. Схема кодирования классов приведена в таблице 2.1.

Таблица 2.1 – Схема кодирования классов и использование unknown-вершин

Метка в датасете	Интерпретация	Бинарная метка	Использование
illicit	транзакция, размеченная как нелегальная в Elliptic	1	положительный класс
licit	транзакция, размеченная как легальная в Elliptic	0	отрицательный класс
unknown	неразмеченная транзакция	не используется	исключается из обучения с учителем, а в GNN остается как структурный контекст

В эксперименте также рассматривается датасет Elliptic++. Он содержит 183 признака, то есть на 17 больше, чем в Elliptic [21]. Полный набор Elliptic++ включает представления транзакций, адресов, двудольного графа и сущностей [21], но в этой главе используются только транзакционные данные. За счет этого в обоих случаях сохраняется одна и та же единица классификации и можно проверить, меняется ли результат после расширения признакового описания.

2.2 Постановка задачи и экспериментальный протокол

Формальная постановка задачи

Транзакции и связи между ними образуют направленный граф. Запишем его в виде (2.1):

$$G = (V, E, \tau), \tag{2.1}$$

где $V = \{v_1, \dots, v_n\}$ - множество транзакций, $E \subseteq V \times V$ - направленные ребра между ними. Ребро отражает движение средств от одной транзакции к другой. $\tau(v_i) \in \{1, \dots, 49\}$ - временной шаг транзакции v_i. Для каждой транзакции задан набор признаков $x_i \in \mathbb{R}^d$, где $d = 166$ для Elliptic и $d = 183$ для Elliptic++.

Размеченную часть графа запишем в виде (2.2):

$$L = \{v_i \in V \mid y_i \in \{0,1\}\}, \quad (2.2)$$

где $y_i = 1$ соответствует классу illicit, а $y_i = 0$ соответствует классу licit.

Для табличной модели прогноз класса запишем в виде (2.3):

$$\hat{y}_i = f_\theta(x_i), \qquad f_\theta: \mathbb{R}^d \to \{0,1\}, \quad (2.3)$$

где $\hat{y}_i$ содержит прогноз для транзакции v_i, f_θ задает функцию классификации, θ содержит параметры, полученные при обучении модели.

Вероятностная оценка (2.4):

$$p_\theta(y_i = 1 \mid x_i) \in [0,1], \quad (2.4)$$

где $p_\theta(y_i = 1 \mid x_i)$ отражает оценку принадлежности транзакции v_i к классу illicit. После применения установленного порога транзакции присваивается бинарная метка $\hat{y}_i$.

Для графовой модели оценка записывается в виде (2.5):

$$p_\theta(y_i = 1 \mid G, X) \in [0,1], \quad (2.5)$$

где X содержит признаки всех транзакций. При расчете учитываются признаки транзакции v_i и информация о связанных с ней транзакциях.

Обучающее множество задается формулой (2.6):

$$L_{\text{train}} = \{v_i \in L \mid \tau(v_i) \leq 34\}, \quad (2.6)$$

где в обучающую часть входят размеченные транзакции временных шагов 1–34.

Для тестовой части используются более поздние транзакции (2.7):

$$L_{\text{test}} = \{v_i \in L \mid \tau(v_i) \geq 35\}, \quad (2.7)$$

где в тестовую часть входят размеченные транзакции временных шагов 35–49.

Экспериментальная схема приведена на рисунке 2.4.

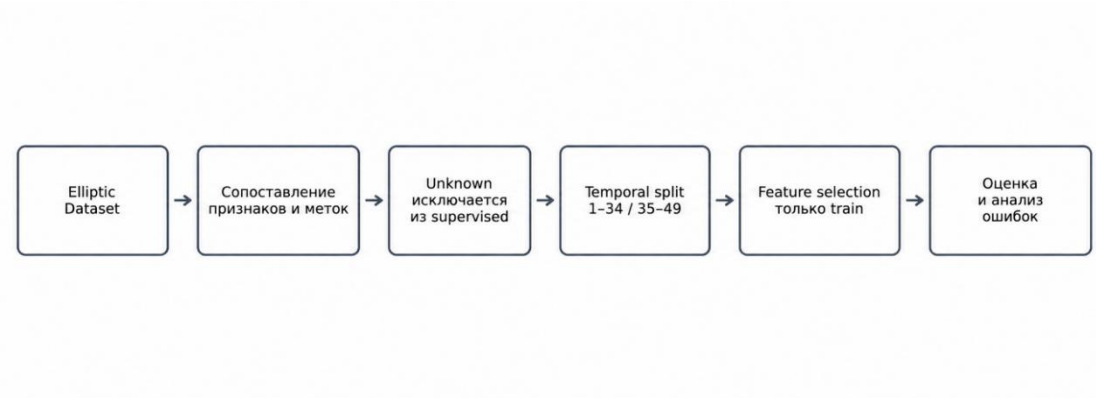


Рисунок 2.4 – Экспериментальная схема

Сравниваемые модели

В качестве основной модели выбран алгоритм случайного леса (Random Forest). Этот алгоритм машинного обучения ранее применялся для классификации транзакций в других исследованиях и показывал высокие результаты [21, 26, 27]. Random Forest способен учитывать нелинейные зависимости и взаимодействия между признаками, не требует их предварительного масштабирования и сравнительно устойчив к шуму. Алгоритм подходит для работы с большим числом признаков и позволяет оценивать их вклад в результат классификации. Random Forest строит деревья на разных подвыборках объектов и признаков, после чего объединяет их прогнозы [47]. Принцип работы модели представлен на рисунке 2.5.

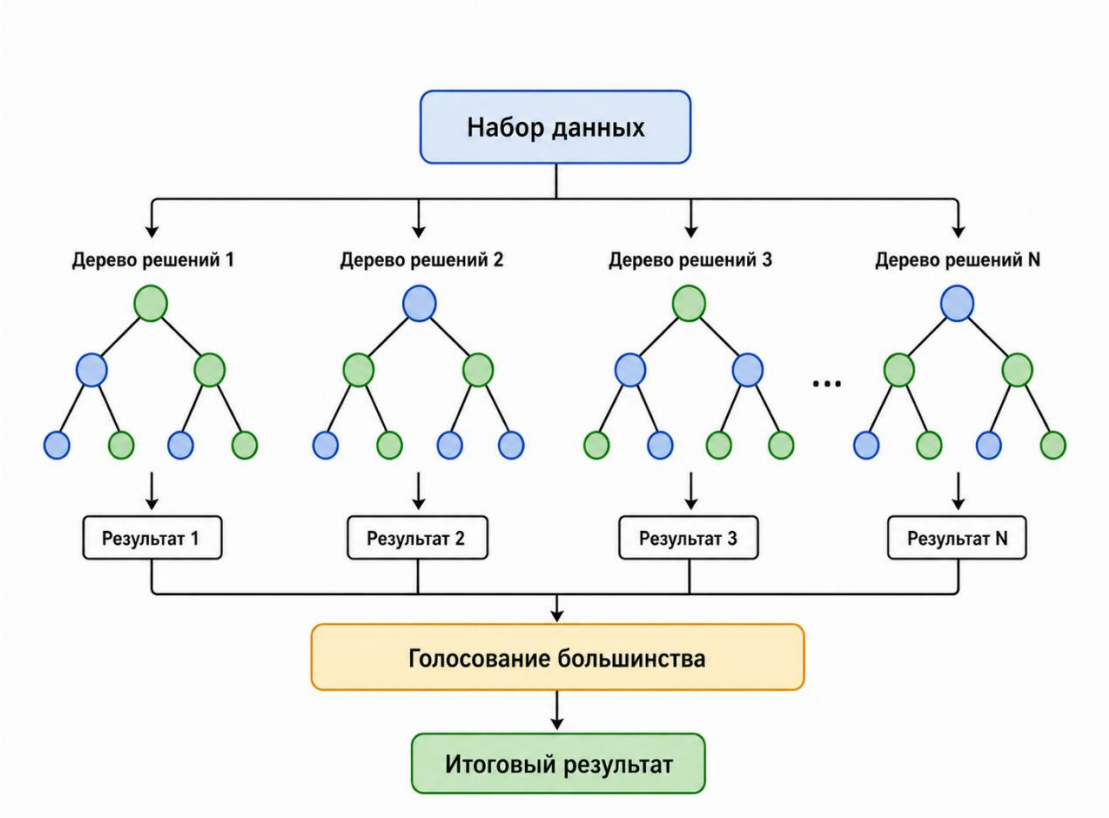


Рисунок 2.5 – Random Forest

Далее оценивалось, улучшает ли использование графовой структуры качество классификации. GNN формируют представление каждой транзакции, используя не только ее собственные признаки, но и признаки соседних транзакций, связанных с ней в графе [38]. Если GNN обеспечивает прирост при сопоставимом экспериментальном протоколе, это указывает на дополнительную полезность явного учета графовой структуры. Отсутствие прироста может быть связано как с наличием агрегированной информации в признаках Elliptic, так и с особенностями архитектуры и настройки графовой модели. Именно в этом состоит роль GNN в дальнейшем сравнении. Во всех экспериментах с GNN направленный граф преобразовывался в симметричный: к каждому ребру добавлялось обратное. В результате модель получала информацию от соседних транзакций в обоих направлениях.

Роль каждой группы моделей в экспериментальной логике главы обобщена в таблице 2.2.

Таблица 2.2 – Роль моделей в экспериментальной логике главы

Группа моделей	Модель	Роль в главе	Причина включения
Табличная базовая модель	Random Forest	сильная модель обучения с учителем	устойчив к нелинейным зависимостям и хорошо зарекомендовал себя на Elliptic [26], [21], [27]
Отбор признаков + классификация	GA + Random Forest	предложенный метод	проверяет, улучшает ли оберточный отбор качество по классу illicit [48]
Графовая базовая линия	GCN, SkipGCN	сопоставление с исходной графовой логикой Elliptic	использовались в исходном эксперименте или близки к нему [26]
Современные GNN	GraphSAGE, GAT, GGNN, GIN, JK-Net, APPNP, SGC, GCNII, PNA	проверка разных механизмов передачи сообщений	охватывают выборку соседей, механизмы внимания, рекуррентное обновление, остаточные связи, глубокое распространение информации и использование нескольких агрегаторов [39–40, 49, 50–55]

Выбранные модели позволяют сопоставить табличный подход с разными способами передачи информации по графу. В условиях анонимизированных признаков важны не только значения метрик, но и воспроизводимость эксперимента и сопоставимость результатов с ранее опубликованными исследованиями.

Метрики оценки при дисбалансе классов

Для Elliptic метрика accuracy не подходит для оценки модели, так как датасет несбалансирован: licit-транзакций значительно больше, чем illicit, примерно 9 к 1. Поэтому использовались другие классические метрики: precision, recall и F1-score. Эти метрики широко используются при работе с несбалансированными датасетами.

Обозначим через TP правильно найденные транзакции illicit, через FP транзакции licit, ошибочно отнесенные к illicit, через FN пропущенные транзакции illicit, через TN правильно распознанные транзакции licit.

Precision показывает, какая доля транзакций, отнесенных моделью к классу illicit, действительно имеет метку illicit (2.8):

$$Precision = \frac{TP}{TP + FP} \tag{2.8}$$

Recall отражает, какую долю транзакций класса illicit обнаружила модель (2.9):

$$Recall = \frac{TP}{TP + FN} \tag{2.9}$$

F1-score отражает общий баланс между precision и recall (2.10):

$$F1 - score = \frac{2 \times Precision \times Recall}{Precision + Recall} \tag{2.10}$$

Эти метрики также использовались в исходных экспериментах на Elliptic и других исследованиях [26]. Ошибки модели по-разному влияют на результаты анализа. Если нелегальная транзакция не обнаружена, она может не попасть на дальнейшую проверку. В другом случае модель принимает легальную транзакцию за нелегальную и направляет ее на дополнительный анализ, что увеличивает нагрузку на аналитиков.

2.3 Отбор признаков на основе генетического алгоритма

В наборах данных Elliptic и Elliptic++ много признаков, большинство из которых анонимизировано. Из-за этого часть характеристик может дублировать уже имеющуюся информацию или вносить шум. Поэтому применяется отбор признаков, при котором сохраняются характеристики, наиболее полезные для модели. Для отбора признаков используется генетический алгоритм (GA) [48].

Генетический алгоритм выполняет стохастический поиск, опираясь на принципы эволюционного отбора [56, 57]. Вместо полного перебора он

работает с популяцией возможных решений и обновляет ее с помощью селекции, кроссовера и мутации. В задаче отбора признаков каждая особь задает собственный набор переменных. При d признаках существует 2^d возможных подмножеств. Для Elliptic это 2^{166} вариантов, а для Elliptic++ это 2^{183} вариантов. Полный перебор здесь не имеет практического смысла, поскольку каждый набор пришлось бы отдельно проверять обучением модели. В работе поиск ведется по ограниченной популяции решений, состав которой меняется от поколения к поколению.

Одно решение кодируется бинарной хромосомой (2.11):

$$z = (z_1, \dots, z_d), \quad z_j \in \{0,1\}, \tag{2.11}$$

где $z_j = 1$ означает, что $j-$ й признак включен в набор, а $z_j = 0$ исключает его.

По хромосоме z формируется подмножество (2.12):

$$S(z) = \{j \mid z_j = 1\}, \tag{2.12}$$

где $S(z)$ содержит индексы признаков, включенных хромосомой. Пример такого кодирования приведен на рисунке 2.6. Единица сохраняет соответствующий признак, а ноль исключает его из набора.

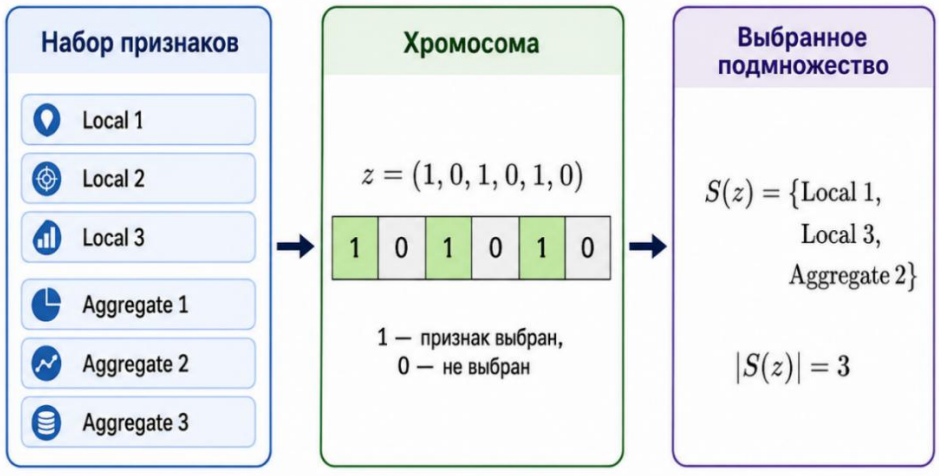


Рисунок 2.6 – Кодирование подмножества признаков бинарной хромосомой

Число выбранных признаков заранее не фиксируется. Оно зависит от количества единиц в конкретной хромосоме и может меняться в ходе поиска. Для Elliptic это оправдано тем, что семантика большинства переменных скрыта. Заранее определить, какие из них связаны с поведением транзакции, а какие повторяют уже имеющуюся информацию, нельзя. Кроме того, слабый по отдельности признак может оказаться полезным в сочетании с другими.

Начальная популяция включала 250 случайных бинарных масок [48]. Для каждой непустой хромосомы Random Forest обучался на выбранных столбцах

внутренней обучающей части, а затем проверялся на валидационной. Если маска не содержала ни одного признака, классификатор не обучался и хромосоме присваивалась нулевая пригодность:

$$Fitness(z) = F1_{illicit}\big(y_{val}, \hat{y}_{val}(z)\big), \quad (2.13)$$

где y_{val} содержит реальные метки, а $\hat{y}_{val}(z)$ обозначает прогноз Random Forest на признаках, выбранных хромосомой z. Пустой маске присваивается нулевая пригодность. Количество выбранных признаков в функцию пригодности не входило и отдельно не минимизировалось.

Такой способ относится к оберточному отбору признаков [58]. Фильтрационные методы обычно оценивают переменные по одной и работают быстрее, но могут не заметить полезное взаимодействие между ними. Встроенный отбор опирается на внутренний механизм конкретной модели [28]. Здесь набор сравнивается по фактическому результату Random Forest, поэтому в оценку попадает совместное действие всех признаков маски. У этого решения есть цена: классификатор приходится обучать многократно, а найденное подмножество связано с выбранной моделью, метрикой и способом разделения данных.

Для сравнения использовался фильтрационный метод SelectKBest. Признаки ранжировались по критерию *f_classif*, основанному на однофакторной ANOVA F-статистике и оценивающему каждый признак независимо от остальных переменных. Для Elliptic сохранялись 53 признака, а для Elliptic++ – 85, то есть столько же, сколько было выбрано генетическим алгоритмом. Отбор выполнялся без использования тестовых временных срезов.

После оценки популяции родительские хромосомы выбирались турнирной селекцией. В каждом турнире случайно сравнивались три маски, и преимущество получала хромосома с более высоким F1-score. Состав турниров менялся, поэтому решения с меньшей оценкой не исключались из поиска сразу и могли участвовать в последующих выборах.

К выбранной паре применялся двухточечный кроссовер с вероятностью 0,9. Две позиции задавали границы участка, которым обменивались родительские маски. Так в одном потомке могли соединиться, например, локальные характеристики транзакции из одного решения и агрегированные признаки окружения из другого. После кроссовера новая хромосома проходила полную оценку с повторным обучением Random Forest [48].

Мутация применялась к хромосоме с вероятностью 0,2. Если оператор срабатывал, каждый бит инвертировался независимо с вероятностью 0,05. Переход из 0 в 1 возвращал признак в набор, а переход из 1 в 0 исключал его. При заданной вероятности мутация обычно затрагивала небольшую часть маски [48].

Селекция, двухточечный кроссовер, побитовая мутация, а также повторная оценка формировали одно поколение. Поиск выполнялся в течение 100 поколений [48]. Лучшее решение сохранялось отдельно на протяжении всего запуска. После каждого поколения его значение функции

приспособленности сравнивалось с наилучшим значением, полученным ранее. Для итогового обучения выбиралась хромосома с наибольшим F1-score за все поколения. Схема GA+Random Forest показана на рисунке 2.7.

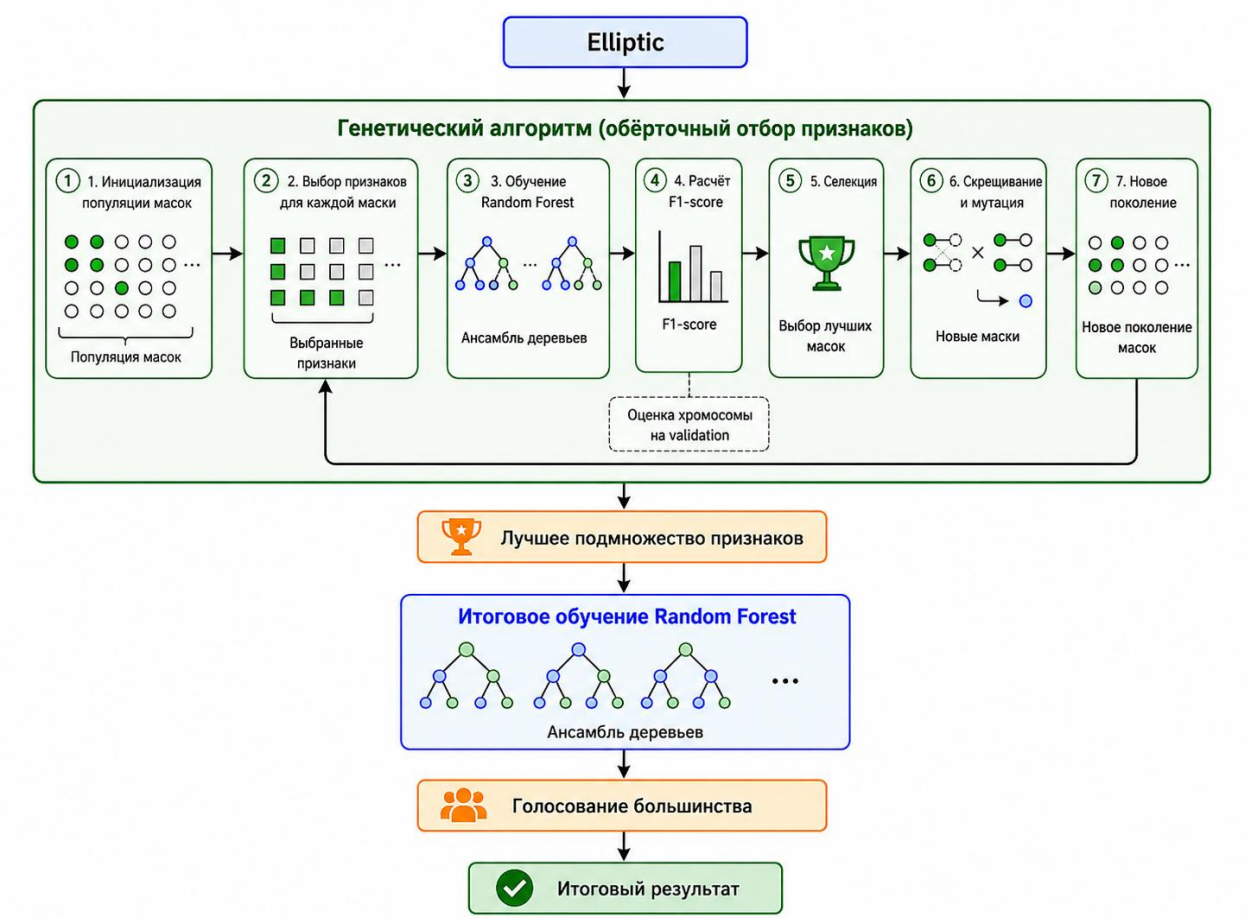


Рисунок 2.7 – Схема предложенного метода отбора признаков и классификации

Параметры итогового запуска подбирались эмпирическим путем. Использованная конфигурация приведена в таблице 2.3.

Таблица 2.3 – Конфигурация генетического алгоритма отбора признаков

Параметр	Значение	Назначение
Кодировка особи	бинарная маска	включение или исключение каждого признака
Оценочная модель	Random Forest, 100 деревьев, max_features = "sqrt"	оценка маски по F1-score класса illicit
Размер популяции	250	число хромосом в одном поколении
Число поколений	100	число циклов обновления популяции
Селекция	турнирная	выбор родительских хромосом

Продолжение таблицы 2.3

Размер турнира	3	число масок, сравниваемых при одном выборе
Кроссовер	двухточечный	обмен участком между родительскими масками
Вероятность кроссовера	0,9	вероятность применения оператора к родительской паре
Мутация	побитовая инверсия	изменение отдельных позиций бинарной маски
Вероятность мутации хромосомы	0,2	вероятность применения оператора к особи
Вероятность изменения бита	0,05	вероятность инверсии каждого бита при мутации
Пустая маска	пригодность 0	Random Forest не обучается без выбранных признаков
Сохранение лучшего решения	лучшее за все поколения	фиксация глобально лучшей хромосомы

Также GA был применен для Elliptic++. В обоих экспериментах генетический отбор выполнялся отдельно и использовались одинаковые параметры генетического алгоритма и Random Forest. Лучшая маска определялась независимо для каждого набора данных. Для генетического поиска контроль временной утечки особенно важен. Если использовать поздние транзакции при расчете пригодности, алгоритм начнет подбирать маски непосредственно под будущую тестовую выборку. Поэтому GA имел доступ только к шагам 1–34. На данных временных шагов 1–34 выполнялись обучение моделей и отбор признаков, а шаги 35–49 оставались закрытыми до финальной оценки. Те же границы соблюдались при настройке моделей и выборе порога. Порядок доступа к данным по всем этапам приведен в таблице 2.4.

Таблица 2.4 – Использование данных и контроль информационной утечки на этапах эксперимента

Этап	Процедура	Используемые данные	Как контролируется
Отбор признаков GA	Функция пригодности оценивается с использованием внутреннего разделения обучающей области	t=1–34	срезы t=35–49 недоступны для GA

Продолжение таблицы 2.4

Подбор моделей	Гиперпараметры подбираются и проверяются внутри обучающей области	t=1–34 с внутренним разделением на обучение и валидацию	тестовая часть не используется для настройки параметров модели
Порог классификации	Порог определяется внутри обучающей области до финального тестирования	внутренняя валидационная часть $t = 1–34$	тестовые срезы не используются для выбора порога
Финальная оценка	Рассчитываются Precision, Recall и F1-score на поздних временных срезах	test: $t = 35–49$	независимая проверка модели

2.4 Результаты экспериментов

Результаты предложенного метода GA+Random Forest

Благодаря генетическому алгоритму количество признаков Elliptic сократилось с 166 до 53. В итоговый набор вошли 27 локальных признаков и 26 агрегированных признаков соседних транзакций, или 31,9% исходного набора. Для Elliptic++ число признаков сократилось со 183 до 85, или до 46,4% исходного набора. Итоговое подмножество Elliptic++ включало 44 локальных, 36 агрегированных и пять дополнительных признаков. Результаты генетического отбора для обоих наборов данных представлены в таблице 2.5.

Таблица 2.5 – Результат отбора признаков генетическим алгоритмом для Elliptic и Elliptic++

Набор данных	Группа признаков	Исходное количество	Отобрано GA	Доля от исходной группы
Elliptic	локальные признаки	94	27	28,7%
Elliptic	агрегированные признаки	72	26	36,1%
	Всего	166	53	31,9%
Elliptic++	локальные признаки	94	44	46,8%
Elliptic++	агрегированные признаки	72	36	50,0%
Elliptic++	Дополнительные признаки	17	5	29,4%
	Всего	183	85	46,4%

На наборе Elliptic Random Forest на всех 166 признаках достиг F1-score 82,90%, а SelectKBest при сохранении 53 признаков показал F1-score 78,77%.

Предложенный метод GA+Random Forest при том же количестве признаков обеспечил F1-score 84,26%. Прирост относительно полного набора составил 1,36 п. п., а относительно SelectKBest – 5,49 п. п.

На наборе Elliptic++ Random Forest на всех 183 признаках достиг F1-score 82,50%, SelectKBest при сохранении 85 признаков – 80,65%, а GA+Random Forest – 84,07%. Прирост относительно полного набора составил 1,57 п. п., а относительно SelectKBest составил 3,42 п. п. Метрики приведены в таблице 2.6.

Таблица 2.6 – Сравнение способов формирования признакового набора

Набор данных	Способ формирования признаков	Число признаков	Precision	Recall	F1-score
Elliptic	Все признаки	166	97,15%	72,30%	82,90%
Elliptic	SelectKBest	53	86,52%	72,30%	78,77%
Elliptic	GA	53	99,37%	73,13%	84,26%
Elliptic++	Все признаки	183	96,54%	72,02%	82,50%
Elliptic++	SelectKBest	85	92,69%	71,38%	80,65%
Elliptic++	GA	85	99,37%	72,85%	84,07%

Таким образом, преимущество предложенного метода связано не только с сокращением признаков. При одинаковом числе признаков GA обеспечил более высокий F1-score, чем SelectKBest, поскольку оценивал подмножества совместно в модели Random Forest, а не ранжировал признаки по отдельности. Изменение F1-score относительно полного набора с учетом доли сохраненных признаков показано на рисунке 2.8.

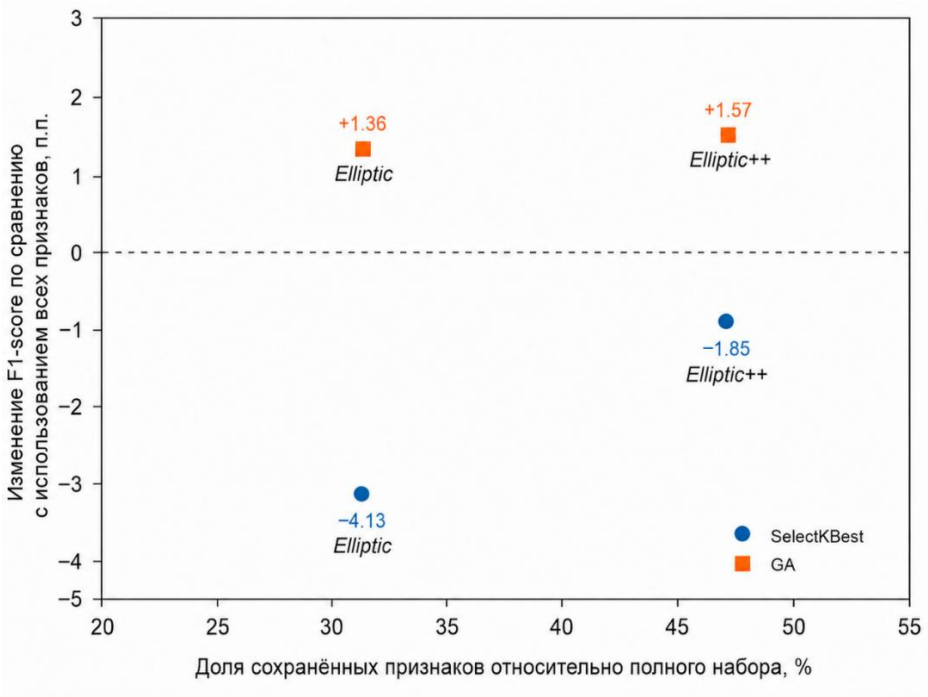


Рисунок 2.8 – Соотношение доли сохраненных признаков и изменения F1-score относительно полного набора

Результаты GA+Random Forest на Elliptic и Elliptic++ различались незначительно: precision остался на уровне 99,37%, recall снизился на 0,28 п. п., а F1-score снизился на 0,19 п. п. Продолжительность генетического поиска составила 41 час для Elliptic и 51 час для Elliptic++ [48]. Сравнение результатов показано на рисунке 2.9.

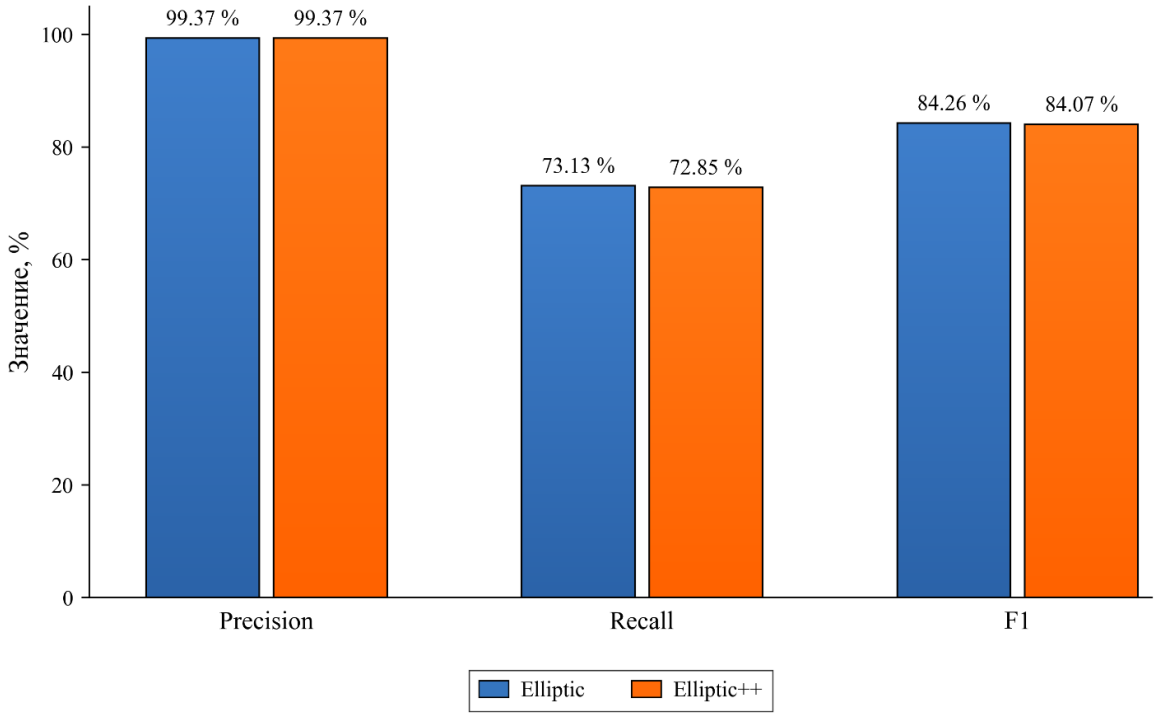


Рисунок 2.9 – Сравнение метрик Precision, Recall и F1-score для Elliptic и Elliptic++

Таким образом, расширение датасета с 166 признаков Elliptic до 183 признаков Elliptic++ не привело к повышению качества ни при использовании полного набора признаков, ни после генетического отбора. В рамках примененного экспериментального протокола дополнительные 17 признаков не обеспечили повышения качества классификации.

Результаты графовых моделей

Также были проверены графовые модели GCN, SkipGCN, GraphSAGE, GAT, GGNN, GIN, JK-Net, APPNP, SGC, GCNII и PNA. Эти архитектуры охватывают разные способы работы с графовой структурой: сверточное агрегирование, выборку соседей, механизм внимания, рекуррентное обновление, остаточные связи, глубокое распространение и многоканальную агрегацию. GNN-эксперименты выполнялись по временному протоколу и правилам работы с разметкой, описанным в разделе 2.2. Во всех случаях использовались 166 признаков Elliptic. Результаты сравнения GNN-архитектур приведены в таблице 2.7.

Таблица 2.7 – Результаты GNN-архитектур на Elliptic

Модель	Precision	Recall	F1-score	Интерпретация
GCNII	91,65%	55,77%	69,35%	наибольший F1-score среди GNN
GraphSAGE	77,22%	59,46%	67,19%	наиболее близкие значения precision и recall среди ведущих GNN
PNA	92,73%	51,80%	66,47%	высокое значение precision, низкое значение recall
JK-Net	88,39%	51,34%	64,95%	ограниченная полнота
GGNN	96,61%	47,37%	63,57%	высокое значение precision, низкое значение recall
SkipGCN	79,89%	51,34%	62,51%	умеренный результат
GCN	76,48%	50,14%	60,57%	базовая графовая свертка
SGC	69,89%	50,78%	58,82%	упрощенная модель
GIN	68,95%	50,23%	58,12%	низкий F1-score
GAT	34,63%	67,59%	45,79%	высокое значение recall, низкое значение precision
APPNP	35,95%	42,66%	39,02%	наименьший F1-score

Результаты GNN различались по соотношению precision и recall. Модели GCNII и PNA реже относили легальные транзакции к нелегальным, но пропускали значительную часть нелегальных транзакций. У других архитектур повышение recall сопровождалось снижением precision. Для итогового сравнения выбраны три GNN-модели с наиболее высокими значениями F1-score. Их результаты вместе с показателями GA+Random Forest приведены в таблице 2.8.

Таблица 2.8 – Сводное сравнение основных моделей

Модель	Precision illicit	Recall illicit	F1-score illicit
GA+Random Forest	99,37%	73,13%	84,26%
GCNII	91,65%	55,77%	69,35%
GraphSAGE	77,22%	59,46%	67,19%
PNA	92,73%	51,80%	66,47%

В проведенном эксперименте все исследованные GNN-архитектуры уступили предложенному методу GA+Random Forest. Наиболее высокий результат среди GNN показала GCNII с F1-score 69,35%, что на 14,91 п. п. ниже результата GA+Random Forest. Примерно такое же преимущество табличных моделей над отдельными графовыми конфигурациями наблюдалось и в исходном benchmark Elliptic [26]. Это может объясняться составом исходных признаков, в котором 72 агрегированных признака уже содержат сведения о соседних транзакциях.

Сравнение с предыдущими исследованиями

Сравнивать результаты предложенной модели с ранее опубликованными исследованиями можно только при близких условиях эксперимента. Прямое сравнение возможно с работами на исходном Elliptic, где используются классы licit и illicit и сохранено временное разделение данных. Для сравнения были отобраны не все работы, использующие Elliptic или Elliptic++, а исследования, наиболее близкие по методологии: постановке задачи классификации licit/illicit, режиму разбиения данных, учету временной структуры, работе с частичной разметкой и используемым метрикам. Такой отбор позволяет избежать некорректного сравнения моделей, обученных в существенно разных условиях, и сосредоточиться на подходах, сопоставимых по данным, разметке и логике экспериментальной проверки.

Оценка эффективности предложенного метода проводится по двум направлениям. Первое основано на контролируемом сравнении с Random Forest на полном наборе признаков и фильтрационным методом SelectKBest в рамках единого экспериментального протокола. Результаты приведены в таблице 2.6. Такое сравнение позволяет оценить непосредственный вклад генетического отбора признаков. Второе направление включает сопоставление с опубликованными результатами на наборах данных Elliptic и Elliptic++, приведенное в таблице 2.9, и позволяет оценить конкурентоспособность предложенного метода относительно известных подходов.

Таблица 2.9 – Сравнение с исследованиями на Elliptic и Elliptic++

Источник	Датасет	Подход	Результат	Ограничение
Weber et al. (2019) [26]	Elliptic	RF	P=95,6%, R=67,0%, F1=78,8%	исходный эксперимент, признаки анонимизированы
Weber et al. (2019) [26]	Elliptic	RF+GCN-эмбеддинги	P=97,1%, R=67,5%, F1=79,6%	исходный эксперимент, признаки анонимизированы
Alarab et al. (2020) [27]	Elliptic	ансамбль RF, Extra Trees, Bagging	P=99,11%, R=71,93%, F1=83,36%	акцент на supervised ensemble, признаки анонимизированы
Alarab et al. (2020) [59]	Elliptic	гибридная GCN + MLP	P=89,9%, R=67,8%, F1=77,3%	условия GNN могут отличаться
Lorenz et al. (2020) [60]	Elliptic	активное обучение + RF	5% размеченных данных достигают уровня supervised baseline	фокус на дефиците меток, а не максимальной F1
Lo et al. (2023) [35]	Elliptic	Inspection-L: DGI + GIN + RF	P=97,2%, R=72,1%, F1=82,8%	самообучаемые представления

Продолжение таблицы 2.9

Elmougy, Liu (2023) [21]	Elliptic++	RF + отбор признаков	P=98,6%, R=72,7%, F1=83,6%	расширенный набор данных не полностью тождественен Elliptic
Предложенный метод	Elliptic	признаки, отобранные GA + RF	P=99,37%, R=73,13%, F1=84,26%	высокая вычислительная стоимость, признаки анонимизированы
Предложенный метод	Elliptic++	признаки, отобранные GA + RF	P=99,37%, R=72,85%, F1=84,07%	высокая вычислительная стоимость, признаки анонимизированы

Наиболее близкими к текущей постановке на наборе Elliptic являются работы Weber et al. [26] и Alarab et al. [27], поскольку в них используется сходная схема supervised-классификации транзакций licit/illicit. Для сопоставления результатов на расширенном наборе Elliptic++ рассматривается работа Elmougy и Liu [21].

В исследовании Weber et al. Random Forest на всех 166 признаках достиг F1-score 78,8%, а при добавлении GCN-эмбеддингов узлов 79,6%. Результат предложенной модели GA+Random Forest на Elliptic, равный 84,26%, выше этих показателей на 5,46 и 4,66 п. п. соответственно. По сравнению с ансамблевой моделью Alarab et al., для которой F1-score составил 83,36%, разница достигает 0,90 п. п. На наборе Elliptic++ предложенный метод получил F1-score 84,07%, что на 0,47 п. п. выше результата Elmougy и Liu, равного 83,6%. Различие между собственным результатом на полном наборе признаков и результатом Weber et al. может быть связано с разными настройками модели: числом деревьев и параметром max_features.

Совокупность внутреннего сравнения и сопоставления с опубликованными исследованиями позволяет считать предложенный метод GA+Random Forest конкурентоспособным среди рассмотренных подходов. Его значение состоит не в утверждении универсального превосходства над всеми существующими моделями, а в том, что оберточный отбор признаков внутри временно корректного протокола позволяет сократить признаковое пространство и повысить качество выявления класса illicit без применения явного механизма передачи сообщений по графу.

Полученные результаты позволяют сформулировать более общий методологический вывод. В задачах анализа Bitcoin-транзакций качество модели зависит не только от архитектуры, но и от того, какая информация уже включена в признаки, как устроено временное разбиение, как обрабатываются неизвестные метки и насколько строго исключена утечка тестовой информации. Поэтому простое сопоставление чисел F1-score без анализа протокола может приводить к неверной оценке преимуществ той или иной модели.

2.5 Интерпретация результатов и ограничения исследования

Матрица ошибок показывает распределение правильных и ошибочных прогнозов GA+Random Forest на наборе Elliptic. Из 1 083 транзакций класса illicit модель правильно классифицировала 792, а 291 отнесла к классу licit. Среди 15 587 транзакций класса licit пять были ошибочно классифицированы как illicit, остальные 15 582 распознаны правильно. Матрица ошибок представлена на рисунке 2.10.

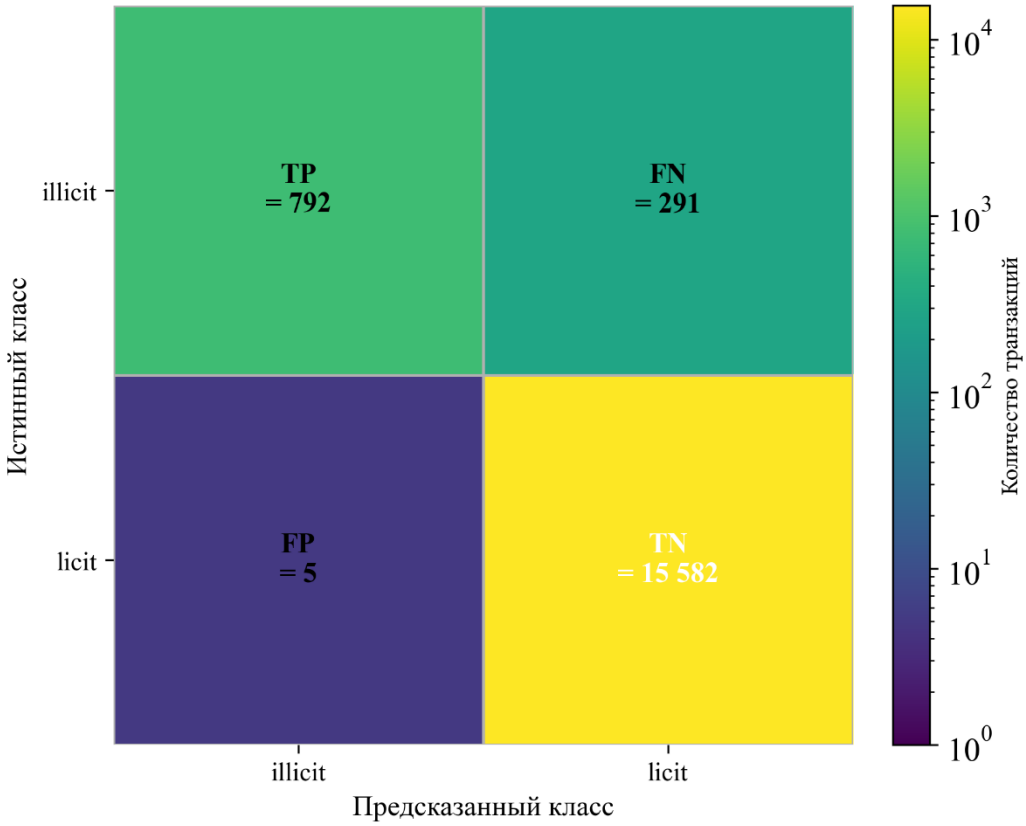


Рисунок 2.10 – Матрица ошибок итоговой модели Random Forest с генетическим отбором признаков на Elliptic

Этим объясняется сочетание очень высокого precision с более умеренным recall. Модель почти не допускает ложных срабатываний, но пропускает примерно четверть размеченных нелегальных транзакций.

В задаче анализа Bitcoin-транзакций это важно: такие операции могут не попасть в очередь экспертной проверки. Но механическое повышение recall за счет резкого снижения precision также нежелательно, поскольку оно увеличивает число ложных срабатываний и создает избыточную нагрузку на аналитиков. Поэтому модель следует рассматривать как средство предварительной проверки, а не как окончательное решение о правовой природе транзакции.

Ложное срабатывание может означать, что легальная транзакция похожа на нелегальную по анонимизированному признаковому профилю. В

прикладном анализе такой случай требует проверки по дополнительным данным: адресной истории, связям с сервисами, временной динамике, суммам, цепочкам переводов и внешним источникам. Пропуск нелегальных транзакций, напротив, может указывать на то, что часть противоправного поведения не отражена в доступных признаках Elliptic либо меняется во времени.

Главное ограничение интерпретации связано с анонимизацией признаков. Важность признаков и SHAP-значения позволяют оценить вклад переменных в решение модели [41, 47]. Пример такой визуализации представлен на рисунке 2.11. Однако в случае Elliptic они не дают полноценного криминалистического объяснения, поскольку семантика признаков скрыта. Вывод вида «local_feature_61 повышает вероятность класса illicit» полезен для анализа поведения модели, но сам по себе не объясняет, какой именно транзакционный механизм за этим стоит, то есть не раскрывает реальную экономическую или криминалистическую природу соответствующих переменных.

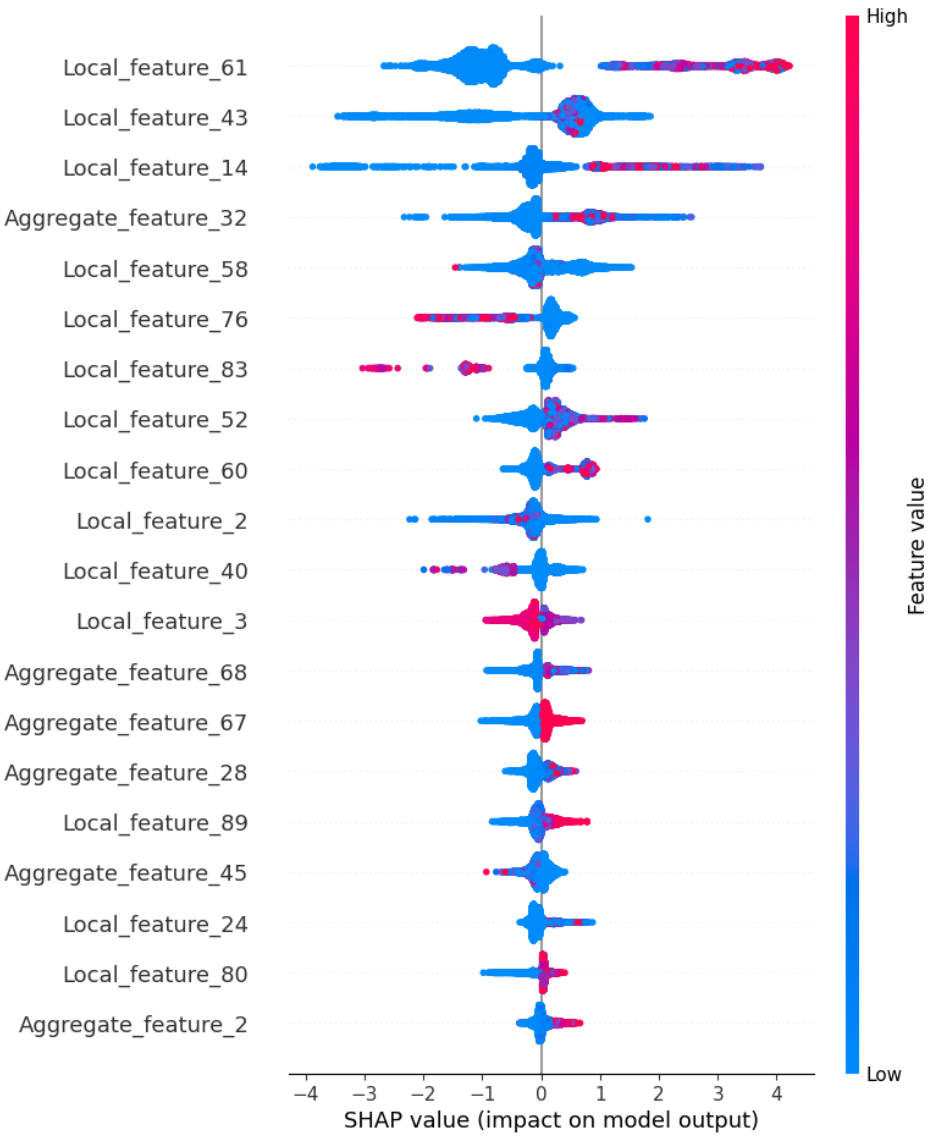


Рисунок 2.11 – SHAP-анализ

Отдельное ограничение связано с частичной разметкой Elliptic.

Значительная часть транзакций имеет статус unknown и не участвует в оценке качества моделей в задаче обучения с учителем. Поэтому значения precision, recall и F1-score отражают качество классификации только на размеченной части графа.

Кроме того, следует отметить высокую вычислительную стоимость генетического отбора признаков. Для оценки каждой комбинации признаков Random Forest обучался заново. При размере популяции 250 особей и выполнении 100 поколений эту процедуру приходилось повторять многократно, что значительно увеличивало продолжительность поиска.

Генетический алгоритм имеет стохастическую природу, поэтому состав найденного подмножества может зависеть от начальной популяции и последовательности применения генетических операторов. В настоящем исследовании устойчивость состава признаков по нескольким независимым запускам отдельно не оценивалась из-за высокой вычислительной стоимости.

2.6 Выводы по разделу 2

Во второй главе были исследованы методы машинного обучения для выявления нелегальных Bitcoin-транзакций на данных Elliptic. Наилучший результат среди проверенных конфигураций показала модель Random Forest с генетическим отбором признаков. При выявлении нелегальных транзакций значения precision, recall и F1-score составили 99,37%, 73,13% и 84,26% соответственно.

Научная новизна результатов главы состоит в предложенном методе отбора признаков для блокчейн-наборов данных с анонимизированными признаками, основанном на генетическом поиске подмножеств признаков и их обёрточной оценке моделью Random Forest по F1-score нелегального класса. Применение предложенного метода к набору Elliptic сократило число признаков со 166 до 53 и в рамках контролируемого эксперимента повысило F1-score с 82,90 до 84,26%. При одинаковом количестве признаков метод SelectKBest достиг F1-score 78,77%. Полученные значения precision, recall и F1-score предложенного метода также выше опубликованных показателей модели RF+GCN из исходного benchmark Elliptic соответственно на 2,3, 5,6 и 4,7 п. п.

Несмотря на высокие значения метрик, анонимизация признаков делает невозможным практическое применение модели для анализа реальных Bitcoin-транзакций. Модель различает классы licit и illicit только в пределах разметки Elliptic, но не показывает, какие наблюдаемые характеристики транзакции повлияли на результат. Из-за этого аналитик не может содержательно проверить и обосновать полученное решение. По этой причине в следующей главе используются открытые и интерпретируемые характеристики Bitcoin-транзакций: транзакционные и структурно-графовые признаки, признаки локального отклонения от окружения, временные признаки последующего расходования и признаки предшествующей транзакционной истории.

3 РАЗРАБОТКА КРИМИНАЛИСТИЧЕСКИ ИНТЕРПРЕТИРУЕМЫХ ПРИЗНАКОВ И МОДЕЛИ ВЫЯВЛЕНИЯ НЕЛЕГАЛЬНЫХ BITCOIN-ТРАНЗАКЦИЙ

В данной главе описывается подход к решению проблемы классификации Bitcoin-транзакций. Для этого создается новый расширенный датасет на основе Elliptic, но уже с открытыми и доступными признаками. На основе анализа известных случаев перемещения нелегальных средств, связанных со взломами, мошенничеством, вымогательством и иными видами противоправной деятельности, разработаны три группы криминалистически интерпретируемых признаков. Они дополняют базовые транзакционные и структурно-графовые характеристики. Признаки рассчитываются по открытым данным блокчейна, привязываются к определенному временному срезу и допускают содержательную интерпретацию через параметры транзакции, ее связи и движение средств. Модельные и поведенческие индикаторы рассматриваются вместе с контекстом транзакций и доступными сведениями об атрибуции [2, 12].

Эффективность подхода оценена на ансамблевых моделях. Дополнительно проведены абляционный анализ, интерпретация важности признаков, оценка вычислительной эффективности и анализ ошибок предложенного подхода.

3.1 Формирование интерпретируемого набора данных

Исходная структура Elliptic и ограничение анонимизированных признаков

Поскольку структура датасета Elliptic и его признаки уже рассмотрены в главе 2, здесь датасет используется как основа для формирования нового интерпретируемого датасета. Из исходного набора сохраняются идентификаторы транзакций, связи между ними, временные срезы и метки licit, illicit и unknown. Все 166 анонимизированных признаков исключаются из обучения, поскольку их содержательный смысл не раскрыт и не допускает прямой криминалистической интерпретации. Такое решение сохраняет графовую структуру и разметку Elliptic, но заменяет анонимные признаки local_feature_37 и aggregate_feature_12 признаками, полученными из открытых блокчейн-данных. Фрагмент исходного набора анонимизированных признаков Elliptic приведен на рисунке 3.1.

	txId	Local_feature_1	Local_feature_2	Local_feature_3	Local_feature_4	Local_feature_5	Local_feature_6	Local_feature_7	Local_feature_8	Local_feature_9
0	232438397	0.163054	1.963790	-0.646376	12.409294	-0.063725	9.782742	12.414558	-0.163645	-0.115831
1	232029206	-0.005027	0.578941	-0.091383	4.380281	-0.063725	4.667146	0.851305	-0.163645	-0.144554
2	232344069	-0.147852	-0.184668	-1.201369	-0.121970	-0.043875	-0.113002	-0.061584	-0.137933	-0.144108
3	27553029	-0.151357	-0.184668	-1.201369	-0.121970	-0.043875	-0.113002	-0.061584	-0.141519	-0.147643
4	3881097	-0.172306	-0.184668	-1.201369	0.028105	-0.043875	-0.029140	0.242712	-0.163640	-0.169115
5	232457116	-0.172304	-0.184668	-1.201369	-0.046932	-0.024025	-0.029140	-0.061584	-0.163637	-0.168783
6	232412405	-0.165140	-0.184668	-1.201369	-0.121970	-0.043875	-0.113002	-0.061584	-0.155621	-0.161548
7	232470342	-0.172350	-0.155133	0.463609	0.328255	-0.043875	0.390171	-0.061584	-0.163645	-0.169226
8	230550393	0.028482	0.048298	-1.201369	1.678931	-0.063725	1.564243	-0.061584	-0.163639	-0.084762
9	232051089	-0.172914	-0.184668	-1.201369	-0.046932	-0.024025	-0.029140	-0.061584	-0.163639	-0.169397
10	232470704	-0.172900	-0.184668	-1.201369	0.028105	-0.043875	0.054722	-0.061584	-0.163645	-0.169396
11	232033533	-0.156114	-0.184668	-1.201369	-0.046932	-0.043875	-0.029140	-0.061584	-0.161356	-0.154700
12	230473487	-0.172290	-0.184668	-1.201369	-0.046932	-0.043875	-0.029140	-0.061584	-0.163582	-0.168824
13	7089694	-0.157608	-0.181768	0.463609	0.328255	-0.043875	0.390171	-0.061584	-0.163612	-0.159833
14	231179595	-0.172729	-0.184668	-1.201369	-0.046932	-0.024025	-0.029140	-0.061584	-0.163634	-0.169215
15	231177927	-0.171669	-0.184668	-1.201369	0.028105	-0.043875	0.054722	-0.061584	-0.163635	-0.168435
16	2758467	0.092328	1.239009	-0.646376	8.207194	-0.063725	8.608671	1.155601	-0.163645	-0.103495
17	232437171	-0.167243	-0.115037	-0.091383	0.403293	-0.043875	0.474034	-0.061584	-0.163645	-0.166505
18	3878886	-0.172886	-0.184668	-1.201369	-0.046932	-0.043875	-0.029140	-0.061584	-0.163639	-0.169368
19	231182296	-0.172310	-0.184668	-1.201369	-0.046932	-0.024025	-0.029140	-0.061584	-0.163640	-0.168787
20	14660781	-0.172771	-0.184668	-1.201369	-0.046932	-0.024025	-0.029140	-0.061584	-0.163641	-0.169251

Рисунок 3.1 – Фрагмент исходной таблицы анонимизированных признаков датасета Elliptic

Формирование начинается с сопоставления внутренних идентификаторов Elliptic с публичными хэшами Bitcoin-транзакций. Для этого использован опубликованный набор данных «Deanonymized 99.5 pct of Elliptic transactions», содержащий соответствие между идентификаторами Elliptic и публичным txid примерно для 99,5% вершин графа [61]. В результате сопоставления публичные идентификаторы были установлены для 202 804 из 203 769 транзакций. Для остальных 965 транзакций соответствующие txid отсутствовали, поэтому они были исключены из дальнейшего анализа.

После восстановления идентификаторов для транзакций были собраны открытые ончейн-характеристики. С помощью Blockchair API извлекались высота блока, комиссия, число входов и выходов, размер транзакции, суммы входов и выходов и другие доступные параметры Bitcoin-транзакций [62]. Эти характеристики составили базовый набор признаков. В отличие от исходных анонимизированных переменных, каждый его признак имеет содержательное объяснение и может быть проверен по данным блокчейна.

На следующем этапе по восстановленному графу и данным блокчейна рассчитывались производные признаки: структурные характеристики вершины, признаки локального отклонения от окружения, временные признаки последующего расходования и признаки предшествующей транзакционной истории. Базовый набор содержит характеристики транзакций, восстановленные по данным блокчейна, а расширенный включает те же признаки вместе с дескрипторами, имеющими криминалистическую интерпретацию.

Расширение разметки

Часть транзакций со статусом unknown была проверена через сервис Crystal Intelligence, который используется при расследовании и анализе Bitcoin-транзакций [63]. Оригинальные метки licit и illicit не менялись. Для ранее неразмеченной транзакции внешняя метка проставлялась только при однозначной атрибуции в Crystal Intelligence к категории licit или illicit, то есть если имеющаяся информация не позволяла однозначно определить, является транзакция легальной или нелегальной, то метка оставалась unknown.

Благодаря такой проверке удалось присвоить метки 2 304 транзакциям. Из них 2 187 были отнесены к licit, еще 117 отнесены к illicit. Общее число размеченных транзакций достигло 48 239, в том числе 43 588 licit и 4 651 illicit. У остальных 154 565 транзакций статус unknown сохранился. Эти данные исключались из обучения с учителем и расчета метрик, но оставались в графе при построении структурных признаков. Их удаление изменило бы значения PageRank, степени вершин, размеры компонент, состав локальных соседств и цепочки происхождения средств. Порядок сопоставления исходной и внешней разметки представлен в таблице 3.1.

Таблица 3.1 – Правила согласования исходной и внешней разметки

№	Исходная метка Elliptic	Внешняя оценка Crystal	Правило	Итоговая метка	Количество
1	licit	не проверялась	сохраняется исходная метка	licit	41 401
2	illicit	не проверялась	сохраняется исходная метка	illicit	4 534
3	unknown	явная licit-атрибуция	перенос метки из Crystal	licit	2 187
4	unknown	явная illicit-атрибуция	перенос метки из Crystal	illicit	117
5	unknown	неоднозначная / промежуточная / отсутствует	сохраняется unknown	unknown	154 565

Представление данных как 49 согласованных графовых срезов

При работе с набором Elliptic важно учитывать, что характер Bitcoin-транзакций меняется со временем. Хотя значения исходных признаков анонимизированы, они отражают особенности операций и связей между транзакциями в конкретный период. Например, в исходном исследовании снижение качества классификации на поздних временных шагах связывалось с закрытием теневого рынка [26]. После таких событий меняются частота и объемы переводов, состав связанных транзакций и маршруты средств. Поэтому признаки, полезные для ранних периодов, могут хуже работать на более поздних данных. По этой причине в стандартном протоколе Elliptic модель

обучается на временных шагах 1–34 и тестируется на шагах 35–49. Случайное распределение отдельных транзакций между выборками могло бы привести к смешиванию разных периодов и завышенной оценке качества.

В данном эксперименте решалась другая задача: модели обучались на транзакциях одних временных графов и проверялись на транзакциях других графов, не использованных при обучении. Такой подход учитывает графовую структуру Bitcoin-транзакций и позволяет оценить способность моделей сохранять качество классификации при переходе к новым графам, а не только к отдельным ранее не наблюдавшимся транзакциям.

Для каждого из 49 временных периодов строился отдельный граф. Каждый граф целиком включался либо в обучающую, либо в тестовую выборку. Это исключало попадание транзакций одного периода одновременно в обе выборки. Графовые признаки рассчитывались только по транзакциям и связям соответствующего периода. Конкретная схема формирования обучающей и тестовой частей приведена в подразделе «Экспериментальный дизайн».

3.2 Базовые и структурно-графовые признаки Bitcoin-транзакций

Во всех формулах v обозначает рассматриваемую транзакцию, а t обозначает временной срез транзакционного графа.

Базовые транзакционные признаки

Базовые признаки описывают параметры самой транзакции: суммы входов и выходов, структуру входов и выходов, размер, комиссию, концентрацию средств и временные интервалы. Максимальные и медианные значения, число адресов и размер транзакции относятся к стандартным характеристикам. Расчеты, требующие точного определения, представлены отдельными формулами. В отличие от анонимизированных переменных Elliptic, значения этих характеристик можно повторно вычислить и проверить по открытым данным блокчейна.

Общие суммы входов и выходов рассчитываются по значениям отдельных входов и выходов транзакции:

$$A_{in}(v) = \sum_{i \in I(v)} a_i^{in}, \quad A_{out}(v) = \sum_{j \in O(v)} a_j^{out} \tag{3.1}$$

где $A_{\text{in}}(v)$ и $A_{\text{out}}(v)$ – общие суммы входов и выходов транзакции, $I(v)$ и $O(v)$ – множества ее входов и выходов, a_i^{in} и a_j^{out} – значения отдельных входов и выходов, i и j – их индексы.

Комиссия определяется как разность между общей суммой входов и общей суммой выходов:

$$F(v) = A_{\text{in}}(v) - A_{\text{out}}(v) \tag{3.2}$$

где $F(v)$ – комиссия транзакции, $A_{\text{in}}(v)$ и $A_{\text{out}}(v)$ – общие суммы ее входов и выходов. Комиссия используется как промежуточная величина для расчета ставки и доли комиссии и отдельно в базовый набор не включается.

Ставка комиссии рассчитывается относительно размера транзакции:

$$r_F(v) = \frac{10^8 F(v)}{L(v)} \tag{3.3}$$

где $r_F(v)$ – ставка комиссии в satoshi на байт, $F(v)$ – комиссия в BTC, $L(v)$ – размер транзакции в байтах, множитель 10^8 переводит BTC в satoshi.

Доля комиссии показывает ее величину относительно общей суммы входов:

$$q_F(v) = \frac{F(v)}{\max\{A_{\text{in}}(v), \varepsilon\}} \tag{3.4}$$

где $q_F(v)$ – доля комиссии в общей сумме входов, ε – малое положительное значение, предотвращающее деление на ноль, max – оператор выбора наибольшего значения.

Концентрация средств определяется по долям крупнейшего входа и выхода:

$$\begin{aligned} q_{\text{in}}^{\max}(v) &= \frac{A_{\text{in}}^{\max}(v)}{\max\{A_{\text{in}}(v), \varepsilon\}} \\ q_{\text{out}}^{\max}(v) &= \frac{A_{\text{out}}^{\max}(v)}{\max\{A_{\text{out}}(v), \varepsilon\}} \end{aligned} \tag{3.5}$$

где $q_{\text{in}}^{\max}(v)$ и $q_{\text{out}}^{\max}(v)$ – доли крупнейшего входа и выхода, $A_{\text{in}}^{\max}(v)$ и $A_{\text{out}}^{\max}(v)$ – максимальные суммы среди входов и выходов, $A_{\text{in}}(v)$ и $A_{\text{out}}(v)$ – их общие суммы. Оба показателя принимают значения от 0 до 1.

Медианный возраст расходуемых выходов рассчитывается по высотам блоков:

$$\tilde{\tau}_{in}(v) = med_{i \in I(v)}\big[b(v) - b\big(prev(i)\big)\big] \tag{3.6}$$

где $\tilde{\tau}_{\text{in}}(v)$ – медианный возраст выходов, расходуемых во входах транзакции, $b(v)$ – высота блока, содержащего текущую транзакцию, $\text{prev}(i)$ – транзакция, создавшая выход, расходуемый входом i, $I(v)$ – множество входов, med – оператор медианы.

Медианный интервал до последующего расходования выходов определяется отдельно:

$$\tilde{\tau}_{out}(v) = med_{j \in O^{spent}(v)}\left[b\left(spend(j)\right) - b(v)\right] \quad (3.7)$$

где $\tilde{\tau}_{\text{out}}(v)$ – медианный интервал до последующего расходования выходов, $O^{\text{spent}}(v)$ – множество выходов, расходование которых наблюдается в исследуемом периоде, $\text{spend}(j)$ – транзакция, расходующая выход j, $\varnothing$ – пустое множество.

Базовые транзакционные признаки приведены в таблице 3.2.

Таблица 3.2 – Базовое 26-признаковое представление Bitcoin-транзакции

№	Признак	Обозначение	Содержание
Транзакционные признаки – 17 характеристик			
1	Суммарное значение входов и выходов	$A_{\Sigma}(v)$	Сумма всех входов и выходов транзакции
2	Число входных адресов	$n_{\text{addr}}^{\text{in}}(v)$	Число адресов во входах транзакции
3	Число выходных адресов	$n_{\text{addr}}^{\text{out}}(v)$	Число адресов в выходах транзакции
4	Размер транзакции	$L(v)$	Размер транзакции в байтах
5	Максимальная сумма входа	$A_{\text{in}}^{\max}(v)$	Максимальная сумма среди входов транзакции
6	Медианная сумма входа	$A_{\text{in}}^{\text{med}}(v)$	Медианная сумма среди входов транзакции
7	Общая сумма входов	$A_{\text{in}}(v)$	Сумма всех входов транзакции по формуле (3.1)
8	Максимальная сумма выхода	$A_{\text{out}}^{\max}(v)$	Максимальная сумма среди выходов транзакции
9	Медианная сумма выхода	$A_{\text{out}}^{\text{med}}(v)$	Медианная сумма среди выходов транзакции
10	Общая сумма выходов	$A_{\text{out}}(v)$	Сумма всех выходов транзакции по формуле (3.1)
11	Индикатор консолидации	$C(v)$	1, если число входов больше числа выходов, иначе 0
12	Доля крупнейшего входа	$q_{\text{in}}^{\max}(v)$	Отношение крупнейшего входа к общей сумме входов по формуле (3.5), от 0 до 1

Продолжение таблицы 3.2

13	Доля крупнейшего выхода	$q_{\text{out}}^{\max}(v)$	Отношение крупнейшего выхода к общей сумме выходов по формуле (3.5), от 0 до 1
14	Ставка комиссии	$r_F(v)$	Комиссия на единицу размера по формуле (3.3)
15	Доля комиссии	$q_F(v)$	Отношение комиссии к общей сумме входов по формуле (3.4)
16	Медианный возраст входов	$\tilde{\tau}_{\text{in}}(v)$	Медианный возраст расходуемых выходов по формуле (3.6)
17	Медианный интервал до расходования выходов	$\tilde{\tau}_{\text{out}}(v)$	Медианный интервал до последующего расходования выходов по формуле (3.7)
Структурные и графовые признаки – 9 характеристик			
18	Входящая степень	$d_{\text{in},t}(v)$	Число транзакций-предшественников по формуле (3.10)
19	Исходящая степень	$d_{\text{out},t}(v)$	Число транзакций-потомков по формуле (3.10)
20	PageRank	$\text{PR}_t(v)$	Значимость транзакции с учетом входящих связей по формуле (3.11)
21	HITS authority	$\text{Auth}_t(v)$	Значимость транзакции как получателя связей от hub-вершин по формуле (3.12)
22	HITS hub	$\text{Hub}_t(v)$	Значимость транзакции как источника связей к authority-вершинам по формуле (3.12)
23	Средняя степень соседних транзакций	$\overline{d}_{N,t}(v)$	Среднее число связей у соседних транзакций по формуле (3.14)
24	Собственновекторная центральность	$\text{EC}_t(v)$	Значимость транзакции с учетом значимости соседей по формуле (3.13)
25	Размер слабосвязной компоненты	$c_{W,t}(v)$	Число транзакций в слабосвязной компоненте по формуле (3.15)
26	Номер k-ядра	$k_{c,t}(v)$	Наибольшее k для ядра, в которое входит транзакция, по формуле (3.16)

Транзакционный граф

Для каждого временного среза Bitcoin-транзакции представляются невзвешенным направленным графом. Вершина соответствует транзакции, а ребро отражает расходование хотя бы одного выхода одной транзакции во входе другой. Если между одной парой транзакций существует несколько UTXO-связей, при расчете структурных показателей используется одно ребро. Формально граф временного среза задается следующим образом:

$$G_t = (V_t, E_t) \tag{3.8}$$

где G_t – направленный транзакционный граф временного среза t, V_t – множество транзакций в этом срезе, E_t – множество направленных ребер. Ребро $(u, v) \in E_t$ означает, что выход транзакции u расходуется во входе транзакции v.

Входящее и исходящее окружения определяются направлением ребра:

$$\begin{gathered} N_{\text{in},t}(v) = \{u \in V_t : (u, v) \in E_t\} \\ N_{\text{out},t}(v) = \{u \in V_t : (v, u) \in E_t\} \end{gathered} \tag{3.9}$$

где $N_{\text{in},t}(v)$ – множество непосредственных транзакций-предшественников, $N_{\text{out},t}(v)$ – множество непосредственных транзакций-потомков, u – соседняя транзакция, V_t и E_t – множества вершин и ребер графа.

Входящая и исходящая степени равны числу элементов соответствующих множеств:

$$d_{\text{in},t}(v) = \left|N_{\text{in},t}(v)\right|, \qquad d_{\text{out},t}(v) = \left|N_{\text{out},t}(v)\right| \tag{3.10}$$

где $d_{\text{in},t}(v)$ и $d_{\text{out},t}(v)$ – входящая и исходящая степени транзакции, $N_{\text{in},t}(v)$ и $N_{\text{out},t}(v)$ – множества ее предшественников и потомков, вертикальные черты обозначают число элементов множества.

Входящая степень и число входных адресов являются разными характеристиками. Первая показывает число связанных транзакций-предшественников в графе, вторая – число адресов во входах текущей транзакции. Аналогично исходящая степень не равна числу выходных адресов.

Структурные и графовые признаки

PageRank, HITS и собственновекторная центральность описывают положение транзакции в графе, но не измеряют объем денежного потока и сами по себе не указывают на противоправный характер транзакции. PageRank (PR) для направленного графового среза определяется следующим выражением [64]:

$$PR_t(v) = \frac{1 - \alpha}{|V_t|} + \alpha \sum_{u \in N_{in,t}(v)} \frac{PR_t(u)}{d_{out,t}(u)} \tag{3.11}$$

где $\mathrm{PR}_t(v)$ – значение PageRank транзакции, $\alpha \in (0,1)$ – коэффициент затухания, $|V_t|$ – число вершин графа, $N_{\mathrm{in},t}(v)$ – множество предшественников, $\mathrm{PR}_t(u)$ – PageRank предшественника u, $d_{\mathrm{out},t}(u)$ – его исходящая степень. Для вершин без исходящих ребер используется стандартное перераспределение PageRank-массы по всем вершинам графа.

Алгоритм HITS различает взаимосвязанные роли authority (авторитетной вершины) и hub (хаб-вершины) [65]:

$$\begin{aligned} Auth_t(v) &= \sum_{u \in N_{in,t}(v)} H\,ub_t(u) \\ Hub_t(v) &= \sum_{w \in N_{out,t}(v)} A\,uth_t(w) \end{aligned} \tag{3.12}$$

где $\mathrm{Auth}_t(v)$ – оценка authority транзакции, $\mathrm{Hub}_t(v)$ – ее оценка hub, $N_{\mathrm{in},t}(v)$ и $N_{\mathrm{out},t}(v)$ – множества входящих и исходящих соседей, u и w – соседние транзакции. После каждой итерации векторы authority и hub нормируются.

Для остальных структурных показателей используется ненаправленная проекция графа, в которой направление ребер игнорируется. Собственновекторная центральность (Eigenvector Centrality) определяется через центральности соседних вершин:

$$EC_t(v) = \frac{1}{\lambda_t} \sum_{u \in N_t(v)} E\,C_t(u) \tag{3.13}$$

где $\mathrm{EC}_t(v)$ – собственновекторная центральность транзакции, $N_t(v)$ – множество ее соседей в ненаправленной проекции графа, $\mathrm{EC}_t(u)$ – центральность соседней вершины u, λ_t – собственное значение матрицы смежности этой проекции.

Средняя степень соседних транзакций рассчитывается как:

$$\overline{d}_{N,t}(v) = \begin{cases} \dfrac{1}{|N_t(v)|} \displaystyle\sum_{u \in N_t(v)} d_t\,(u), & |N_t(v)| > 0, \\ 0, & |N_t(v)| = 0, \end{cases} \tag{3.14}$$

где $\overline{d}_{N,t}(v)$ – средняя степень соседних транзакций, $N_t(v)$ – множество соседей, $d_t(u)$ – степень соседней вершины u в ненаправленной проекции. Для изолированной вершины показатель принимается равным 0.

Размер слабосвязной компоненты определяется числом содержащихся в ней вершин:

$$c_{W,t}(v) = |W_t(v)| \tag{3.15}$$

где $c_{W,t}(v)$ – размер слабосвязной компоненты, содержащей транзакцию, $W_t(v)$ – множество вершин этой компоненты, вертикальные черты обозначают число ее вершин.

Номер k-ядра показывает глубину включения транзакции в плотную часть графа:

$$k_{c,t}(v) = \max\{k: v \in K_{t,k}\} \tag{3.16}$$

где $k_{c,t}(v)$ – номер k-ядра транзакции, $K_{t,k}$ – максимальный подграф ненаправленной проекции, в котором степень каждой вершины не меньше k, max – оператор выбора наибольшего допустимого значения.

Семнадцать транзакционных и девять структурных характеристик образуют базовое 26-признаковое представление. Приведенные формулы задают единый способ расчета признаков и исключают смешение адресных характеристик с графовыми степенями. Выбор структурных показателей опирается на общие подходы к анализу сетей и центральности [66–68].

3.3 Анализ перемещения средств в сети Bitcoin по материалам расследований

Разработка новых признаков опиралась не только на формальные свойства графа, но и на практические кейсы, связанные с расследованиями взломов, атак с использованием программ-вымогателей, деятельности сервисов смешивания и способов вывода средств. Такие материалы использовались как источник повторяющихся наблюдаемых паттернов, которые затем формализуются и проверяются экспериментально [69].

Взлом Zaif, 2018 год. В открытых источниках описан несанкционированный доступ к горячим кошелькам японской биржи Zaif и хищение криптоактивов примерно на 6,7 млрд иен, включая 5 966 BTC, Bitcoin Cash и MonaCoin. Reuters сообщал о краже около 60 млн долларов [70], а CoinDesk отмечал необычный исходящий поток средств из кошельков биржи [71]. На рисунке 3.2 показан резкий вывод средств из сервисного окружения Zaif с их последующим перемещением через несколько транзакций.



Рисунок 3.2 – Взлом криптобиржи Zaif и последующее перемещение средств

Взлом DMM Bitcoin, 2024 год. FBI, Defense Cyber Crime Center и Национальное полицейское агентство Японии связали хищение 4 502,9 BTC стоимостью около 308 млн долларов у DMM Bitcoin с группой TraderTraitor [72]. Согласно сообщению, злоумышленники манипулировали легитимным запросом на транзакцию, после чего средства были переведены на контролируемые ими адреса. Elliptic также отмечала раннее распределение похищенных Bitcoin по нескольким новым адресам [73]. Этот паттерн связан с признаками веерного распределения, дробления суммы, ускоренного последующего расходования и отклонения характеристик транзакции от предшествующей транзакционной истории.

Взлом Bitfinex, 2016 год. По данным Министерства юстиции США, с Bitfinex было похищено 119 754 BTC, после чего часть средств в течение нескольких лет перемещалась через различные сервисы и механизмы сокрытия происхождения [74]. Анализ Elliptic указывает на последовательное отделение частей суммы и сервисные переходы, затрудняющие трассировку [75]. Этот кейс обосновывает учет не только текущей транзакции, но и ее восходящей истории.

Colonial Pipeline и DarkSide. Министерство юстиции США сообщило об изъятии 63,7 BTC, составлявших часть выкупного платежа группе DarkSide [76]. Chainalysis описала распределение платежа в модели «вымогательское ПО как услуга», при которой средства делятся между участниками схемы [77]. Elliptic связала адреса DarkSide с многочисленными платежами и последующими переводами к инфраструктурным точкам [78]. Для формализации таких сценариев используются интервалы до последующего расходования, степень разделения потока, концентрация входящих платежей и ускоренное последующее расходование.

Helix, ChipMixer и Bitcoin Fog. Материалы по сервисам смешивания средств отражают другую группу паттернов. Министерство юстиции США характеризовало Helix как даркнет-сервис отмывания средств, через который было перемещено более 350 000 BTC, значительная часть которых была связана с даркнет-маркетплейсами [79]. В материалах по ChipMixer указывалась обработка средств, связанных с вымогательским ПО, похищенными активами и даркнет-маркетплейсами [80]. Bitcoin Fog, по данным Министерства юстиции США, обработал более 1,2 млн BTC и длительное время функционировал как Bitcoin-миксер в даркнете [81]. Эти кейсы обосновывают включение признаков усложнения трассировки: дисбаланса входящих и исходящих потоков, распределения выходных сумм, динамики последующего расходования и последующей консолидации.

Whirlpool и Ricochet. В материалах Министерства юстиции США Whirlpool описывается как сервис смешивания Bitcoin, а Ricochet как механизм добавления промежуточных транзакций между отправителем и получателем [82]. Использование таких сервисов направлено на затруднение отслеживания происхождения и дальнейшего движения средств. Структура, характерная для CoinJoin, сама по себе не свидетельствует о незаконности операции. Она приобретает значение только с учетом дополнительного контекста, включая предшествующую транзакционную историю, особенности последующего вывода средств и наличие нескольких выходов с одинаковыми или близкими суммами. Для Ricochet дополнительным признаком является увеличение числа промежуточных транзакций.

BTC-e и Mt. Gox**.** По данным Министерства юстиции США, BTC-e использовалась для операций, связанных с хакерскими атаками, кражей персональных данных и незаконным оборотом наркотиков, а также с перемещением средств после взлома Mt. Gox [83]. Вместе с тем сам по себе перевод средств на биржу или другую инфраструктурную площадку не свидетельствует о подозрительном характере транзакции. Основания для дополнительной проверки возникают, если такому переводу предшествуют дробление суммы, быстрые переходы через промежуточные адреса или иные подозрительные признаки в предшествующей транзакционной истории.

Похожие наблюдения представлены в исследованиях взломов, платежей по вымогательскому ПО и сервисов смешивания. Goldsmith et al. показывают значение временных интервалов и последовательности переводов при движении похищенных средств к точкам вывода [84]. Paquet-Clouston et al. обращают внимание на последующие операции вывода средств после платежей по вымогательскому ПО [85]. В Elliptic2 рассматриваются подозрительные подграфы, цепочки последовательного отделения средств, миксеры, даркнет-маркетплейсы и вложенные сервисы [43]. Wu et al. показывают, что при выявлении сервисов смешивания информативны не только адресные характеристики, но и параметры транзакций, включая суммы и временные интервалы [86].

Переход от эмпирических наблюдений к криминалистическим гипотезам

Рассмотренные кейсы показывают, что движение средств, связанное с расследуемой нелегальной деятельностью, редко описывается одним правилом. Крупная сумма может соответствовать обычной биржевой операции, большое число выходов может означать пакетную выплату, короткий интервал может говорить об автоматизированной работе платежного сервиса, а консолидация UTXO может соответствовать стандартной операционной практике. Поэтому вывод следует делать по сочетанию нескольких признаков с учетом конкретного контекста.

На этой основе формулируются три проверяемые криминалистические гипотезы [87].

Первая гипотеза – локальное отклонение от окружения. Транзакция может представлять интерес не только вследствие абсолютного значения ее параметров, но и при заметном отличии от ближайшего входящего и исходящего окружения. Например, среди небольших регулярных переводов отклонение транзакции по сумме, комиссии, числу выходов или темпу последующего расходования может быть информативнее абсолютного значения соответствующего признака.

Вторая гипотеза – ускоренное последующее расходование. После взлома, выплаты выкупа или получения средств в результате иной нелегальной деятельности участники могут стремиться быстро переместить их дальше. В транзакционном графе это может проявляться короткими интервалами до последующего расходования выходов, появлением нескольких транзакций-потомков и их концентрацией в небольшом временном интервале.

Третья гипотеза – отклонение характеристик транзакции от предшествующей транзакционной истории. Даже при обычных значениях отдельных параметров транзакция может заметно отличаться от предыдущих переводов. Например, после последовательности однотипных переводов текущая транзакция может характеризоваться резким изменением суммы, комиссии, размера или числа выходов. Поэтому ее характеристики целесообразно сопоставлять с характеристиками предшествующих транзакций.

Далее каждая гипотеза преобразуется в формально определенную группу признаков.

3.4 Формализация криминалистически интерпретируемых признаков

Общий признаковый вектор

Для каждой размеченной транзакции $v \in V_t$ итоговый вектор включает пять групп признаков:

$$x_v = \left[x_v^{tx};\ x_v^{topo};\ x_v^{nbr};\ x_v^{temp};\ x_v^{GAR}\right]. \tag{3.17}$$

где x_v^{tx} – базовые транзакционные признаки, x_v^{topo} – структурные и графовые признаки, x_v^{nbr} – признаки локального отклонения от окружения, x_v^{temp} – временные признаки последующего расходования, x_v^{GAR} – признаки графовой авторегрессии по восходящей транзакционной истории, включающие агрегированные значения признаков предшествующих транзакций, ожидаемые значения и остатки (GAR-признаки) [87].

Группа 1: локальное отклонение от окружения

На основе анализа кейсов было установлено, что нелегальные транзакции в большинстве случаев отличались от локального окружения. В частности, наблюдались резкое увеличение суммы транзакции, комиссии, размера, числа входных и выходных адресов и других характеристик. Поэтому предлагается ввести блок признаков, отражающий локальные отклонения от значений, характерных для окружения [87].

Пусть имеется конечная числовая выборка

$$X = (x_1, x_2, \dots, x_n), \qquad n \geq 1.$$

Пусть $X' = \left(x_{(1)}, x_{(2)}, \dots, x_{(n)}\right)$ – та же выборка, но упорядоченная по значениям, то есть выполняется условие

$$x_{(1)} \leq x_{(2)} \leq \cdots \leq x_{(n)}.$$

Медиана определяется формулой

$$\text{median}(X) = \begin{cases} x_{\frac{n+1}{2}}, & n \text{ нечетно}, \\ \dfrac{x_{\frac{n}{2}} + x_{\frac{n}{2}+1}}{2}, & n \text{ четно}. \end{cases}$$

Для расчета локальных дескрипторов используются направленный граф $G_t = (V_t, E_t)$, множества непосредственных предшественников $N_t^-(v)$и потомков $N_t^+(v)$, а также входящая и исходящая степени $d_t^-(v)$и $d_t^+(v)$, определенные формулами (3.8)–(3.10). При наличии нескольких UTXO-связей между одной и той же парой транзакций сосед учитывается один раз.

Пусть $s: V \to \mathbb{R}$ – один скалярный транзакционный сигнал, dir ∈ {in,out} – направление, а $N_{\text{dir}}(v)$ и $d_{\text{dir}}(v) = |N_{\text{dir}}(v)|$ – соответственно множество направленных соседей и их число. Для фиксированных v, s и dir положим $n = d_{\text{dir}}(v)$.

Локальное сравнение выполняется для множества семи транзакционных сигналов $\mathcal{S}$:

$$\boldsymbol{\mathcal{S}} = \left\{\boldsymbol{A_\Sigma(v)},\ \boldsymbol{n_{addr}^{in}(v)},\ \boldsymbol{n_{addr}^{out}(v)},\ \boldsymbol{L(v)},\ \boldsymbol{q_F(v)},\ \boldsymbol{\tilde{\tau}_{in}(v)},\ \boldsymbol{\tilde{\tau}_{out}(v)}\right\}.$$

Эти сигналы обозначаются как $s_j \in \mathcal{S}, j = 1, \dots, 7$.

После упорядочивания локальных значений

$$s^{(1)}_{\text{dir},j}(v) \le s^{(2)}_{\text{dir},j}(v) \le \cdots \le s^{(n)}_{\text{dir},j}(v)$$

вычислим локальную медиану следующим образом:

$$\text{med}_{\text{dir},j}(v) = \begin{cases} s^{\left(\frac{n+1}{2}\right)}_{\text{dir},j}(v), & n \text{ нечетно}, \\ \dfrac{s^{\left(\frac{n}{2}\right)}_{\text{dir},j}(v) + s^{\left(\frac{n}{2}+1\right)}_{\text{dir},j}(v)}{2}, & n \text{ четно}. \end{cases}$$

Таким образом, для любого числового транзакционного сигнала $s(v)$, например суммы, комиссии, размера, числа входов, числа выходов или концентрации выходов, локальную медиану в обобщенном виде можно определить следующим образом:

$$\text{med}_{\text{dir},s}(v) = \text{median}_{u \in N_{\text{dir}}(v)} s(u), \qquad \text{dir} \in \{\text{in,out}\}. \qquad (3.18)$$

Определенная таким образом величина $\text{med}_{\text{dir},s}(v)$ является локальной медианой рассматриваемой выборки для входящего или исходящего локального окружения, а не медианой сигнала по всем вершинам графа.

MAD – медианное абсолютное отклонение значений

Для общей выборки $X = (x_1, \dots, x_n)$ сначала вычисляется ее медиана $\bar{x} = \text{median}(X)$.

Затем вычисляются абсолютные отклонения от медианы:

$$a_i = |x_i - \tilde{x}|, \qquad i = 1, \dots, n.$$

Значения a_i упорядочиваются по возрастанию так, чтобы выполнялось условие

$$a_{(1)} \le a_{(2)} \le \cdots \le a_{(n)}$$

тогда медианное абсолютное отклонение значений вычисляется следующим образом:

$$\text{MAD}(X) = \begin{cases} a_{\frac{n+1}{2}}, & n \text{ нечетно}, \\ \dfrac{a_{\frac{n}{2}} + a_{\frac{n}{2}+1}}{2}, & n \text{ четно}. \end{cases}$$

Адаптация MAD к направленному локальному окружению.

Для каждого соседа $u \in N_{\text{dir}}(v)$ сначала вычисляется локальное абсолютное отклонение:

$$\delta_{\text{dir},s}(u; v) = \left|s(u) - \text{med}_{\text{dir},s}(v)\right|.$$

Полученные значения $\delta_{\text{dir},s}(u; v)$ упорядочиваются по возрастанию так, чтобы выполнялось условие

$$\delta_{\text{dir},s}^{(1)}(v) \leq \cdots \leq \delta_{\text{dir},s}^{(n)}(v)$$

тогда локальный MAD вычисляется как

$$\text{MAD}_{\text{dir},s}(v) = \begin{cases} \delta_{\text{dir},s}^{\left(\frac{n+1}{2}\right)}(v), & n \text{ нечетно}, \\ \dfrac{\delta_{\text{dir},s}^{\left(\frac{n}{2}\right)}(v) + \delta_{\text{dir},s}^{\left(\frac{n}{2}+1\right)}(v)}{2}, & n \text{ четно}. \end{cases}$$

или, эквивалентно,

$$\text{MAD}_{\text{dir},s}(v) = \text{median}_{u \in N_{\text{dir}}(v)}\left|s(u) - \text{med}_{\text{dir},s}(v)\right|, \tag{3.19}$$

где $\text{MAD}_{\text{dir},s}(v)$ – медианное абсолютное отклонение значений признака s в локальном окружении транзакции v в направлении dir, то есть устойчивая мера локального разброса. Использование медианы и MAD снижает влияние выбросов, что важно для Bitcoin-графа с тяжелыми хвостами распределений сумм, комиссий и степеней [88].

Устойчивый нормированный показатель локального окружения задается следующим образом:

$$z_{\text{dir},s}^{\text{rob}}(v) = \frac{s(v) - \text{med}_{\text{dir},s}(v)}{\max\{c \cdot \text{MAD}_{\text{dir},s}(v), \kappa(s)\}}, \tag{3.20}$$

где $z_{\text{dir},s}^{\text{rob}}(v)$ – устойчивый локальный z-показатель, $s(v)$ – значение признака у текущей транзакции, $c = 1{,}4826$ – нормировочный коэффициент MAD, обеспечивающий согласование с нормальным распределением, $\kappa(s) > 0$ – стабилизирующий параметр для признака s, оператор $\max(\cdot)$ задает нижнюю границу знаменателя. Чем больше абсолютное значение $\left|z_{\text{dir},s}^{\text{rob}}(v)\right|$, тем сильнее транзакция отличается от локального центра своего окружения.

Формулы медианы и MAD математически определены только при $d_{\text{dir}}(v) \geq 1$. Стабилизатор $\kappa(s)$ предотвращает деление на ноль при $\text{MAD}_{\text{dir},s}(v) = 0$, но сам по себе не определяет медиану пустого множества при $d_{\text{dir}}(v) = 0$.

Коэффициент c не подбирается по данным Bitcoin-графа. Это классический коэффициент нормальной согласованности немасштабированного MAD: он выбирается так, чтобы для нормального распределения масштабированный MAD совпадал со стандартным отклонением.

Пусть случайная величина X имеет нормальное распределение [88]:

$$X \sim \mathcal{N}(\mu, \sigma^2),$$

$$Z = \frac{X - \mu}{\sigma} \sim \mathcal{N}(0,1).$$

Для симметричного нормального распределения $\mathrm{median}(X) = \mu$. Обозначим популяционное немасштабированное медианное абсолютное отклонение через

$$m = \mathrm{median}|X - \mu|.$$

По определению медианы случайной величины $|X - \mu|$ выполняется

$$P(|X - \mu| \le m) = \frac{1}{2}.$$

После стандартизации получаем

$$P\left(|Z| \le \frac{m}{\sigma}\right) = \frac{1}{2}.$$

Пусть $\Phi(z) = P(Z \le z)$ – функция распределения стандартной нормальной случайной величины. Тогда вследствие симметрии $\Phi(-z) = 1 - \Phi(z)$:

$$P\left(-\frac{m}{\sigma} \le Z \le \frac{m}{\sigma}\right) = \Phi\left(\frac{m}{\sigma}\right) - \Phi\left(-\frac{m}{\sigma}\right).$$

С учетом равенства $\Phi(-z) = 1 - \Phi(z)$ последнее выражение принимает вид

$$2\Phi\left(\frac{m}{\sigma}\right) - 1 = \frac{1}{2}.$$

Следовательно,

$$\Phi\left(\frac{m}{\sigma}\right) = \frac{3}{4},$$

$$\frac{m}{\sigma} = \Phi^{-1}\left(\frac{3}{4}\right).$$

Численное значение квантиля равно

$$q_{0.75} = \Phi^{-1}(0.75) = 0.6744897501960817.$$

Поэтому

$$m = 0.6744897501960817\,\sigma,$$

а обратный коэффициент равен

$$c = \frac{1}{q_{0.75}} = \frac{1}{\Phi^{-1}(0.75)} = 1.482602218505602.$$

После округления до четырех знаков после запятой используется

$$c \approx 1.4826.$$

Таким образом, при нормальной модели на популяционном уровне выполняется соотношение

$$\sigma = c\,m.$$

Для выборки величина $c\,\widehat{\mathrm{MAD}}$ является асимптотически согласованной оценкой стандартного отклонения σ. Коэффициент c задает нормальный эталон масштаба.

Стабилизатор $\kappa(s)$ определяется для каждого признака s как максимум между минимально допустимым масштабом и глобальным робастным масштабом признака:

$$\kappa(s) = \max\left\{\kappa_{\min}(s),\, c \cdot \mathrm{MAD}_{\mathrm{global},s}\right\}, \tag{3.21}$$

где $\mathrm{MAD}_{\mathrm{global},s}$ – глобальный немасштабированный MAD сигнала s, вычисляемый в пределах рассматриваемого графового среза, $\kappa_{\min}(s)$ – минимально допустимый масштаб. Его значение зависит от типа признака:

$$\kappa_{\min}(s) = \begin{cases} 1, & s \in \{n^{in}_{addr}(v),\ n^{out}_{addr}(v),\ L(v)\}, \\ 0{,}05, & s \in \{\tilde{\tau}_{in}(v),\ \tilde{\tau}_{out}(v)\}, \\ 10^{-6}, & \text{для остальных признаков, включая } q_F(v) \text{ и } A_\Sigma(v). \end{cases}$$

То есть фактический знаменатель в коде равен:

$$\max\{c \cdot \mathrm{MAD}_{\mathrm{dir},s}(v),\ \kappa(s)\}.$$

Например, если для $n_{addr}^{in}(v)$ локальный $\mathrm{MAD} = 0$, а глобальный робастный масштаб равен $0{,}7$, то:

$$\kappa(s) = max\{1;\ 0{,}7\} = 1.$$

Если глобальный масштаб равен $2{,}4$, тогда:

$$\kappa(s) = \max\{1;\ 2{,}4\} = 2{,}4.$$

Важный момент: при $d_{\mathrm{dir}}(v) = 0$, то есть, когда у транзакции вообще нет соседей данного направления, медиана и MAD остаются неопределенными, а итоговый локальный z-показатель записывается как NaN. Стабилизатор $\kappa(s)$ применяется только тогда, когда локальное множество существует, но его разброс равен нулю или слишком мал. $\kappa(s)$ представляет собой зависящий от типа признака нижний предел масштаба, дополнительно ограниченный снизу глобальной робастной оценкой разброса соответствующего признака. При отсутствии соседей локальная медиана, MAD и локальный z-показатель считаются неопределенными.

Чтобы учесть не только нормированное отклонение от локальной медианы, но и общее расхождение транзакции с направленным окружением, вводится направленная локальная энергия расхождения, основанная на среднем квадрате отклонений:

$$E_{\mathrm{dir},s}(v) = \frac{1}{d_{\mathrm{dir}}(v)} \sum_{u \in N_{\mathrm{dir}}(v)} \big(s(v) - s(u)\big)^2, \qquad (3.22)$$

где $E_{\mathrm{dir},s}(v)$ – направленная локальная энергия расхождения с окружением для признака s, определяемая как среднее значение квадратов различий между значением признака текущей транзакции и значениями того же признака у ее направленных соседей, $d_{\mathrm{dir}}(v) = |N_{\mathrm{dir}}(v)|$ – число соседей соответствующего направления, $s(u)$ – значение признака у соседней транзакции. Формула (3.22) применяется при $d_{\mathrm{dir}}(v) \geq 1$. При $d_{\mathrm{dir}}(v) = 0$ показатель считается неопределенным и записывается как NaN. При наличии соседей значение $E_{\mathrm{dir},s}(v) = 0$ означает, что значение рассматриваемого признака у текущей транзакции совпадает со значениями этого признака у всех ее направленных соседей. По смыслу этот показатель является локальным направленным аналогом вариации графового сигнала [89].

Итоговый блок признаков локального отклонения от окружения формируется объединением устойчивых z-показателей и энергетических дескрипторов:

$$x_v^{\mathrm{nbr}} = \mathrm{concat}_{\substack{s\in\mathcal{S} \\ \mathrm{dir}\in\{\mathrm{in,out}\}}} \left[z_{\mathrm{dir},s}^{\mathrm{rob}}(v), E_{\mathrm{dir},s}(v)\right], \quad (3.23)$$

где $\mathcal{S}$ – определенное выше множество семи транзакционных сигналов, $\mathrm{concat}(\cdot)$ – операция объединения признаков в единый вектор. Для каждого сигнала вычисляются два дескриптора в двух направлениях, поэтому итоговый блок содержит $7 \times 2 \times 2 = 28$ признаков. В криминалистической интерпретации блок характеризует степень отклонения транзакции от ее непосредственных соседей.

Интерпретация признаков

Значение $z_{\mathrm{dir},s}^{\mathrm{rob}}(v)$ отвечает на вопрос, насколько значение $s(v)$ необычно относительно типичного значения у предшественников или потомков.

Значение $E_{\mathrm{dir},s}(v)$ показывает средний квадрат различий между значением признака текущей транзакции и значениями этого признака у ее предшественников или потомков.

Группа 2: временные признаки последующего расходования

Поскольку в работе рассматривается ретроспективный киберкриминалистический анализ, данные признаки вычисляются по последующему расходованию, наблюдаемому в пределах соответствующего графового среза. Вторая группа признаков характеризует скорость и временную концентрацию наблюдаемых транзакций-потомков, расходующих выходы рассматриваемой транзакции. Признаки рассчитываются по связям между транзакциями и высотам блоков [87].

Для фиксированного графового среза используется множество исходящих соседей $O(v)$, определенное формулой (3.9). Перед расчетом признаков повторяющиеся пары (v, u) удаляются, поэтому, если одна и та же транзакция расходует несколько выходов транзакции v, соответствующая пара учитывается один раз. Ребра, для которых отсутствует высота блока исходной транзакции v или транзакции-потомка u, исключаются из дальнейших вычислений. Далее под $O(v)$ понимается множество уникальных транзакций-потомков после указанной фильтрации.

Число исходящих транзакций-потомков определяется следующим образом:

$$k_{out}(v) = |O(v)|, \quad (3.24)$$

где $k_{\mathrm{out}}(v)$ – число уникальных транзакций-потомков.

Обозначим через $bh(u)$ высоту блока, представляющую собой порядковый номер блока в цепочке Bitcoin. Тогда разность высот блоков транзакций uи vопределяет расстояние между ними в количестве блоков. Вычислим для пары транзакций v, uэто расстояние (block-height difference):

$$\Delta_{v\to u} = bh(u) - bh(v). \tag{3.25}$$

Значение $\Delta_{v\to u}$ фактически определяет задержку при расходовании поступивших средств и измеряется в блоках. Это значение дает нам информацию о том, через сколько блоков поступившая сумма будет переведена (израсходована), или, другими словами, сколько блоков она будет находиться в исходной транзакции до дальнейшего перемещения. Поэтому в научной литературе часто используется термин «лаг» (lag – задержка). В русскоязычной литературе данный термин пока не имеет устоявшегося аналога, поэтому в дальнейшем будут использоваться оба обозначения, поскольку их смысл совпадает.

Для непустого множества $O(v)$ выборка исходящих лагов с сохранением повторяющихся значений определяется следующим образом:

$$\mathcal{L}_{out}(v) = \{\Delta_{v\to u} : u \in O(v)\}, \qquad |\mathcal{L}_{out}(v)| = k_{out}(v). \tag{3.26}$$

Минимальный исходящий лаг равен:

$$L_{\min}^{out}(v) = \min_{u\in O(v)} \Delta_{v\to u}. \tag{3.27}$$

Минимальный исходящий лаг характеризует наименьший интервал между транзакцией (v) и последующим расходованием одного из ее выходов.

Медианный исходящий лаг определяется как:

$$L_{med}^{out}(v) = \operatorname*{median}_{u\in O(v)} \Delta_{v\to u}. \tag{3.28}$$

Он отражает типичный интервал в блоках до появления наблюдаемых транзакций-потомков.

Для расчета стандартного отклонения определяется среднее значение исходящих лагов:

$$\overline{\Delta}(v) = \frac{1}{k_{out}(v)} \sum_{u\in O(v)} \Delta_{v\to u}. \tag{3.29}$$

Средний лаг является промежуточной величиной и отдельно в итоговый признаковый вектор не включается.

Стандартное отклонение исходящих лагов задается следующим образом:

$$L_{std}^{out}(v) = \sqrt{\frac{1}{k_{out}(v)} \sum_{u\in O(v)} \left(\Delta_{v\to u} - \overline{\Delta}(v)\right)^2}. \tag{3.30}$$

Если $O(v) = \emptyset$, то $k_{\text{out}}(v) = 0$, а лаговые показатели сохраняются как пропущенные значения. При $k_{\text{out}}(v) = 1$ минимальный и медианный лаги совпадают с единственным наблюдаемым значением, а стандартное отклонение

равно нулю. Медианный возраст выходов рассчитывается по отдельным выходам, тогда как медианный исходящий лаг рассчитывается по уникальным транзакциям-потомкам.

Временной размах исходящих транзакций-потомков, измеряемый в блоках, определяется как:

$$\Delta t(v) = \begin{cases} \max\limits_{u \in O(v)} bh(u) - \min\limits_{u \in O(v)} bh(u), & k_{out}(v) \geq 2, \\ 0, & k_{out}(v) < 2. \end{cases} \tag{3.31}$$

При $k_{\text{out}}(v) \geq 2$ этот показатель также равен разности максимального и минимального исходящих лагов, поскольку общий член $bh(v)$ сокращается:

$$\Delta t(v) = \max_{u \in O(v)} \Delta_{v \to u} - \min_{u \in O(v)} \Delta_{v \to u}. \tag{3.32}$$

Однако прямые показатели интенсивности, основанные на $\Delta t(v)$, могут становиться нестабильными, если несколько переводов сосредоточены в очень коротком интервале между блоками. Поэтому введем сглаживающую регуляризацию. Учтем, что при нулевом временном размахе деление на ноль должно отсутствовать, функция должна быть гладкой и монотонной, при больших значениях совпадать с исходным временным размахом. Регуляризованный временной размах определяется следующим образом:

$$\Delta t_{reg}(v) = \Delta t(v) + \tau \ln\left(1 + (e-1)\exp\left(-\frac{\Delta t(v)}{\tau}\right)\right), \tag{3.33}$$

где $\tau > 0$ – масштабный параметр, измеряемый в блоках. В исследовании используется фиксированное значение $\tau = 50$ блоков, одинаковое для обучающей и тестовой выборок.

Коэффициент $e - 1$ обеспечивает выполнение граничного условия:

$$\Delta t_{reg}(v)|_{\Delta t(v)=0} = \tau \ln(1 + e - 1) = \tau. \tag{3.34}$$

Для больших значений $\Delta t(v)/\tau$ функция имеет асимптотику

$$\Delta t_{\text{reg}}(v) \sim \Delta t(v), \qquad \frac{\Delta t(v)}{\tau} \to \infty. \tag{3.35}$$

Знак $\sim$ означает, что отношение $\Delta t_{\text{reg}}(v)/\Delta t(v)$ стремится к единице при $\Delta t(v)/\tau \to \infty$. Следовательно, влияние сглаживания при больших значениях временного размаха становится пренебрежимо малым.

На основе регуляризованного размаха определяется интенсивность последующего расходования:

$$\rho(v) = \frac{(k_{out}(v)-1)^{\alpha}}{\left(\Delta t_{reg}(v)\right)^{\beta}}, \tag{3.36}$$

где $k_{out}(v) - 1$ – число дополнительных транзакций-потомков сверх одного базового продолжения, $\alpha \geq 0$ – параметр чувствительности к числу потомков, $\beta \geq 0$ – параметр чувствительности к временному размаху. В рассматриваемой экспериментальной параметризации используются $\alpha = 1$ и $\beta = 1$. Формула (3.36) применяется при $k_{\text{out}}(v) \geq 2$. При $k_{\text{out}}(v) < 2$ принимается $\rho(v) = 0$, что соответствует отсутствию импульсного разветвления.

Для стабилизации распределения интенсивности применяется логарифмическое преобразование:

$$\phi_{\text{out}}(v) = \ln\left(1 + \tau^{\beta}\rho(v)\right), \tag{3.37}$$

где $\phi_{\text{out}}(v)$ – итоговый дескриптор временной концентрации последующего расходования, τ – масштабный параметр, $\rho(v)$ – интенсивность по формуле (3.36). Произведение $\tau^{\beta}\rho(v)$ является безразмерным, поэтому аргумент логарифма корректен. Высокое значение $\phi_{\text{out}}(v)$ соответствует концентрации нескольких транзакций-потомков в относительно коротком интервале блоков.

При $k_{out}(v) < 2$ из принятой конвенции следует $\phi_{out}(v) = 0$. Контрольный случай для $k_{out}(v) \geq 2$, $\Delta t(v) = 0$ и $\alpha = \beta = 1$ дает

$$\Delta t_{reg}(v) = \tau, \qquad \rho(v) = \frac{k_{out}(v)-1}{\tau}, \qquad \phi_{out}(v) = \ln k_{out}(v). \tag{3.38}$$

Следовательно, значение признака остается конечным даже в случае, когда несколько транзакций-потомков включены в один блок.

Итоговый блок временных признаков включает пять характеристик: число уникальных транзакций-потомков, итоговый показатель интенсивности последующего расходования, минимальный и медианный исходящие лаги, а также стандартное отклонение исходящих лагов.

Группа 3: признаки предшествующей транзакционной истории (GAR-признаки)

Третья группа включает признаки графовой авторегрессии по восходящей транзакционной истории: агрегированные значения признаков предшествующих транзакций, ожидаемые значения и остатки. Направленные входящие связи UTXO-графа задают последовательность предшествующих транзакций, по которой агрегируются скалярные транзакционные сигналы. GAR-признаки позволяют оценить, насколько характеристики текущей транзакции отклоняются от значений, ожидаемых на основе ее предшествующей транзакционной истории [87].

В GAR-блоке используется то же множество семи скалярных транзакционных сигналов, что и при расчете признаков локального окружения:

$$\boldsymbol{X} = \left\{\boldsymbol{A_{\Sigma}}(\boldsymbol{v}),\ \boldsymbol{n_{addr}^{in}}(\boldsymbol{v}),\ \boldsymbol{n_{addr}^{out}}(\boldsymbol{v}),\ \boldsymbol{L}(\boldsymbol{v}),\ \boldsymbol{q_F}(\boldsymbol{v}),\ \tilde{\boldsymbol{\tau}}_{\boldsymbol{in}}(\boldsymbol{v}),\ \tilde{\boldsymbol{\tau}}_{\boldsymbol{out}}(\boldsymbol{v})\right\}.$$

Для каждого сигнала рассчитываются значения первого и второго уровней восходящей истории, ожидаемое значение и остаток.

В GAR-блоке используется множество непосредственных предшественников $N_t^-(v)$, определенное формулой (3.9). Если одна транзакция связана с транзакцией vнесколькими расходуемыми выходами, она учитывается один раз. Последующее усреднение выполняется по уникальным транзакциям-предшественникам, а не по отдельным входам транзакции.

Для формального описания ограниченной восходящей окрестности введем множество предков глубины не более d:

$$\mathrm{Anc}_d(v) = \{u \in V_t : u \rightsquigarrow v, 1 \le \mathrm{dist}(u, v) \le d\}, \qquad (3.39)$$

где $u \rightsquigarrow v$ означает существование направленного пути от u к v, $\mathrm{dist}(u, v)$ – длина кратчайшего такого пути, $d \in \mathbb{N}$ – предельная глубина анализа. Условие $\mathrm{dist}(u, v) \ge 1$ исключает v из множества ее предков. В GAR-модели максимальная глубина анализа задается параметром $P_{\max}$, поэтому принимается $d = P_{\max}$.

Формула (3.39) определяет достижимых предков, но не способ агрегации их сигналов. При расчете GAR-признаков применяется рекурсивное усреднение по непосредственным входящим соседям на каждом шаге. Поэтому $x^{(k)}(v)$ в общем случае не совпадает со средним значением сигнала по уникальным предкам, находящимся на расстоянии k: вклад каждого предка зависит от структуры направленных путей.

Пусть $x : V_t \to \mathbb{R}$ – выбранный скалярный транзакционный сигнал. Нулевой уровень GAR-рекурсии совпадает с фактическим значением сигнала у транзакции:

$$x^{(0)}(v) = x(v), \qquad (3.40)$$

где $x(v)$ – фактическое значение сигнала у транзакции v, а $x^{(0)}(v)$ начальное значение рекурсии. Нулевой уровень не содержит усреднения и не относится к предкам транзакции.

Для $k \ge 1$ с учетом возможных пропущенных значений рекурсия имеет следующий вид:

$$x^{(k)}(v) = \begin{cases} \dfrac{1}{m_k(v)} \displaystyle\sum_{u \in N_k^-(v)} x^{(k-1)}(u), & m_k(v) > 0, \\ 0, & d^-(v) = 0, \\ NaN, & \text{иначе.} \end{cases} \tag{3.41}$$

где $N_k^-(v)$ – множество непосредственных предшественников, для которых значение предыдущего уровня $x^{(k-1)}(u)$ является конечным, $m_k(v)$ – их число. Если у транзакции отсутствуют предшественники, то есть $d^-(v) = 0$, для любого $k \geq 1$ принимается $x^{(k)}(v) = 0$. Если предшественники существуют, но ни у одного из них нет конечного значения предыдущего шага, принимается значение NaN. Ноль в данном случае обозначает отсутствие восходящей истории, а не нулевое среднее значение сигнала. При $P_{\max} = 2$ последовательно рассчитываются первый и второй шаги GAR-рекурсии $x^{(1)}(v)$ и $x^{(2)}(v)$ по формуле (3.41).

На первом шаге усредняются конечные значения сигнала у непосредственных предшественников. На втором шаге усредняются значения $x^{(1)}$ этих предшественников, что отражает двухшаговую восходящую историю. Если одна вершина достижима несколькими направленными путями, ее сигнал может косвенно участвовать несколько раз. Вес каждого пути определяется произведением обратных чисел допустимых предшественников на последовательных шагах.

Ожидаемое значение сигнала, согласованное с восходящей историей, определяется графовой авторегрессионной моделью. При применении уже оцененных коэффициентов пропущенные значения GAR-уровней заменяются нулем только внутри линейной комбинации:

$$\tilde{x}^{(k)}(v) = \begin{cases} x^{(k)}(v), & x^{(k)}(v) \in \mathbb{R}, \\ 0, & x^{(k)}(v) \notin \mathbb{R}, \end{cases}$$
$$\hat{x}(v) = b_0 + \sum_{k=1}^{P_{\max}} \varphi_k \, \tilde{x}^{(k)}(v), \tag{3.42}$$

где $\hat{x}(v)$ – ожидаемое значение сигнала, с учетом восходящей истории, b_0 – свободный член, φ_k – коэффициент влияния GAR-уровня k, $P_{\max}$ – максимальная глубина рекурсии, $\tilde{x}^{(k)}(v)$ – значение уровня, используемое при применении модели. Вершины с пропущенными значениями GAR-признаков не используются при оценивании коэффициентов GAR-модели.

Остаток GAR-модели определяется как

$$r(v) = x(v) - \hat{x}(v), \tag{3.43}$$

где $r(v)$ – остаток GAR-модели, то есть разница между фактическим и ожидаемым значениями сигнала. Положительный остаток означает

превышение ожидаемого значения, отрицательный означает значение ниже ожидаемого. Величина $|r(v)|$ характеризует степень отклонения от ожидаемого значения, рассчитанного по предшествующей транзакционной истории. Остатки разных сигналов имеют разные единицы и масштабы, поэтому их абсолютные значения нельзя непосредственно сравнивать между собой без дополнительной стандартизации.

Для каждого сигнала x коэффициенты $b_0, \varphi_1, \dots, \varphi_{P_{\max}}$ оцениваются отдельно. Используется взвешенная ridge-регрессия с зависящими от глубины весами квадратичного штрафа [90]. Веса w_k применяются к штрафам коэффициентов GAR-уровней, а не к отдельным обучающим наблюдениям:

$$\mathcal{V}_{\text{train}} = \left\{ v \in \bigcup_{t \in T_{\text{train}}} V_t \colon x(v), x^{(1)}(v), \dots, x^{(P_{\max})}(v) \in \mathbb{R} \right\},$$
$$J(b_0, \varphi) = \sum_{v \in V_{train}} \left(x(v) - b_0 - \sum_{k=1}^{P_{max}} \varphi_k \, x^{(k)}(v) \right)^2 + \lambda \sum_{k=1}^{P_{max}} w_k \, \varphi_k^2, \quad J \to \min_{b_0, \varphi}, \tag{3.44}$$

где $\mathcal{V}_{\text{train}}$ – множество вершин обучающих графовых срезов, для которых исходный сигнал и значения всех шагов GAR-рекурсии являются конечными, $\mathcal{T}_{\text{train}}$– множество индексов обучающих срезов, J – целевая функция, λ – коэффициент регуляризации, $w_k > 0$ – вес штрафа для k-го шага, а φ – вектор коэффициентов. Свободный член b_0не регуляризуется. Классовые метки при оценивании GAR-коэффициентов не используются, поэтому в $\mathcal{V}_{\text{train}}$ могут входить легальные, нелегальные и неразмеченные транзакции.

Оценки параметров определяются как значения, минимизирующие целевую функцию

$$\left(\hat{b}_0, \hat{\varphi}\right) = \arg\min_{b_0, \varphi} J(b_0, \varphi). \tag{3.45}$$

Для явного получения решения задачи (3.45) пронумеруем обучающие вершины $v_1, \dots, v_n$ и введем

$$\mathrm{y} = \begin{pmatrix} x(v_1) \\ \vdots \\ x(v_n) \end{pmatrix}, \qquad Z = \begin{pmatrix} 1 & x^{(1)}(v_1) & \cdots & x^{(P_{\max})}(v_1) \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x^{(1)}(v_n) & \cdots & x^{(P_{\max})}(v_n) \end{pmatrix},$$
$$\theta = (b_0 \quad \varphi_1 \quad \cdots \quad \varphi_{P_{\max}})^{\mathrm{T}}, \qquad W = \mathrm{diag}\left(0, w_1, \dots, w_{P_{\max}}\right).$$

Тогда целевая функция записывается как

$$J(\theta) = \| \mathrm{y} - Z\theta \|_2^2 + \lambda \theta^{\mathrm{T}} W \theta,$$

а нормальные уравнения и их решение имеют вид

$$(\mathrm{Z}^{\mathrm{T}}\mathrm{Z} + \lambda\mathrm{W})\hat{\theta} = \mathrm{Z}^{\mathrm{T}}\mathrm{y}, \qquad \hat{\theta} = (\mathrm{Z}^{\mathrm{T}}\mathrm{Z} + \lambda\mathrm{W})^{-1}\mathrm{Z}^{\mathrm{T}}\mathrm{y}.$$

Приведем выводы для вышесказанного. Рассмотрим матрицу нормальных уравнений

$$H = Z^{\mathrm{T}}Z + \lambda W, \qquad W = \mathrm{diag}\left(0, w_1, \dots, w_{P_{\max}}\right).$$

Нулевой первый диагональный элемент матрицы W означает, что свободный член b_0 не подвергается регуляризации. Пусть $n = |\mathcal{V}_{\mathrm{train}}| \geq 1$, первый столбец матрицы Z, соответствующий свободному члену, равен вектору единиц 1_n, параметр регуляризации удовлетворяет условию $\lambda > 0$, а веса штрафа положительны: $w_k > 0$, $k = 1, \dots, P_{\max}$. При этих условиях матрица H является положительно определенной.

Действительно, для произвольного ненулевого вектора

$$\mathrm{a} = \left(a_0, a_1, \dots, a_{P_{\max}}\right)^{\mathrm{T}} \neq 0$$

справедливо равенство

$$\mathrm{a}^{\mathrm{T}}H\mathrm{a} = \|Z\mathrm{a}\|_2^2 + \lambda \sum_{k=1}^{P_{\max}} w_k\, a_k^2.$$

Если хотя бы одна из координат a_k, $k \geq 1$, отлична от нуля, то вследствие условий $\lambda > 0$ и $w_k > 0$ второе слагаемое строго положительно. Если же $a_1 = \dots = a_{P_{\max}} = 0$, то из условия $\mathrm{a} \neq 0$ следует $a_0 \neq 0$. Поскольку первый столбец Z равен 1_n, получаем

$$\|Z\mathrm{a}\|_2^2 = \|a_0 1_n\|_2^2 = n a_0^2 > 0.$$

Следовательно, для любого $\mathrm{a} \neq 0$ выполняется

$$\mathrm{a}^{\mathrm{T}}H\mathrm{a} > 0, \qquad H \succ 0.$$

Гессиан целевой функции этой взвешенной ridge-регрессии имеет вид

$$\nabla^2 J(\theta) = 2(Z^{\mathrm{T}}Z + \lambda W) = 2H.$$

Таким образом, при непустом обучающем множестве, $\lambda > 0$ и $w_k > 0$ целевая функция $J(\theta)$ является строго выпуклой и имеет единственный минимум [91]. Соответственно, нормальные уравнения имеют единственное решение

$$\hat{\theta} = (Z^{\mathrm{T}}Z + \lambda W)^{-1}Z^{\mathrm{T}}\mathrm{y}.$$

Для усиления регуляризации более удаленных уровней используется следующая монотонная схема весов:

$$w_k = \left(1 + \frac{k-1}{P_{\max}-1}(r_w - 1)\right)^{\gamma}, \qquad k = 1, \dots, P_{\max}, \quad r_w \geq 1, \quad \gamma \geq 0, \quad (3.46)$$

где r_w – параметр усиления штрафа на максимальной глубине, а γ – показатель нелинейности. Формула (3.46) применяется при $P_{\max} > 1$. Если $P_{\max} = 1$, отдельно принимается $w_1 = 1$, поскольку знаменатель $P_{\max} - 1$ обращается в ноль. Параметры r_w и γ являются безразмерными.

Из формулы непосредственно следуют граничные значения

$$w_1 = 1, \qquad w_{P_{\max}} = r_w^{\gamma}, \qquad \frac{w_{P_{\max}}}{w_1} = r_w^{\gamma}.$$

Следовательно, параметр r_w совпадает с отношением последнего веса к первому только при $\gamma = 1$. При $r \geq 1$ и $\gamma \geq 0$ веса не убывают:

$$w_1 \leq w_2 \leq \cdots \leq w_{P_{\max}}. \quad (3.47)$$

Таким образом, параметры r_wи γ определяют величину и нелинейность усиления штрафа для более удаленных шагов GAR-рекурсии.

Пусть максимальная глубина восходящей истории установлена равной $P_{\max} = 2$. Это означает, что при моделировании сигнала транзакции используются два агрегированных уровня: $x^{(1)}(v)$, характеризующий непосредственных предшественников транзакции, и $x^{(2)}(v)$, характеризующий двухшаговую восходящую историю. Пусть для воспроизводимости расчетов принимаются

$$P_{\max} = 2, \qquad \lambda = 10^{-2}, \qquad r_w = 2, \qquad \gamma = 1.$$

При этих значениях из формулы (3.46) получаем $w_1 = 1$и $w_2 = 2$. Следовательно, матрица весов штрафа и регуляризационная матрица имеют вид:

$$W = \mathrm{diag}(0,1,2), \qquad \lambda W = \mathrm{diag}(0, 10^{-2}, 2 \cdot 10^{-2}).$$

Нулевой первый диагональный элемент соответствует свободному члену b_0, который не регуляризуется. Коэффициент первого GAR-уровня φ_1 штрафуется с множителем 10^{-2}, а коэффициент второго уровня φ_2 – с множителем $2 \cdot 10^{-2}$. Следовательно, при прочих равных условиях

коэффициент более удаленного, второго уровня подвергается в два раза более сильному квадратичному штрафу. Это не задает заранее отношение между оценками $\hat{\varphi}_1$ и $\hat{\varphi}_2$, а лишь сильнее ограничивает рост абсолютного значения φ_2 при минимизации целевой функции.

Для $P_{\max} = 2$ целевая функция взвешенной ridge-регрессии полностью раскрывается следующим образом:

$$J(b_0, \varphi_1, \varphi_2) = \sum_{v \in V_{train}} \left(x(v) - b_0 - \varphi_1 x^{(1)}(v) - \varphi_2 x^{(2)}(v)\right)^2 + 10^{-2}\varphi_1^2 + 2 \cdot 10^{-2}\varphi_2^2 \to \min.$$

Таким образом, штрафная часть целевой функции равна:

$$\lambda \sum_{k=1}^{2} w_k \, \varphi_k^2 = 10^{-2}(\varphi_1^2 + 2\varphi_2^2) = 10^{-2}\varphi_1^2 + 2 \cdot 10^{-2}\varphi_2^2.$$

Поскольку в формуле используется сумма квадратов ошибок, а не их среднее значение, $\lambda = 10^{-2}$ относится именно к целевой функции в приведенной форме. Относительное влияние регуляризации зависит от числа обучающих наблюдений и масштаба сигнала x. Поэтому для сопоставимости результатов преобразование каждого исходного сигнала, способ формирования обучающего множества и правило обработки пропущенных значений должны быть одинаковыми во всех сравниваемых экспериментальных запусках.

Итоговый GAR-блок строится как:

$$\mathbf{x}_v^{GAR} = \underset{x \in \mathcal{X}}{\text{concat}}\left[x^{(1)}(v), \ldots, x^{(P_{\max})}(v), \hat{x}(v), r(v)\right], \qquad (3.48)$$

где $\mathcal{X}$ – определенное выше множество семи скалярных транзакционных сигналов, $x^{(k)}(v)$ – значение сигнала на k-м уровне восходящей истории транзакции v, $\hat{x}(v)$ обозначает ожидаемое значение, $r(v)$ показывает отклонение наблюдаемого значения от этого ожидания.

При $P_{\max} = 2$ для каждого из семи сигналов формируются два значения GAR-уровней, одно ожидаемое значение и один остаток. Поэтому итоговый GAR-блок содержит $7 \cdot (2 + 1 + 1) = 28$ признаков. GAR-блок характеризует агрегированную предшествующую транзакционную историю, ожидаемое значение сигнала и отклонение наблюдаемого значения от ожидаемого. Крупный остаток указывает на расхождение между текущей транзакцией и значением, ожидаемым на основе ее предшественников.

Экспериментальный дизайн

Эксперимент основан на сравнении двух наборов признаков. Базовый набор содержит 26 транзакционных и графовых признаков. Расширенный набор включает 87 признаков: к базовым добавлен 61 признак, характеризующий

локальное отклонение от окружения, динамику последующего расходования и предшествующую транзакционную историю.

Для оценки влияния криминалистических дескрипторов были обучены восемь ансамблевых моделей: CatBoost, LightGBM, XGBoost, HistGradientBoosting, GradientBoosting, Random Forest, Balanced Bagging и ExtraTrees. Это позволяет проверить, сохраняется ли эффект расширенного представления для разных алгоритмов, а не только для одного классификатора. Методы на основе деревьев выбраны из-за их пригодности для табличных признаков разного масштаба, способности моделировать нелинейные зависимости и возможности последующего анализа важности [47, 92, 93, 94].

Эксперименты проводились на 48 239 размеченных транзакциях, для которых удалось восстановить ончейн-признаки. Данные охватывали 49 временных периодов, для каждого из которых строился отдельный граф. Графовые признаки рассчитывались с учетом всех транзакций соответствующего графа, включая объекты с меткой unknown. При обучении моделей использовались только транзакции с известными метками. Протокол включал 10 повторных разбиений 49 графовых срезов с начальными значениями генератора случайных чисел 42–51. В каждом запуске целые срезы распределялись между обучающей и тестовой частями в соотношении 70/30, в обеих частях требовалось присутствие двух классов. Для всех сравниваемых моделей и конфигураций признаков использовались одни и те же десять разбиений.

Дисбаланс классов учитывался для всех моделей с использованием встроенных механизмов весовой компенсации, предусмотренных соответствующими алгоритмами. Конкретная реализация взвешивания зависела от классификатора, однако во всех экспериментах повышенный вес присваивался объектам менее представленного класса. Обработка пропущенных значений зависела от используемого классификатора. Для CatBoost, LightGBM, HistGradientBoosting и XGBoost пропущенные значения сохранялись в формате NaN и обрабатывались встроенными механизмами соответствующих моделей. Для GradientBoosting, Random Forest, ExtraTrees и Balanced Bagging перед обучением применялось медианное заполнение. Медианы вычислялись только по размеченным транзакциям обучающих графовых срезов каждого запуска и без повторной оценки применялись к тестовой части.

PageRank, HITS и собственновекторная центральность вычислялись итерационными методами с фиксированным числом итераций. Коэффициенты GAR оценивались по объединенным обучающим графам и затем без пересчета применялись к тестовым данным.

Качество выявления транзакций класса illicit оценивалось по Precision, Recall, F1-score и PR-AUC. PR-AUC рассчитывалась как Average Precision по вероятностным прогнозам модели. Для вычисления остальных показателей и матрицы ошибок использовался фиксированный порог 0,5, который не подбирался по тестовым данным.

3.5 Результаты экспериментов

Результаты на базовом наборе признаков

В таблице 3.3 показаны средние значения метрик по итогам десяти запусков моделей с базовым набором из 26 признаков. Он объединяет 17 характеристик самой транзакции и 9 показателей ее положения в графе.

Таблица 3.3 – Качество моделей на базовом наборе из 26 признаков

Модель	PR-AUC illicit, %	Precision illicit, %	Recall illicit, %	F1-score illicit, %
CatBoost	85,10	77,49	75,57	76,44
LightGBM	84,35	82,26	72,43	76,96
XGBoost	82,93	87,99	65,70	75,10
HistGradientBoosting	84,29	90,14	67,11	76,82
GradientBoosting	81,27	88,86	65,02	74,95
Random Forest	83,38	93,52	61,60	74,15
BaggingTreeBalanced	79,92	89,71	62,75	73,74
ExtraTrees	80,19	94,04	56,80	70,74

На базовом наборе CatBoost показал лучшие значения PR-AUC и Recall 85,10% и 75,57% соответственно. Максимальный F1-score, равный 76,96%, получил LightGBM. Различия по F1-score между LightGBM, HistGradientBoosting и CatBoost невелики, однако CatBoost обеспечивает более высокое значение Recall, что важно на этапе первичного выявления транзакций, требующих проверки.

На рисунке 3.3 видно, что Random Forest и ExtraTrees показали наибольшую Precision, составившую 93,52% и 94,04% соответственно. При этом их Recall оказалась ниже и составила 61,60% и 56,80%. Эти модели реже ошибочно относили транзакции к классу illicit, но пропускали большую долю транзакций этого класса.

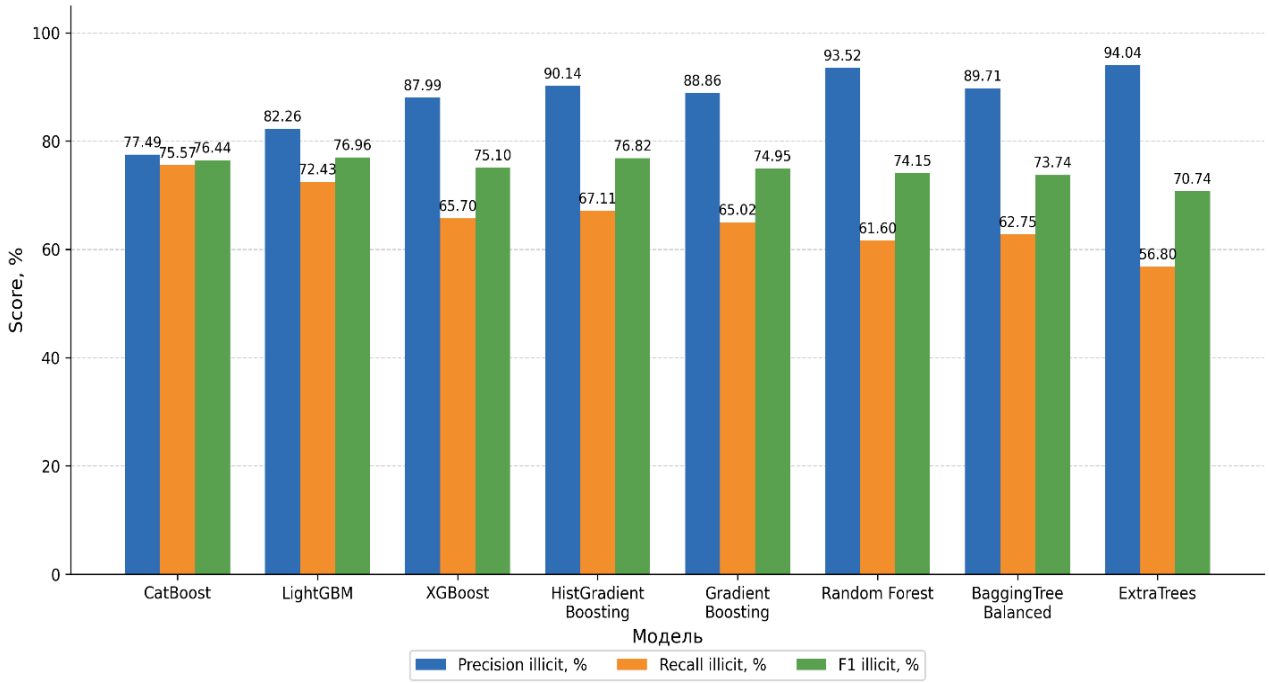


Рисунок 3.3 – Сравнение моделей на базовом наборе

Базовый набор позволяет классифицировать транзакции без использования анонимизированных признаков Elliptic. Однако эти признаки в основном описывают саму транзакцию и ее положение в графе, но слабее учитывают локальные отклонения, последующее расходование и предшествующую транзакционную историю. Поэтому этот набор используется для оценки вклада новых криминалистических дескрипторов.

Результаты на расширенном наборе признаков

В таблице 3.4 приведены результаты моделей на расширенном наборе из 87 признаков. Помимо характеристик транзакции и ее положения в графе, в него вошли дескрипторы локального отклонения от окружения, последующего расходования и предшествующей транзакционной истории.

Таблица 3.4 – Качество моделей на расширенном наборе из 87 признаков

Модель	PR-AUC illicit, %	Precision illicit, %	Recall illicit, %	F1-score illicit, %
CatBoost	90,27	87,04	81,11	83,90
LightGBM	89,54	90,96	76,50	83,04
XGBoost	87,81	93,37	71,56	80,96
HistGradientBoosting	87,82	93,98	71,11	80,89
GradientBoosting	85,12	92,73	68,40	78,69
Random Forest	86,67	95,88	65,64	77,85
BaggingTreeBalanced	82,04	92,57	63,12	74,94
ExtraTrees	83,89	93,61	59,57	72,74

Как показано на рисунке 3.4, лучшие результаты у CatBoost, PR-AUC составил 90,27%, Precision 87,04%, F1-score 83,90%. LightGBM имеет более высокую Precision, но более низкий Recall, чем CatBoost. CatBoost допускает больше ложноположительных решений, однако реже пропускает нелегальные транзакции и достигает более высокого F1-score.

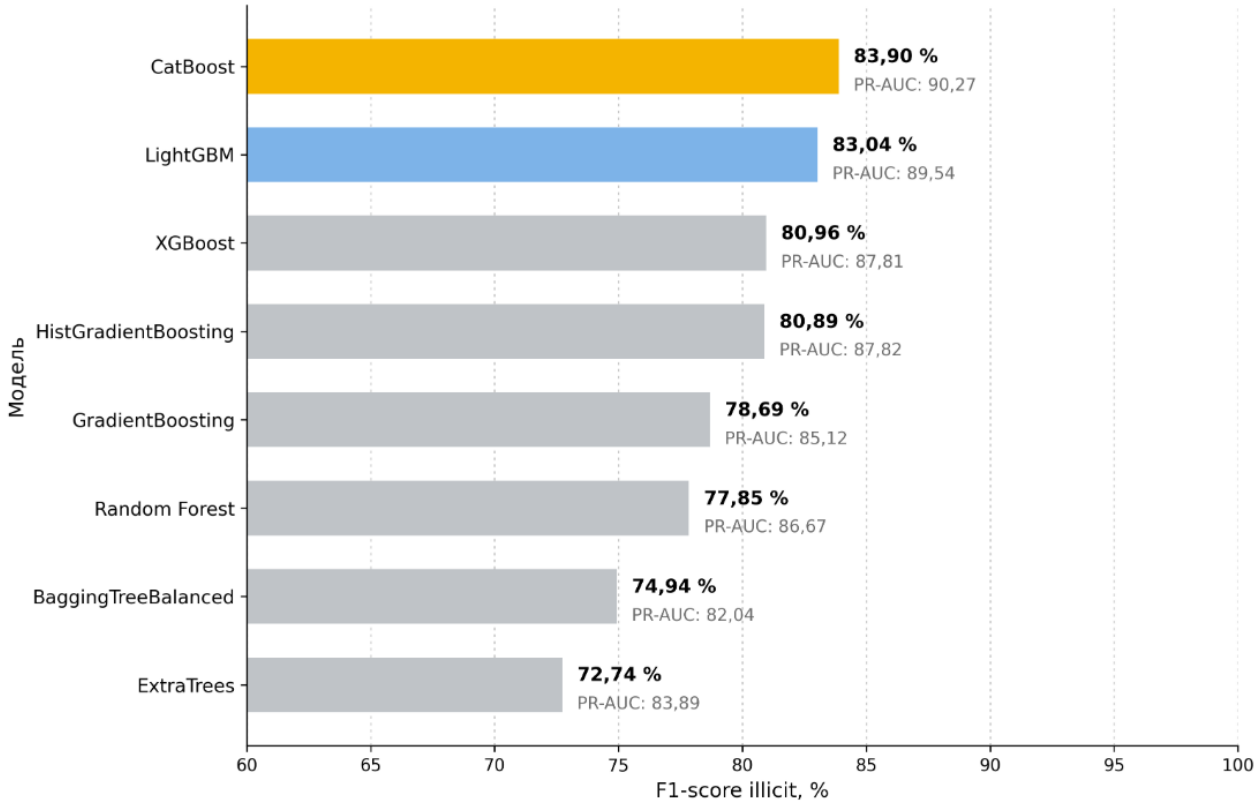


Рисунок 3.4 – Сравнение моделей на расширенном наборе

Random Forest и ExtraTrees действуют более осторожно. Их высокий Precision означает, что большинство отмеченных ими нелегальных транзакций действительно являются такими. Но низкий Recall означает, что значительная часть нелегальных транзакций остается необнаруженной. На этапе первичного отбора целесообразно снижать число пропущенных нелегальных транзакций, даже если это сопровождается умеренным увеличением числа ложных срабатываний. Такие сигналы могут быть дополнительно проверены аналитиком, тогда как пропущенная нелегальная транзакция не попадет в последующий анализ. При этом чрезмерное количество ложных срабатываний также нежелательно, поскольку увеличивает нагрузку на экспертов.

После добавления новых дескрипторов модель учитывает параметры транзакции, ее связи с соседними операциями, динамику последующего расходования и отклонения характеристик от предшествующей транзакционной истории. Это позволяет определить, какие характеристики повлияли на результат классификации, и использовать их при последующем криминалистическом анализе.

Сравнение базового и расширенного наборов признаков

В таблице 3.5 приведено сравнение результатов на базовом и расширенном наборах признаков. Изменения PR-AUC и F1-score представлены на рисунках 3.5 и 3.6 соответственно.

Таблица 3.5 – Сравнение результатов на базовом и расширенном наборах признаков

Модель	PR-AUC Base, %	PR-AUC Extended, %	Δ PR-AUC, п.п.	F1 Base, %	F1 Extended, %	Δ F1, п.п.
CatBoost	85,10	90,27	+5,17	76,44	83,90	+7,46
LightGBM	84,35	89,54	+5,19	76,96	83,04	+6,08
XGBoost	82,93	87,81	+4,88	75,10	80,96	+5,86
HistGradientBoosting	84,29	87,82	+3,53	76,82	80,89	+4,07
GradientBoosting	81,27	85,12	+3,85	74,95	78,69	+3,74
Random Forest	83,38	86,67	+3,29	74,15	77,85	+3,70
BaggingTreeBalanced	79,92	82,04	+2,12	73,74	74,94	+1,20
ExtraTrees	80,19	83,89	+3,70	70,74	72,74	+2,00

После добавления новых дескрипторов значения PR-AUC и F1-score повысились у всех восьми моделей. Средний прирост PR-AUC составил 3,97 п. п., F1-score 4,26 п. п., Recall 3,76 п. п., Precision 4,52 п. п. Наибольшее увеличение F1-score получено для CatBoost и составило 7,46 п. п. На расширенном наборе CatBoost также показал лучшие значения PR-AUC, Recall и F1-score.

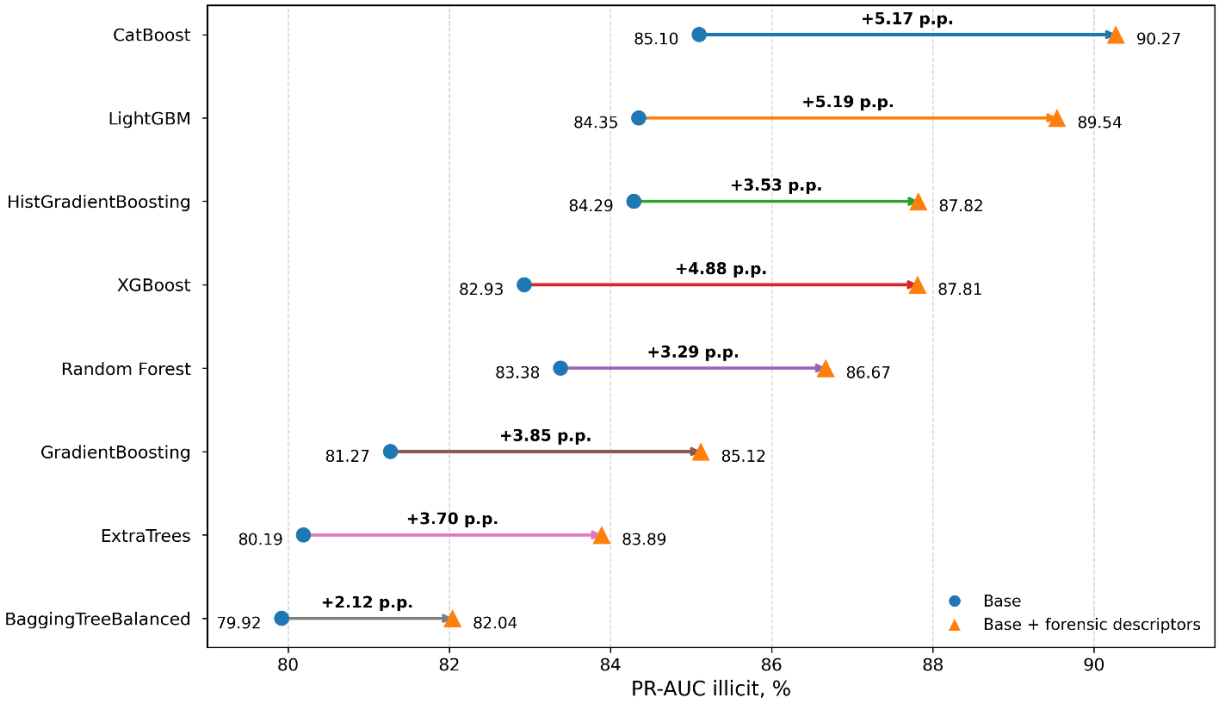


Рисунок 3.5 – Сравнение PR-AUC класса illicit на базовом и расширенном наборах признаков

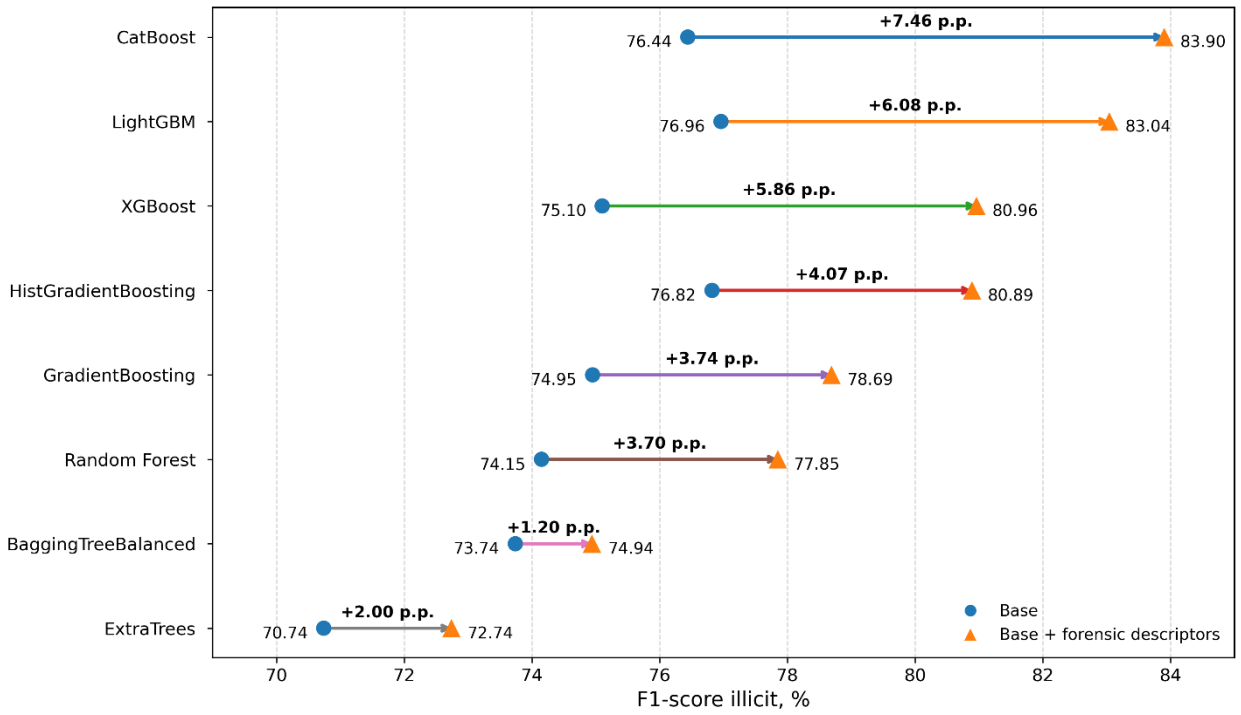


Рисунок 3.6 – Сравнение F1-score класса illicit на базовом и расширенном наборах признаков

Рост PR-AUC и F1-score у всех восьми моделей показывает, что криминалистические дескрипторы содержат дополнительную информацию, полезную для выявления нелегальных транзакций.

Сравнение с графовыми и гибридными базовыми моделями

Для дополнительной проверки результатов CatBoost на расширенном наборе признаков проведено сравнение с графовыми и гибридными моделями.

Все модели оценивались на одних и тех же десяти разбиениях данных. Для них использовались одинаковые обучающие и тестовые маски и единый набор метрик. Вершины с меткой unknown сохранялись в графах, но не учитывались при вычислении функции потерь и оценке качества. Все графовые модели обучались на расширенном наборе из 87 признаков. Для каждого разбиения параметры GNN, GraphMAE и DGI оценивались только по обучающим графовым срезам. Результаты сравнения приведены в таблице 3.6 и на рисунке 3.7.

Таблица 3.6 – Сравнение с графовыми и гибридными моделями

Модель	Семейство	PR-AUC illicit, %	Precision illicit, %	Recall illicit, %	F1-score illicit, %
GCN	GNN	53,43	27,43	70,10	39,43
GraphSAGE	GNN	55,22	31,65	72,33	44,03
APPNP	GNN	52,95	28,09	69,38	39,99
H2GCN	GNN	54,08	33,44	69,86	45,22
SGFormer	графовый трансформер	61,72	43,27	69,22	53,25

Продолжение таблицы 3.6

GraphMAE + CatBoost	гибридные графовые вложения	85,92	78,26	75,52	76,87
DGI + CatBoost	гибридные графовые вложения	83,47	75,90	72,09	73,95
CatBoost	интерпретируемая дескрипторная модель	90,27	87,04	81,11	83,90

GNN-модели обнаруживают значительную часть нелегальных транзакций, но при этом допускают больше ложных срабатываний на легальных транзакциях. Это повышает Recall, однако снижает Precision и F1-score. При практическом применении такое соотношение увеличивает число транзакций, требующих ручной проверки.

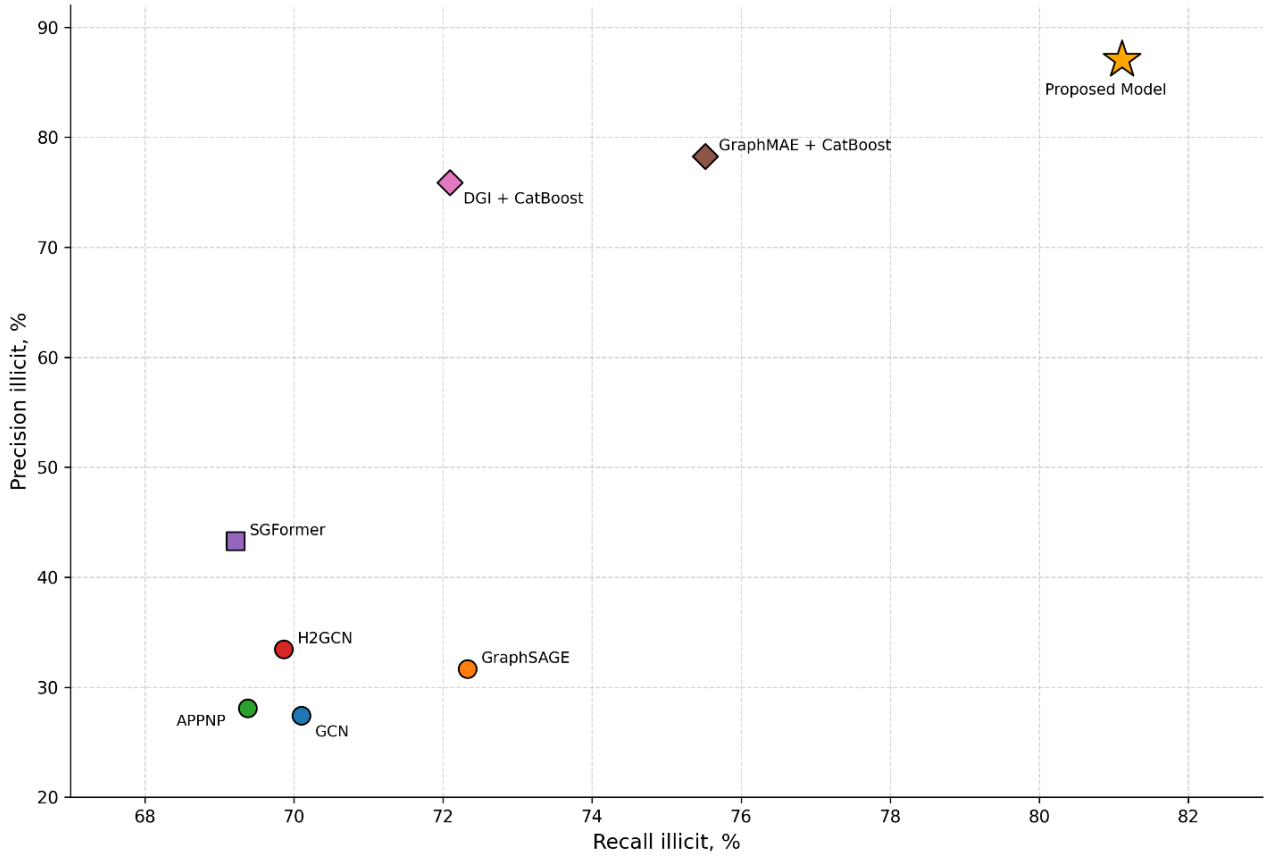


Рисунок 3.7 – Сравнение моделей по Precision и Recall класса illicit

Модели GraphMAE + CatBoost и DGI + CatBoost показали лучшие результаты по сравнению с самостоятельными GNN. В этих подходах графовые вложения передаются в табличный классификатор, что повышает качество классификации. Однако их показатели остались ниже результатов CatBoost.

Анализ вклада трех групп криминалистических дескрипторов

Для оценки вклада новых признаков проведен абляционный анализ CatBoost. Из полной модели поочередно исключались признаки локального

окружения, GAR-признаки и признаки временной динамики. Поочередное исключение групп позволяет оценить вклад каждой группы в присутствии остальных дескрипторов. Результаты приведены в таблице 3.7.

Таблица 3.7 – Абляционный анализ криминалистических дескрипторов

Конфигурация	Удаленная группа	PR-AUC illicit, %	Precision illicit, %	Recall illicit, %	F1-score illicit, %	Δ PR-AUC, п.п.	Δ F1, п.п.
Все признаки	нет	90,27	87,04	81,11	83,90	–	–
Ablation 1	Локальное отклонение	86,97	80,82	77,02	78,79	−3,30	−5,11
Ablation 2	GAR	89,18	86,29	79,24	82,56	−1,09	−1,34
Ablation 3	Последующее расходование	89,98	86,62	80,44	83,34	−0,29	−0,56

На рисунке 3.8 показано снижение PR-AUC и F1-score при удалении отдельных групп дескрипторов. Наибольшее падение наблюдается без признаков локального окружения: PR-AUC снижается с 90,27% до 86,97%, F1-score с 83,90% до 78,79%. Следовательно, важны не только абсолютные значения признаков, но и их несоответствие ближайшему окружению.

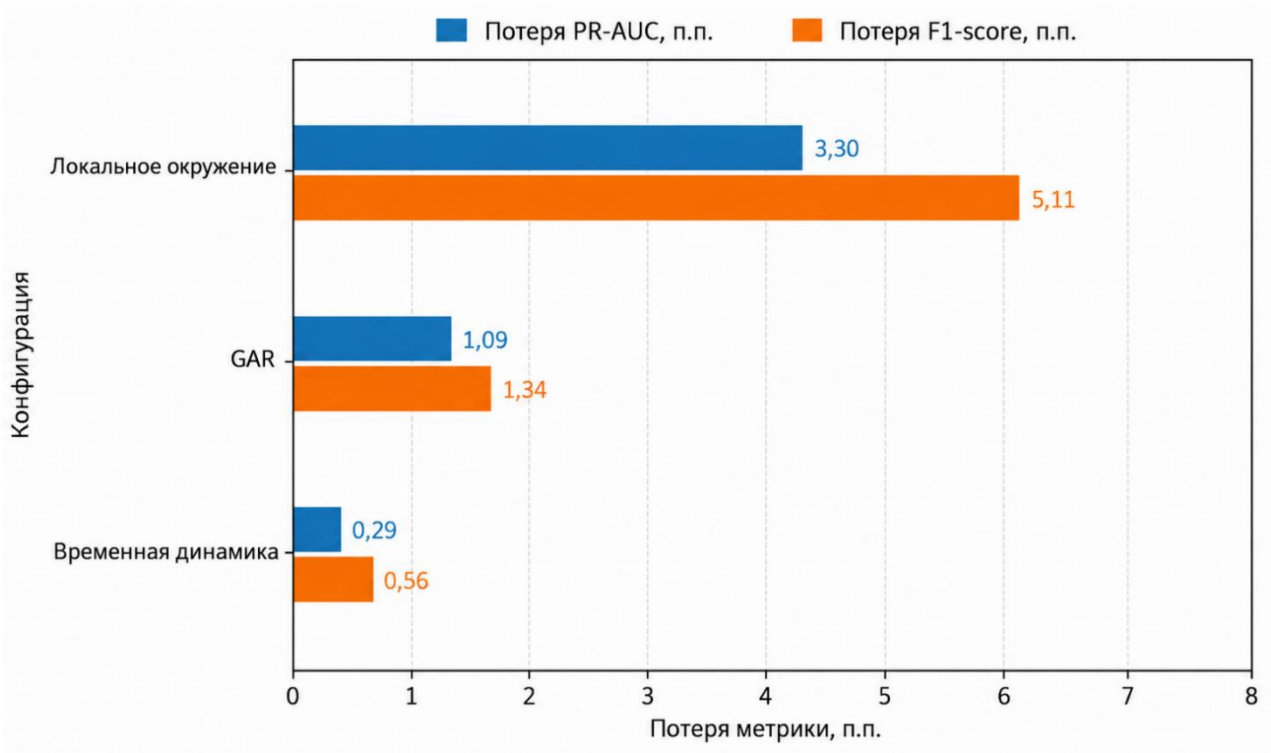


Рисунок 3.8 – Снижение PR-AUC и F1-score при удалении групп криминалистических дескрипторов

Удаление GAR-признаков приводит к более умеренному снижению: PR-AUC на 1,09 п. п., F1-score на 1,34 п. п. Это подтверждает дополнительную ценность информации о предшествующей истории движения средств. Признаки

временной динамики имеют наименьший самостоятельный вклад: при их удалении PR-AUC снижается на 0,29 п. п., F1-score на 0,56 п. п. В данной постановке они выступают как вспомогательный источник контекста. Поскольку полная конфигурация показывает лучший результат, все три группы сохраняются в итоговом представлении.

3.6 Предложенная модель и интерпретация результатов

По результатам сравнительного анализа для выявления нелегальных Bitcoin-транзакций выбрана модель CatBoost, показавшая лучшие результаты среди рассмотренных моделей. Полученное преимущество можно связать с тем, что модель учитывает нелинейные зависимости и взаимодействия между разнородными табличными признаками, обрабатывает пропущенные значения без их предварительного заполнения и поддерживает балансировку весов классов. Эти свойства особенно важны для сформированного набора данных, в котором признаки имеют различную природу, а значения NaN отражают отсутствие локального окружения, последующего расходования выходов или предшествующей транзакционной истории.

На вход модели подается вектор из 87 признаков:

$$x_v = \left[x_v^{tx}, x_v^{topo}, x_v^{nbr}, x_v^{temp}, x_v^{GAR}\right] \in (\mathbb{R} \cup \{\text{NaN}\})^{87},$$

который включает транзакционные, структурно-графовые, локальные, временные и GAR-признаки. Состав признаков и порядок их расчета приведены в подразделах 3.2 и 3.4.

Модель обучалась в течение 400 итераций с глубиной деревьев 8 и скоростью обучения 0,1. Дисбаланс между легальными и нелегальными транзакциями учитывался с помощью автоматической балансировки весов классов.

Результаты отдельных деревьев последовательно объединяются в итоговую оценку модели:

$$F(x_v) = b + \sum_{m=1}^{400} 0{,}1\ T_m(x_v), \qquad (3.49)$$

где b – начальное значение модели, $T_m(x_v)$– результат m-го дерева решений. Полученная оценка преобразуется в распределение вероятностей по двум классам, после чего выбирается класс с наибольшей вероятностью:

$$F(x_v) \to \begin{bmatrix} P(\text{легальная} \mid x_v) \\ P(\text{нелегальная} \mid x_v) \end{bmatrix} \to \arg\max \to \hat{y}_v.$$

Архитектура предложенной модели представлена на рисунке 3.9.

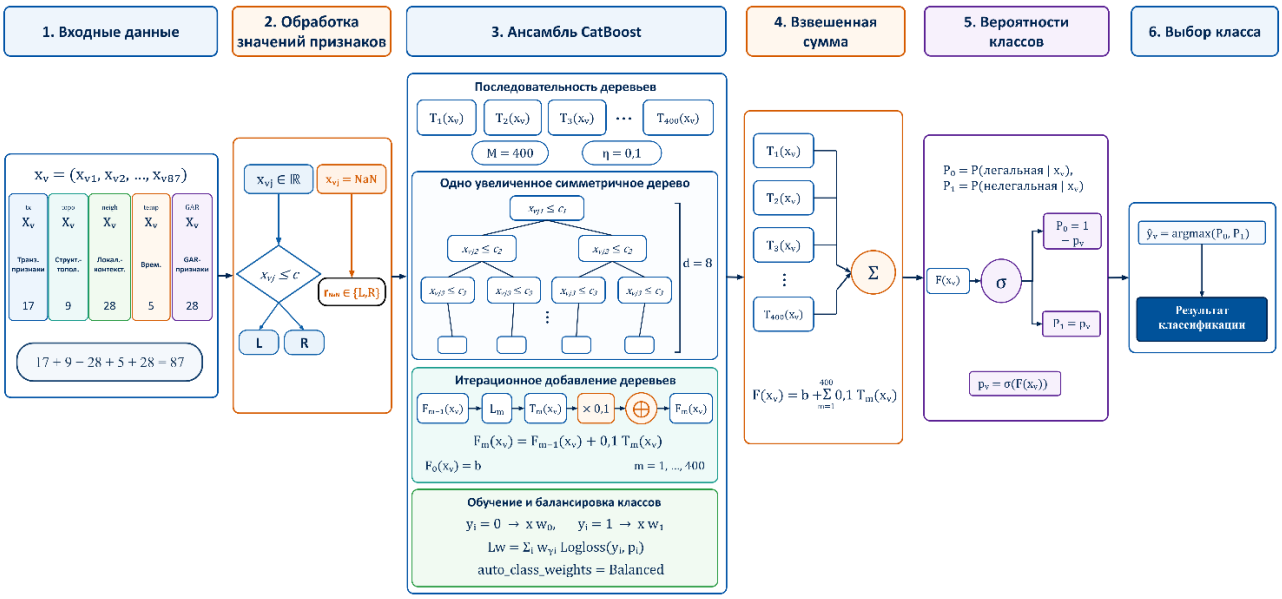


Рисунок 3.9 – Архитектура предложенной модели

Интерпретация важности признаков

Для предложенной модели были рассчитаны SHAP-значения и модельная важность PredictionValuesChange. SHAP-атрибуции позволяют оценить вклад каждого признака в решение модели [41]:

$$f(x_v) = \phi_0 + \sum_{j=1}^{m} \phi_j\,(v). \tag{3.50}$$

где $f(x_v)$ - значение модели для транзакции v, ϕ_0 - базовое значение, $\phi_j(v)$ - вклад признака j в конкретное предсказание, m - число признаков.

Оба способа оценки важности дали близкое ранжирование признаков: коэффициент ранговой корреляции Спирмена составил около 0,94. На рисунке 3.10 показано, что наиболее значимыми являются fee_rate и size, за которыми следуют max_share_out, gar_resid_num_output_addresses, gar_resid_size и weak_cc_size.

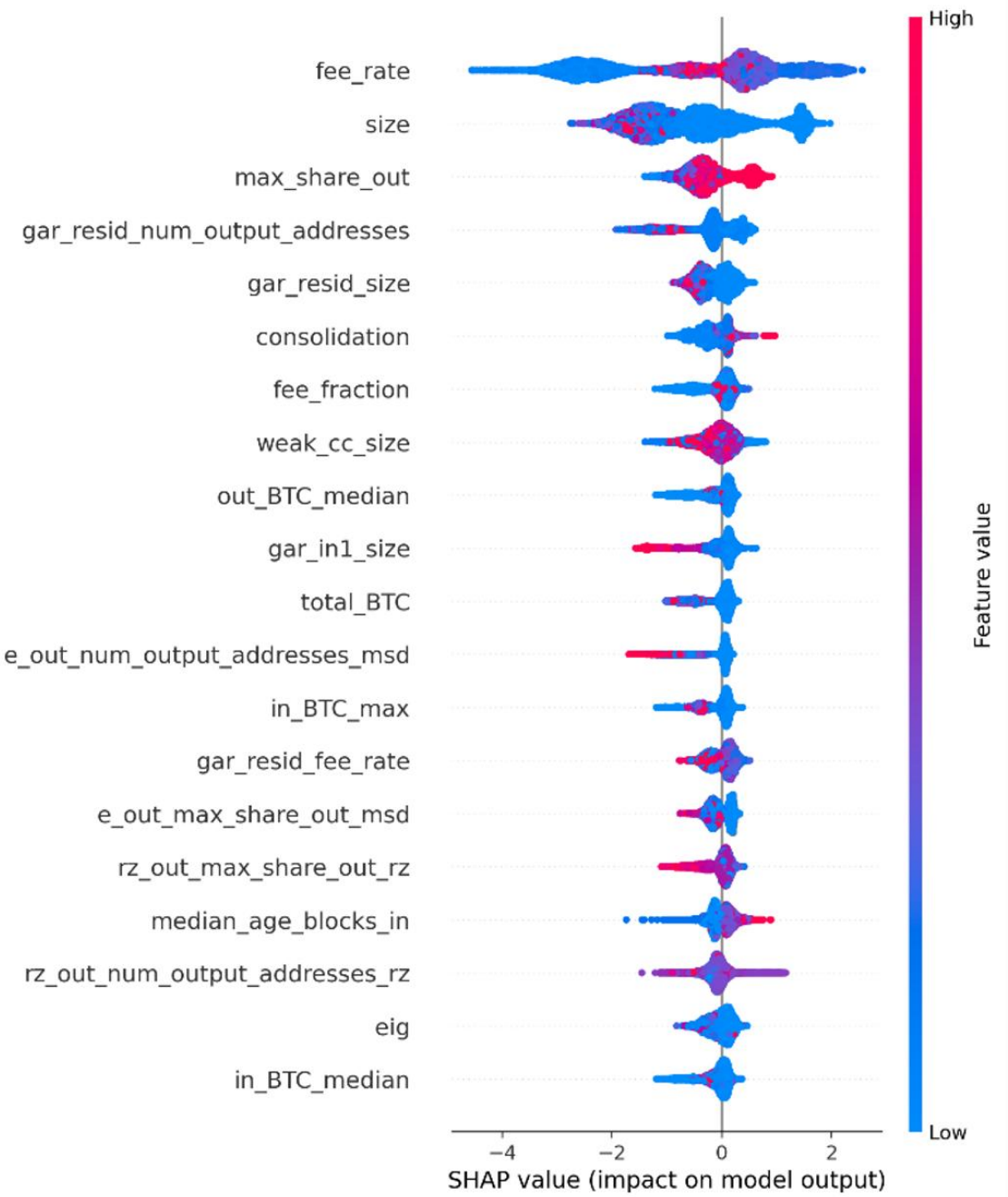


Рисунок 3.10 – Распределение SHAP-значений для 20 наиболее важных признаков модели CatBoost

Распределение важности признаков показывает, что модель опирается на базовые характеристики транзакции, ее предшествующую транзакционную историю и положение в графе. На криминалистические дескрипторы пришлось 45,8% суммарной средней абсолютной SHAP-оценки и 46,4% PredictionValuesChange. Основной вклад внутри этой группы внесли GAR-признаки и характеристики локального окружения, тогда как влияние временных характеристик было слабее. Такой анализ помогает перейти от общей оценки «модель так решила» к пониманию конкретных причин принятого решения. Этот вывод также подтверждается результатами абляционного анализа: исключение новых дескрипторов приводит к снижению точности модели.

Анализ ошибок

Для анализа ошибок использовались результаты предложенной модели на расширенном наборе признаков при seed 42. На тестовой выборке модель пропустила 175 нелегальных транзакций и ошибочно отнесла к ним 206 легальных транзакций. Матрица ошибок представлена на рисунке 3.11.

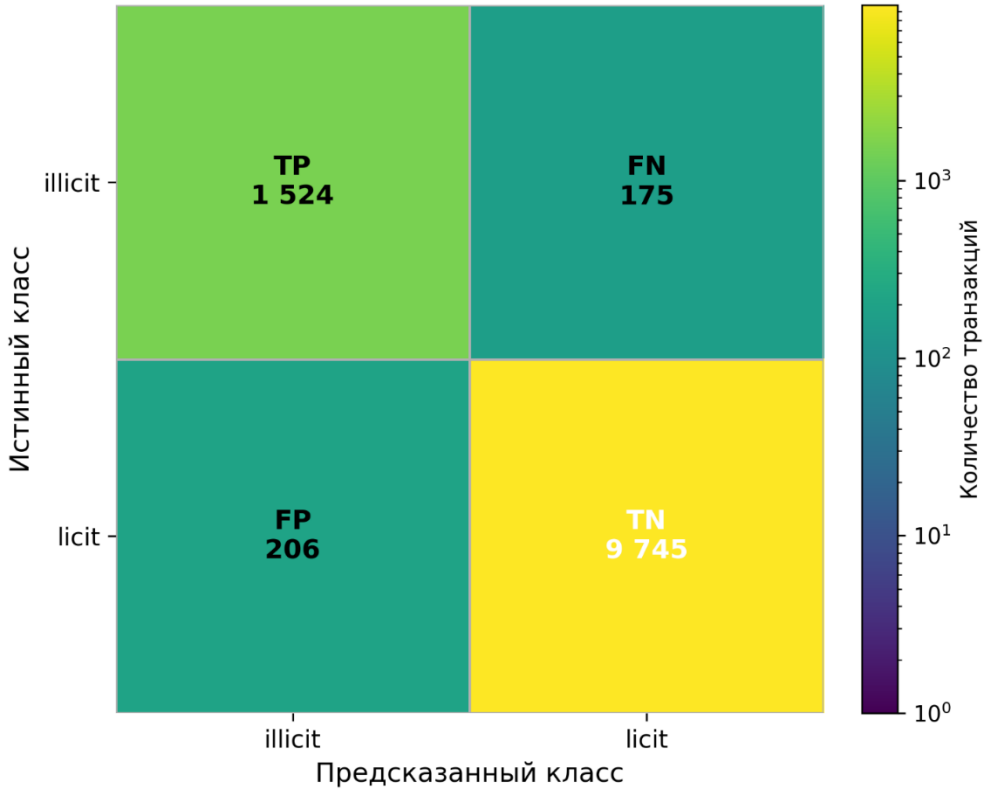


Рисунок 3.11 – Матрица ошибок модели CatBoost

Чаще всего модель пропускала транзакции с небольшим числом связей, которые почти не отличались от соседних. Их суммы, комиссии, количество входов и выходов были близки к значениям соседей. После таких транзакций не наблюдалось быстрого движения средств, а значения GAR оставались низкими. Поэтому по имеющимся признакам модели было сложно отличить эти транзакции от обычных.

Причина, по которой такие транзакции были отнесены к нелегальным, могла быть связана с информацией, отсутствующей в используемых данных. Например, транзакция могла получить такую метку из-за связи адреса с известным сервисом или на основании результатов предыдущих расследований. Эти сведения не входили в набор признаков, поэтому модель не могла учитывать их при классификации. Для этого используется адресная криминалистика, описание которой приведено в следующей главе.

Что касается 206 легальных транзакций, которые модель ошибочно классифицировала как illicit, то эти транзакции заметнее выделялись среди соседних транзакций. Для них были характерны необычная структура связей, быстрое последующее перемещение средств, резкие изменения отдельных параметров и крупные GAR-остатки.

Такой набор признаков встречается не только при нелегальной деятельности, но и при массовых выводах средств, консолидации UTXO, внутренних переводах бирж и других сервисов. По разметке датасета такие случаи считаются ошибочными, хотя выявленное сочетание признаков может дать основание для отдельной проверки.

Полученные ошибки показывают границы модели. Она хорошо распознает транзакции, которые заметно отличаются от соседних транзакций по структуре графа и предшествующему движению средств. Если такая разница выражена слабо, вероятность пропуска возрастает. По этой причине модель лучше использовать как инструмент первичного отбора: она помогает выделить транзакции, которые нужно в дальнейшем изучать детальнее.

Вычислительная эффективность и применимость

Эксперименты проводились на ноутбуке под управлением 64-разрядной операционной системы Windows, оснащенном процессором Intel Core i7-1065G7 с тактовой частотой 1,30 ГГц и 16 ГБ оперативной памяти.

Извлечение основного набора признаков заняло 67,14 с, или около 1,39 мс на одну транзакцию. Калибровка GAR потребовала еще 19,34 с. Весь этап подготовки признаков продолжался 86,48 с, что соответствует примерно 1,79 мс на транзакцию. Обучение CatBoost заняло 23,17 с. После формирования набора признаков классификация одной транзакции выполнялась примерно за 2,05 мс. Пиковое потребление памяти составило 341 МБ. Указанное время относится к локальному расчету признаков после загрузки данных. В текущем виде метод подходит для офлайн-расследований и регулярного пакетного анализа.

3.7 Выводы по разделу 3

В третьей главе сформировано криминалистически интерпретируемое представление Bitcoin-транзакций без использования 166 анонимизированных признаков Elliptic. На основе открытых данных блокчейна, графовой структуры и разметки Elliptic получен расширенный набор из 87 признаков, включающий 26 транзакционных и структурно-графовых характеристик и 61 криминалистически интерпретируемый дескриптор.

В данной главе получены два новых научных результата. Первая научная новизна состоит в разработке системы криминалистически интерпретируемых признаков Bitcoin-транзакций, включающей признаки локального отклонения от окружения, временные признаки последующего расходования и признаки предшествующей транзакционной истории. Вторая научная новизна заключается в разработке модели выявления нелегальных Bitcoin-транзакций, представляющей собой целостную вычислительную схему, которая включает формирование открытых транзакционных, структурно-графовых и криминалистически интерпретируемых признаков, их совместную обработку ансамблевым классификатором и интерпретацию результата по вкладу

отдельных характеристик. Модель исключает зависимость от анонимизированных признаков Elliptic и обеспечивает воспроизводимый расчет входных характеристик по данным публичного блокчейна.

Добавление разработанных криминалистических признаков улучшило выявление нелегальных транзакций у всех восьми классификаторов. В среднем PR-AUC увеличился на 3,97 п. п., а F1-score на 4,26 п. п. Для CatBoost прирост составил 5,17 и 7,46 п. п. соответственно. На расширенном наборе эта модель достигла PR-AUC 90,27% и F1-score 83,90%. Абляционный анализ и оценка важности признаков подтвердили вклад разработанных характеристик в результат классификации.

Полученная модель предназначена для первичного выявления транзакций, требующих дальнейшей проверки, и положена в основу гибридного киберкриминалистического инструментария, представленного в следующей главе.

4 ГИБРИДНАЯ СИСТЕМА КИБЕРКРИМИНАЛИСТИЧЕСКОГО АНАЛИЗА BITCOIN-ТРАНЗАКЦИЙ

В главе разработана архитектура гибридной системы киберкриминалистического анализа Bitcoin-транзакций, включающая модель из главы 3, адресную проверку, поведенческие индикаторы и анализ локального графового окружения. Описаны используемые источники адресной информации, условия определения индикаторов, порядок объединения результатов и программная реализация архитектуры.

4.1 Архитектура гибридной системы анализа Bitcoin-транзакций

Предложенная гибридная архитектура состоит из двух основных функциональных модулей. Первый модуль обрабатывает транзакцию: загружает исходные данные, восстанавливает транзакционный граф, рассчитывает признаки и передает их в модель, разработанную в главе 3. Второй модуль исследует связанные адреса, выполняет поиск по доступным источникам атрибуции, анализирует историю активности и проверяет ближайшее графовое окружение. Структура архитектуры показана на рисунке 4.1.

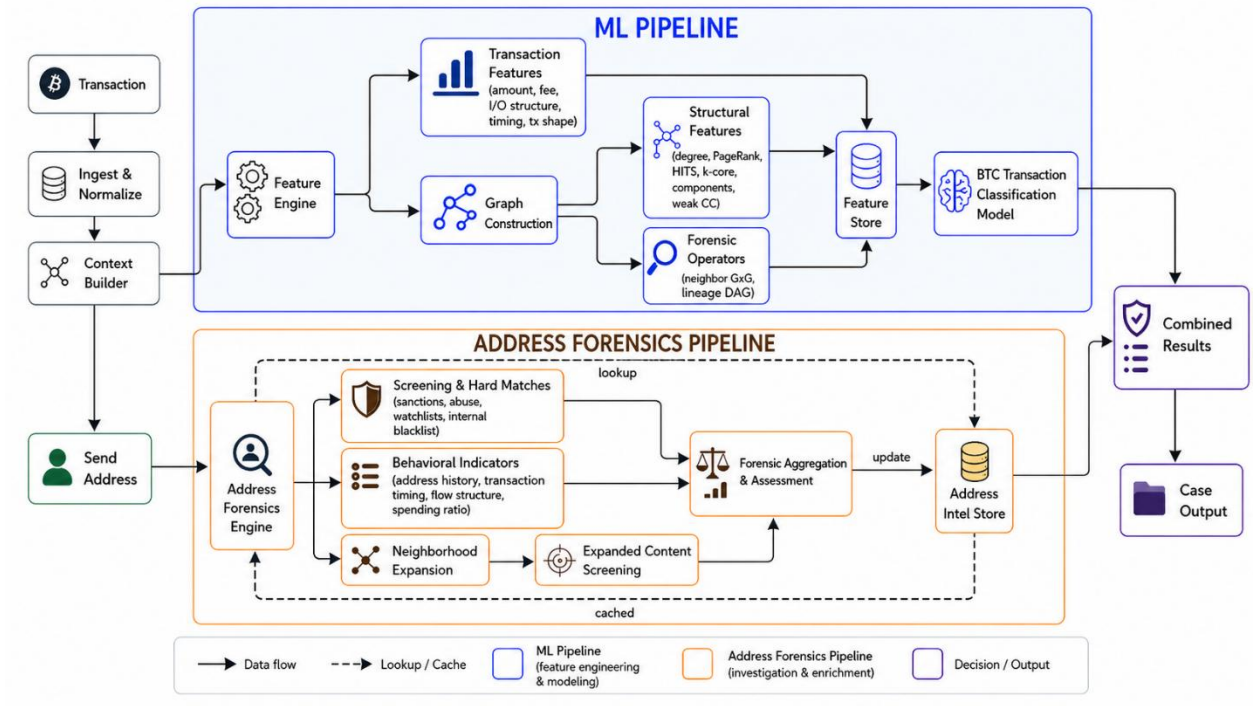


Рисунок 4.1 – Общая логика гибридной архитектуры анализа Bitcoin-транзакции

В модельной ветви обработка начинается с идентификатора исследуемой транзакции. По времени ее включения в блок определяется временной интервал, в пределах которого загружаются связанные транзакции и формируется направленный транзакционный граф, схематично представленный

на рисунке 4.2. Границы временного интервала и правила включения транзакций и связей соответствуют схеме формирования графовых срезов, использованной при обучении модели. На полученном графе рассчитываются транзакционные, структурные, локально-контекстные, временные и GAR-признаки, после чего в модель передается набор признаков исследуемой транзакции.

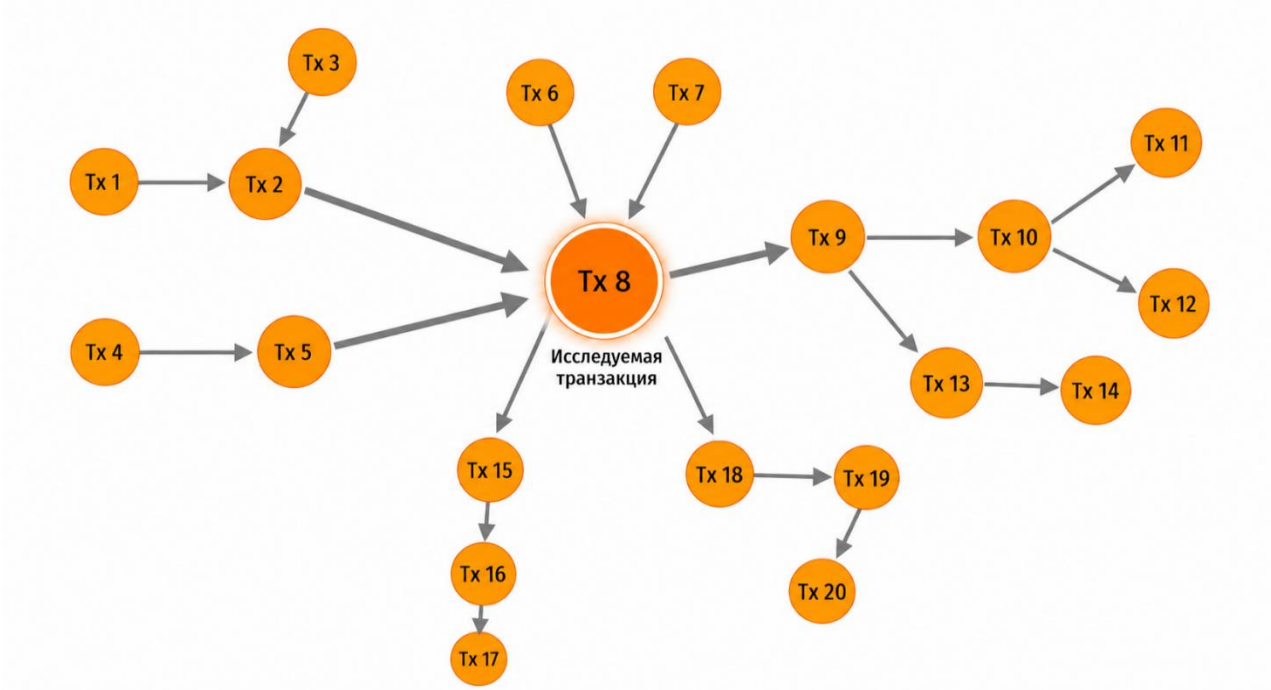


Рисунок 4.2 – Схематичное представление направленного транзакционного графа

Для адресного анализа используется локальный граф «транзакция–адрес». Он включает исследуемую транзакцию, связанные адреса и соседние транзакции. Граф используется для анализа ближайшего окружения адресов и визуализации движения средств.

4.2 Хранилище данных об адресах Bitcoin и проверка источников

При адресной проверке из входов и выходов транзакции извлекаются связанные с ней адреса. Для каждого адреса в пределах заданного временного окна анализируются предыдущие и последующие переводы, периоды активности и ближайшее графовое окружение. Такой анализ позволяет выявлять транзитное перемещение средств, их распределение между несколькими адресами, концентрацию поступлений и вывод средств. Последовательность проверки показана на рисунке 4.3.

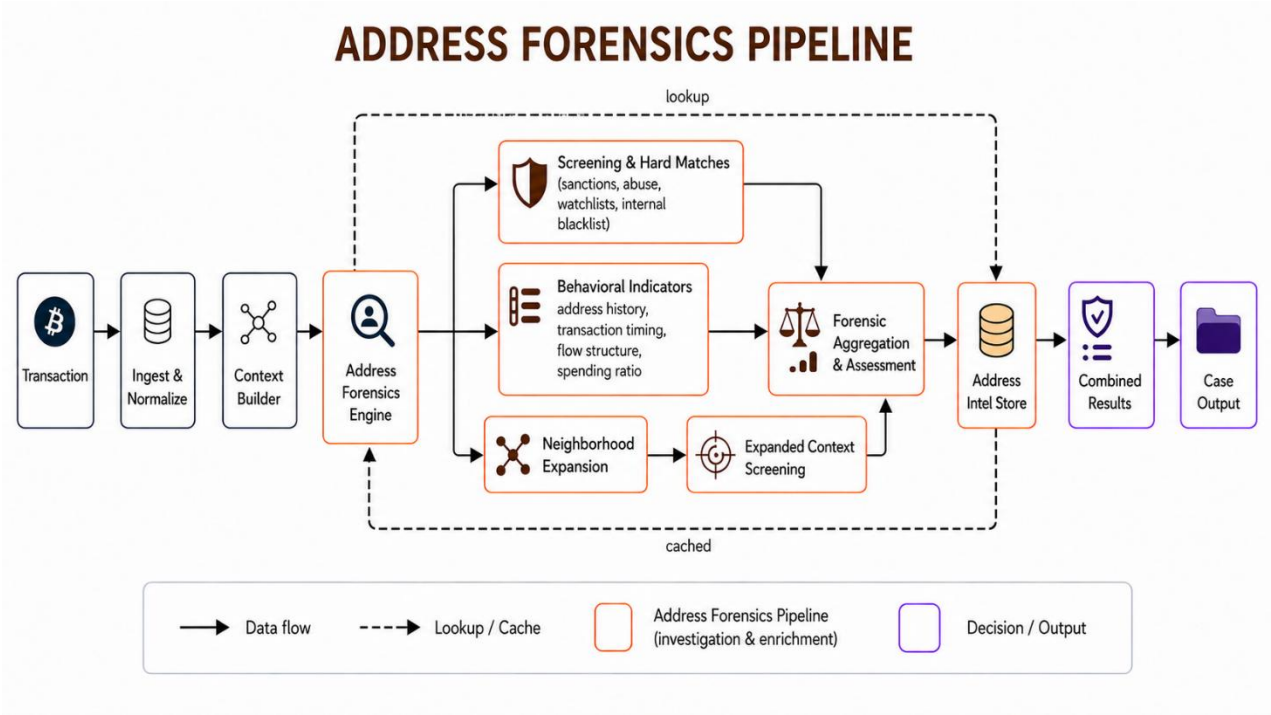


Рисунок 4.3 – Ветвь адресной криминалистики для анализа Bitcoin-транзакции

По истории входящих и исходящих переводов формируется профиль активности адреса, включающий периоды использования, интервалы неактивности и связи с другими адресами.

Поиск совпадений выполняется в хранилище адресной информации. Оно включает официальные санкционные списки, внутренний черный список и проверенные внешние источники. Внутренний черный список содержит около 500 тыс. уникальных Bitcoin-адресов. Этот список был сформирован в ходе исследования. Новые адреса добавляются только после проверки подтверждающих материалов. Для каждого результата сохраняются источник, тип совпадения и связанный адрес. Затем полученные сведения объединяются в модуле криминалистической оценки и включаются в аналитический кейс. Основные группы используемых источников представлены на рисунке 4.4.



Рисунок 4.4 – Адресная проверка

Проверка санкционных совпадений проводится по актуальной версии SDN List [95]. Для получения и поиска записей используются Sanctions List Service [96]. В разъяснениях Управления по контролю за иностранными активами адрес цифровой валюты рассматривается как идентификатор, который может быть связан с лицом или организацией, включенными в санкционный список [97]. Далее адрес проверяется по внутреннему черному списку. Внутренний черный список содержит проверенные адреса, связь которых с противоправной или иной высокорисковой активностью подтверждена исходными материалами.

Сервис Chainabuse используется для поиска публичных сообщений о мошенничестве, вымогательстве и других злоупотреблениях, связанных с Bitcoin-адресами. При чтении записи учитываются категория жалобы, описание события и дата публикации [98]. BitcoinAbuse содержит аналогичные пользовательские сообщения. Их нужно сопоставлять с поведением адреса в блокчейне и проверять независимо, поскольку наличие жалобы еще не подтверждает изложенные в ней обстоятельства [99]. WalletExplorer применяется для изучения возможных групп адресов и меток кошельков. Эти сведения помогают проверить предполагаемую связь адреса с известным сервисом или группой транзакций [100]. OpenSanctions используется для обогащения данных на уровне сущностей. Если запись из OpenSanctions подтверждается в официальном санкционном списке, при интерпретации используются данные этого перечня [101].

Если адрес не найден ни в одном из проверенных источников атрибуции, это означает только, что на дату проверки совпадение не обнаружено. Публичные списки могут быть неполными, а сведения о части схем не попадают в базы жалоб или появляются с задержкой. При повторном анализе поиск выполняется заново, поскольку содержание источников может обновиться.

Подтвержденным считается точное совпадение адреса с адресом, указанным в официальном санкционном списке, либо с записью внутреннего черного списка. Публичные жалобы, внешние метки и другие непроверенные сведения сохраняются как контекстная информация.

4.3 Поведенческие индикаторы, анализ локального окружения и объединение результатов

После проверки по источникам атрибуции анализируются история и характер использования адресов, связанных с Bitcoin-транзакцией. Выделение поведенческих признаков согласуется с риск-индикаторами, применяемыми при анализе виртуальных активов [12]. Аналогичные схемы движения средств рассматриваются в рекомендациях FinCEN [102]. В предлагаемой архитектуре рассматриваются шесть поведенческих индикаторов, объединенных в четыре смысловые группы: история активности адреса, скорость движения средств, структура потоков и степень расходования средств [103, 104]. Индикаторы

рассчитываются в ретроспективном режиме по доступной истории адреса в пределах установленных временных окон. Для каждого индикатора определяется статус «выявлен» или «не выявлен».

1. *Отсутствие наблюдаемой предыстории.* Индикатор выявляется, если до исследуемой транзакции в доступной истории блокчейна не обнаружено других транзакций с участием исследуемого адреса:

$$N_{\text{prev}}^{\text{addr}} = 0.$$

2. *Реактивация после периода неактивности.* Индикатор выявляется, если адрес ранее участвовал в транзакциях, затем длительное время не использовался и вновь появился в анализируемой транзакции:

$$N_{\text{prev}}^{\text{addr}} > 0 \;\&\; T_{\text{inactive}}^{\text{addr}} \geq T_{\text{inactive}}^{\min}.$$

где $N_{\text{prev}}^{\text{addr}}$ – число предыдущих транзакций с участием исследуемого адреса, $T_{\text{inactive}}^{\text{addr}}$ – продолжительность периода неактивности адреса, $T_{\text{inactive}}^{\min}$ – минимальная продолжительность периода неактивности, задаваемая в конфигурации программной системы. Такая последовательность может быть связана не только с подозрительной активностью, но и с переводом средств из холодного кошелька.

3. *Кратковременное транзитное использование*. Для каждого полученного UTXO рассчитывается время между его созданием и последующим расходованием. Индикатор срабатывает, если хотя бы один UTXO был израсходован за время, не превышающее установленного максимального значения:

$$T_{\text{hold}}^{\text{addr}} \leq T_{\text{hold}}^{\max}.$$

где $T_{\text{hold}}^{\text{addr}}$ – интервал между созданием UTXO для исследуемого адреса и его последующим расходованием, $T_{\text{hold}}^{\max}$ – максимальный период удержания, задаваемый в конфигурации программной системы.

4. *Распределение средств между множеством адресов*. Индикатор срабатывает, если средства с адреса переводятся на несколько разных адресов, число которых достигает установленного порога:

$$N_{\text{rec}} \geq N_{\text{rec}}^{\min}.$$

где N_{rec} – число различных адресов-получателей, $N_{\text{rec}}^{\min}$ – их минимальное число, задаваемое в конфигурации программной системы. В текущей реализации $N_{\text{rec}}^{\min} = 3$, что позволяет не учитывать обычные транзакции с двумя выходами, один из которых используется для возврата сдачи. Поскольку выход сдачи отдельно не определяется, результат интерпретируется с учетом

структуры транзакции.

5. *Концентрация поступлений на одном адресе.* Индикатор срабатывает, если за заданный период адрес получил средства из нескольких разных транзакций:

$$N_{\text{in}}(W_{\text{in}}) \geq N_{\text{in}}^{\min}.$$

где $N_{\text{in}}(W_{\text{in}})$ – число входящих транзакций за период W_{in}, $N_{\text{in}}^{\min}$ – минимальное число таких транзакций. Длительность периода и порог задаются в конфигурации программной системы. В текущей реализации $N_{\text{in}}^{\min} = 3$. Множественные поступления могут быть связаны с обычным сбором платежей, использованием депозитного адреса или консолидацией средств, поэтому сами по себе не указывают на нелегальную активность.

6. *Почти полный вывод средств*. Для определения почти полного вывода рассчитывается доля доступных средств адреса, расходуемая в транзакции:

$$R_{\text{spend}}^{\text{addr}} = \frac{Q_{\text{spend}}^{\text{addr}}}{Q_{\text{available}}^{\text{addr}}}, \tag{4.1}$$

где $R_{\text{spend}}^{\text{addr}}$ – доля расходуемых средств, $Q_{\text{spend}}^{\text{addr}}$ – общая сумма UTXO, связанных с адресом и расходуемых в этой транзакции, $Q_{\text{available}}^{\text{addr}}$ – общая сумма UTXO, связанных с адресом и доступных для расходования перед этой транзакцией.

Почти полный вывод фиксируется, если рассчитанная по формуле (4.1) доля не меньше установленного минимального значения:

$$R_{\text{spend}}^{\text{addr}} \geq R_{\text{spend}}^{\min}.$$

где $R_{\text{spend}}^{\min}$ – минимальная доля расходуемых средств, задаваемая в конфигурации программной системы. Почти полный вывод сам по себе не свидетельствует о противоправном характере транзакции [12]. Условия определения поведенческих индикаторов и ограничения их интерпретации обобщены в таблице 4.1.

Таблица 4.1 – Условия определения и ограничения интерпретации поведенческих индикаторов адресов

Группа	Индикатор	Условие выявления	Ограничение интерпретации
История активности	Отсутствие наблюдаемой предыстории	Предшествующие транзакции адреса отсутствуют	Может соответствовать обычному первому использованию адреса

Продолжение таблицы 4.1

История активности	Реактивация адреса	Период неактивности не меньше установленного значения	Возможно, перевод средств из холодного кошелька
Скорость движения	Кратковременный транзит	Время удержания не превышает установленного значения	Такое поведение возможно у бирж, платежных сервисов и горячих кошельков
Структура потоков	Распределение между множеством адресов	Число получателей не меньше установленного значения	Возможны массовые выплаты и выход сдачи
Структура потоков	Концентрация поступлений	Число входящих транзакций в заданном окне не меньше установленного значения	Возможны сбор платежей и консолидация
Степень расходования	Почти полный вывод	Доля расходуемых UTXO не меньше установленного порога	Само по себе не свидетельствует о противоправном характере

В санкционном или внутреннем черном списке могут находиться не адреса исследуемой транзакции, а адреса, связанные с соседними транзакциями [21]. Поэтому по умолчанию также проверяются адреса соседних транзакций, находящихся на расстоянии одного входящего или исходящего перехода. При ручном анализе глубину проверки можно изменить в настройках.

После завершения модельного и адресного анализа система объединяет полученные результаты и формирует один из двух выводов: «требуется дальнейшая проверка» или «не требуется». Проверка требуется, если модель классифицировала транзакцию как нелегальную либо в санкционном или внутреннем черном списке найден хотя бы один из адресов исследуемой транзакции или соседних транзакций. Поведенческие индикаторы используются как дополнительная информация для оценки адреса.

При этом результаты модельного и адресного анализа сохраняются отдельно. Например, модель может отнести транзакцию к легальной, а адресная проверка выявить подтвержденное совпадение. В таком случае в отчете указываются оба результата и причины, по которым требуется дальнейшая проверка. Окончательную оценку проводит аналитик. Это делает вывод системы понятным и проверяемым .

4.4 Разработка программной системы

Для реализации предложенной архитектуры разработано веб-приложение для киберкриминалистического анализа Bitcoin-транзакций. Система включает пользовательский интерфейс, серверное приложение, REST API, базу данных и модули загрузки блокчейн-данных, машинного обучения, адресной проверки, поведенческого и графового анализа. Структура системы представлена на рисунке 4.5.

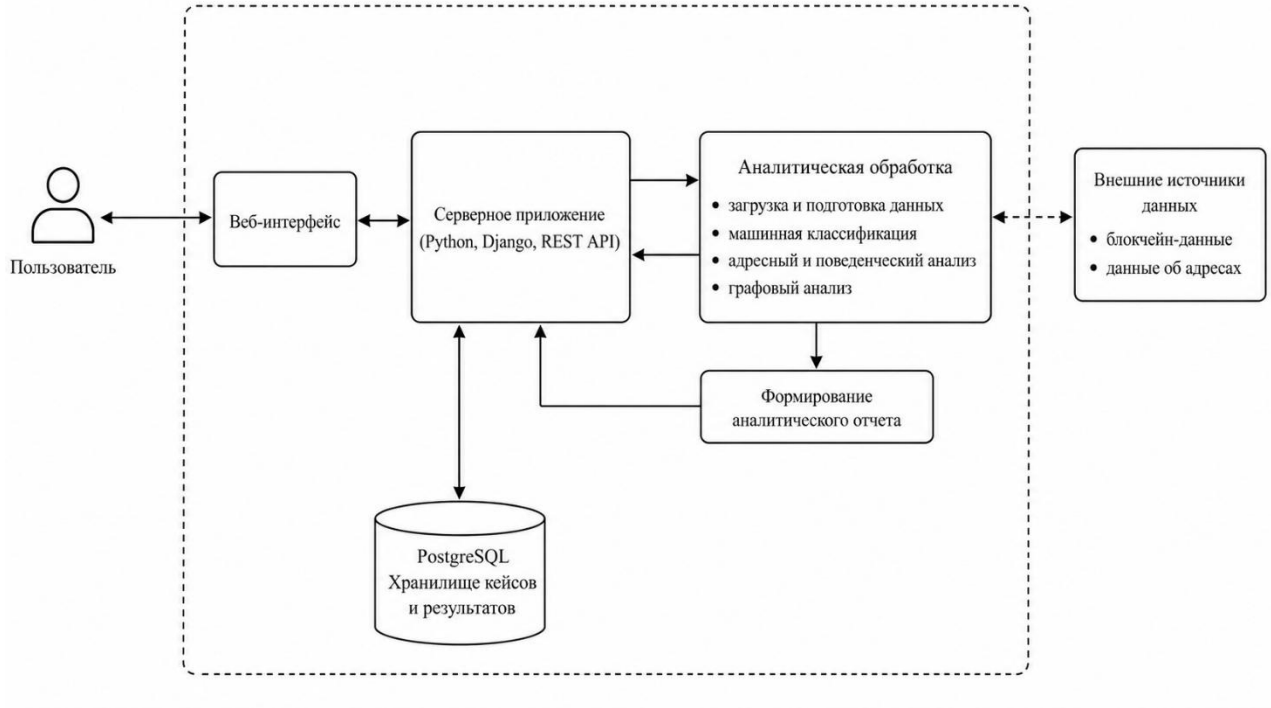


Рисунок 4.5 – Концептуальная архитектура программной системы киберкриминалистического анализа Bitcoin-транзакций

Работа начинается с ввода идентификатора транзакции и создания аналитического кейса. Система загружает данные анализируемой и связанных с ней транзакций в пределах установленного временного интервала, формирует направленный транзакционный граф, рассчитывает признаки исследуемой транзакции и классифицирует ее. Затем система проверяет связанные адреса, выявляет поведенческие индикаторы и строит локальное графовое окружение.

Результаты анализа отображаются в отдельных разделах и объединяются в итоговый аналитический отчет. В отчете сохраняются параметры транзакции, результат классификации, сведения об адресах, поведенческие индикаторы, графовые связи и итоговый вывод. Приложение предназначено для исследователей, специалистов по финансовому мониторингу и сотрудников правоохранительных органов.

Серверная часть реализована на языке Python с использованием Django и Django REST Framework. Django обрабатывает запросы, проверяет входные данные, выполняет серверную логику и взаимодействует с PostgreSQL через ORM. Django REST Framework предоставляет REST API для создания аналитических кейсов, передачи идентификаторов транзакций и получения результатов анализа. В PostgreSQL сохраняются данные транзакции, сведения о

связанных адресах, результаты работы аналитических модулей и итоговые отчеты. После создания кейса сервер загружает и нормализует данные, запускает модель машинного обучения, адресную проверку и анализ поведенческих индикаторов. Затем формируется локальный направленный граф, узлами которого являются транзакции и адреса, а ребра отражают движение средств. Для построения и анализа графа используется библиотека NetworkX.

Главная страница приложения представлена на рисунке 4.6. На ней отображаются общие показатели и последние аналитические кейсы. Панель используется для выбора кейса и контроля хода анализа.

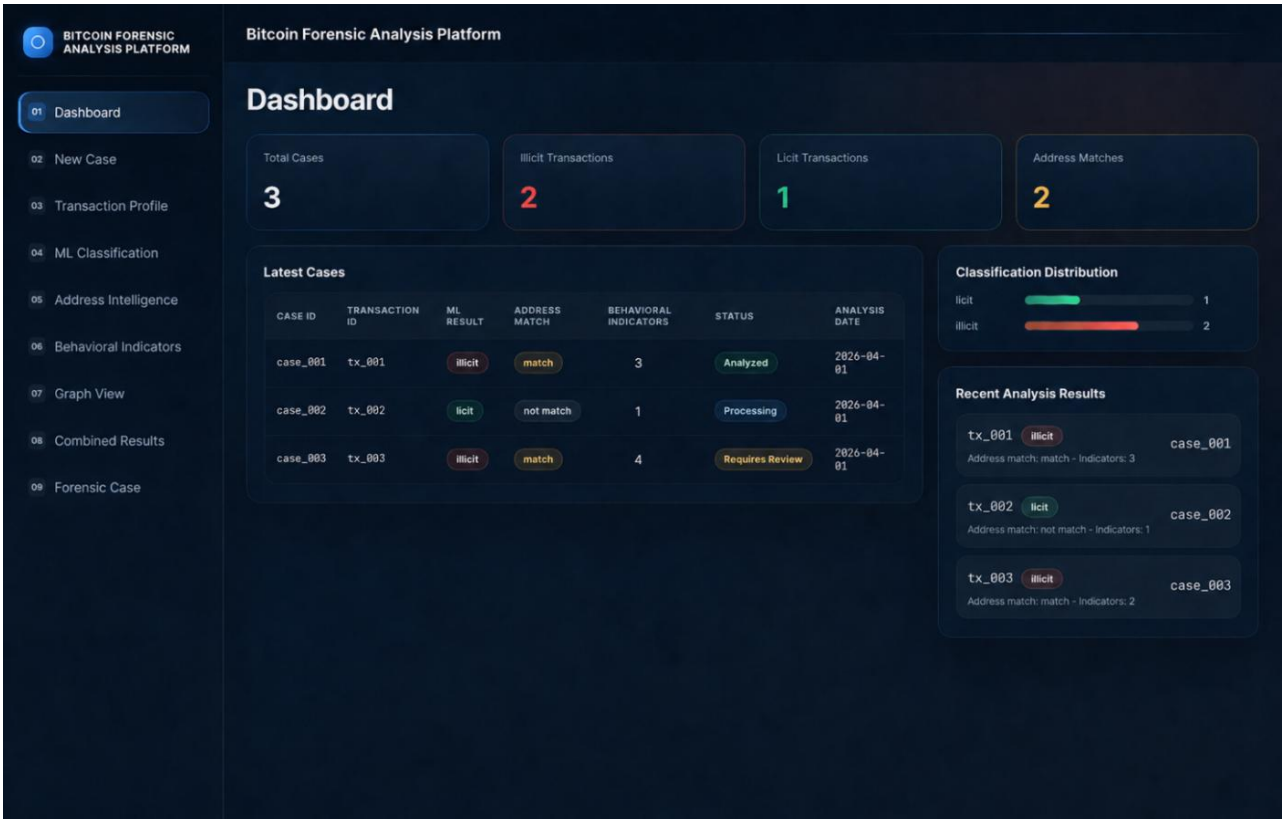


Рисунок 4.6 – Общая панель мониторинга

Параметры анализа задаются в форме создания нового кейса, представленной на рисунке 4.7.

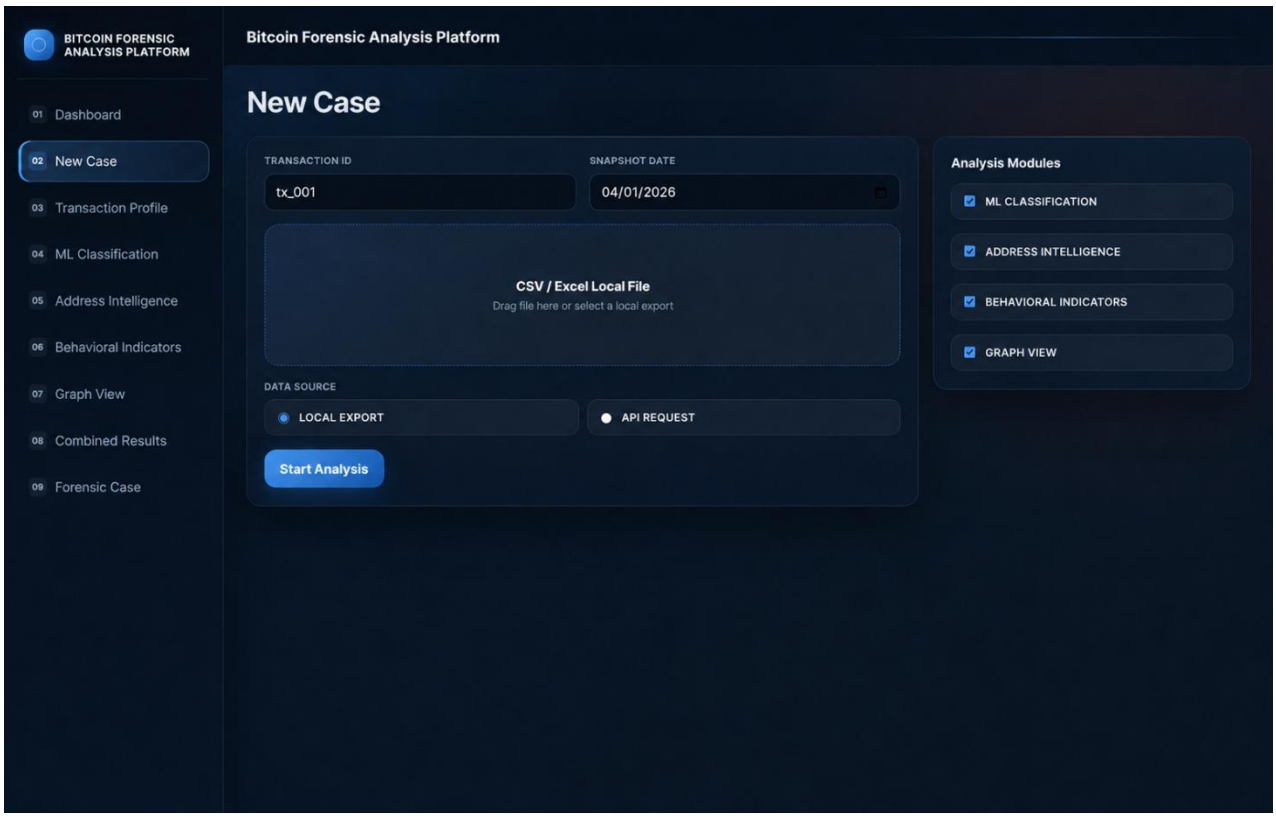


Рисунок 4.7 – Форма создания нового кейса

Модуль создания нового кейса («New Case») предназначен для запуска анализа выбранной Bitcoin-транзакции. Форма принимает идентификатор транзакции. В качестве источника данных можно использовать локальный файл в формате CSV или Excel либо внешний API. В правой части формы выбираются модули модельной классификации («ML Classification»), адресной проверки («Address Intelligence»), поведенческих индикаторов («Behavioral Indicators») и просмотра локального графа («Graph View»). Выбранные параметры сохраняются вместе с кейсом, поэтому позднее можно установить, на каких данных и с помощью каких модулей был получен результат.

После запуска система собирает базовые сведения о транзакции. Транзакционный профиль представлен на рисунке 4.8. Он содержит основные параметры транзакции, входные и выходные адреса и переданные суммы. Он используется для проверки исходных данных перед интерпретацией результатов анализа.

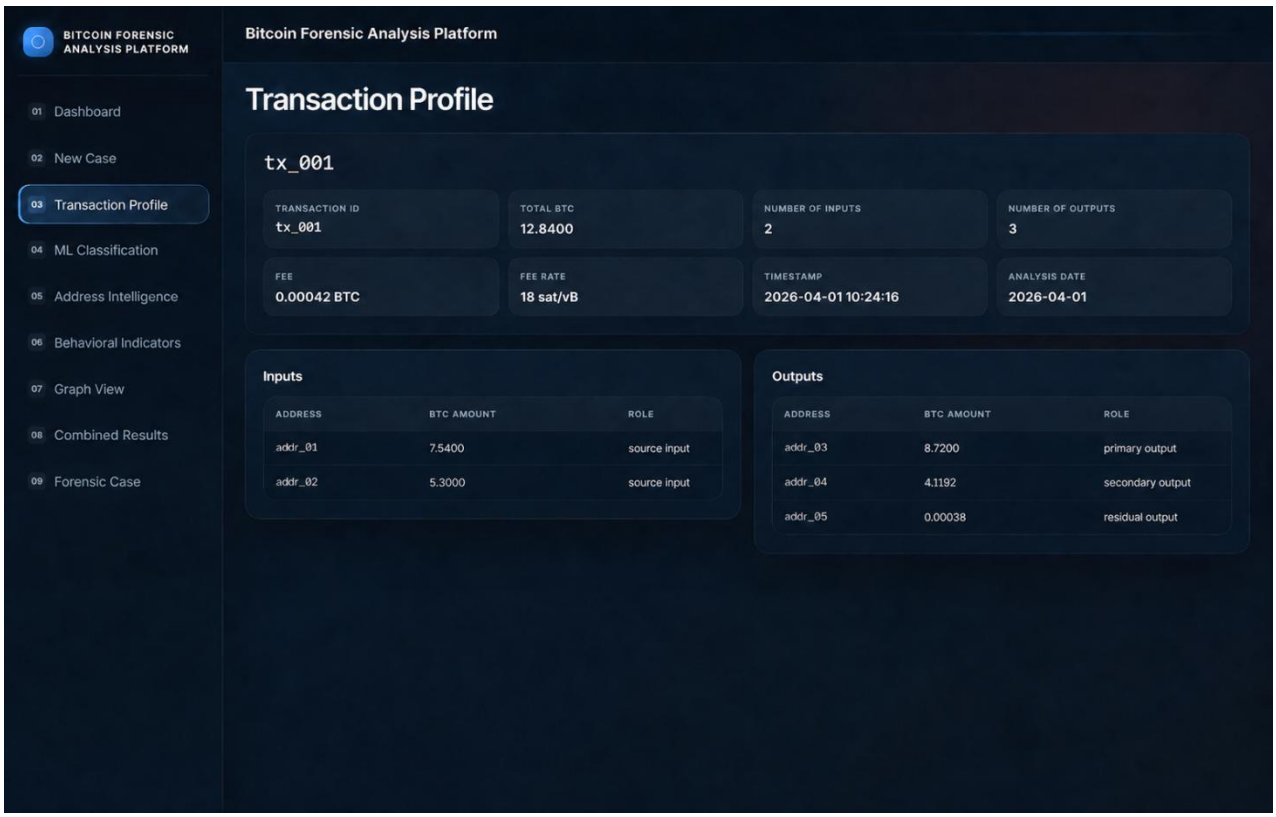


Рисунок 4.8 – Профиль Bitcoin-транзакции

Результат работы модели представлен на рисунке 4.9.

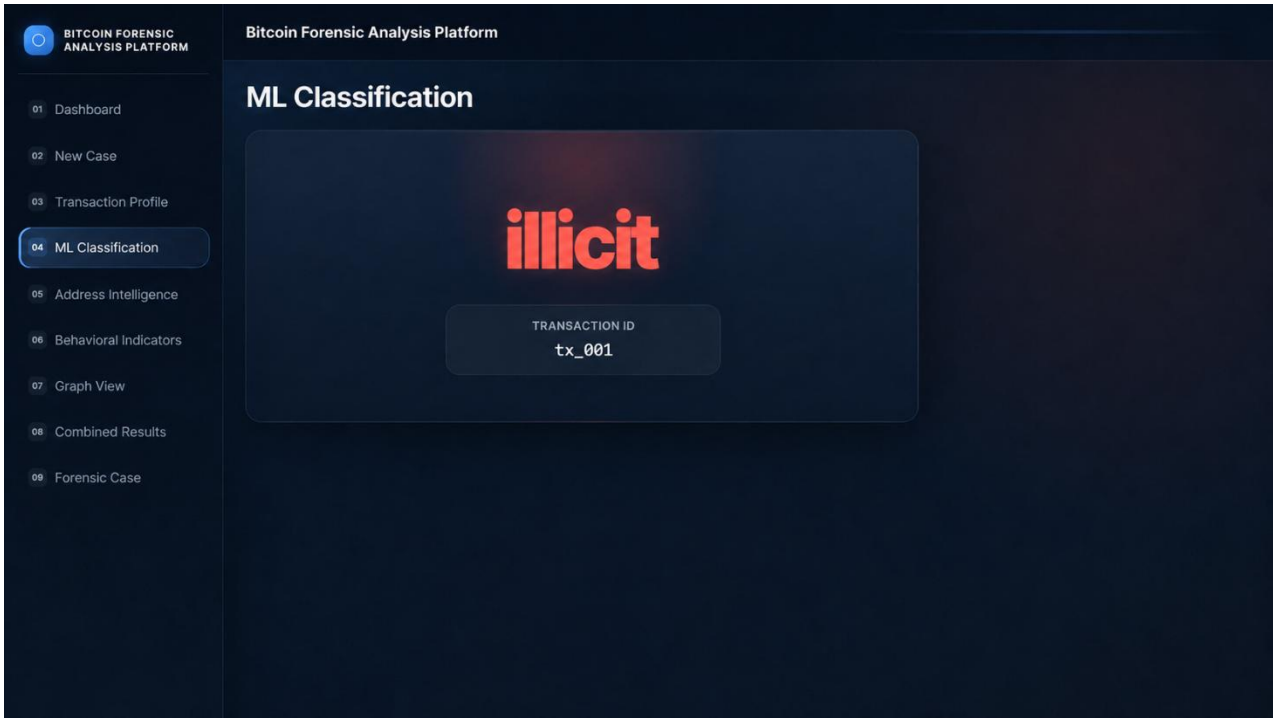


Рисунок 4.9 – Результат модельной классификации транзакции

Результаты проверки адресов представлены в модуле адресной проверки на рисунке 4.10.

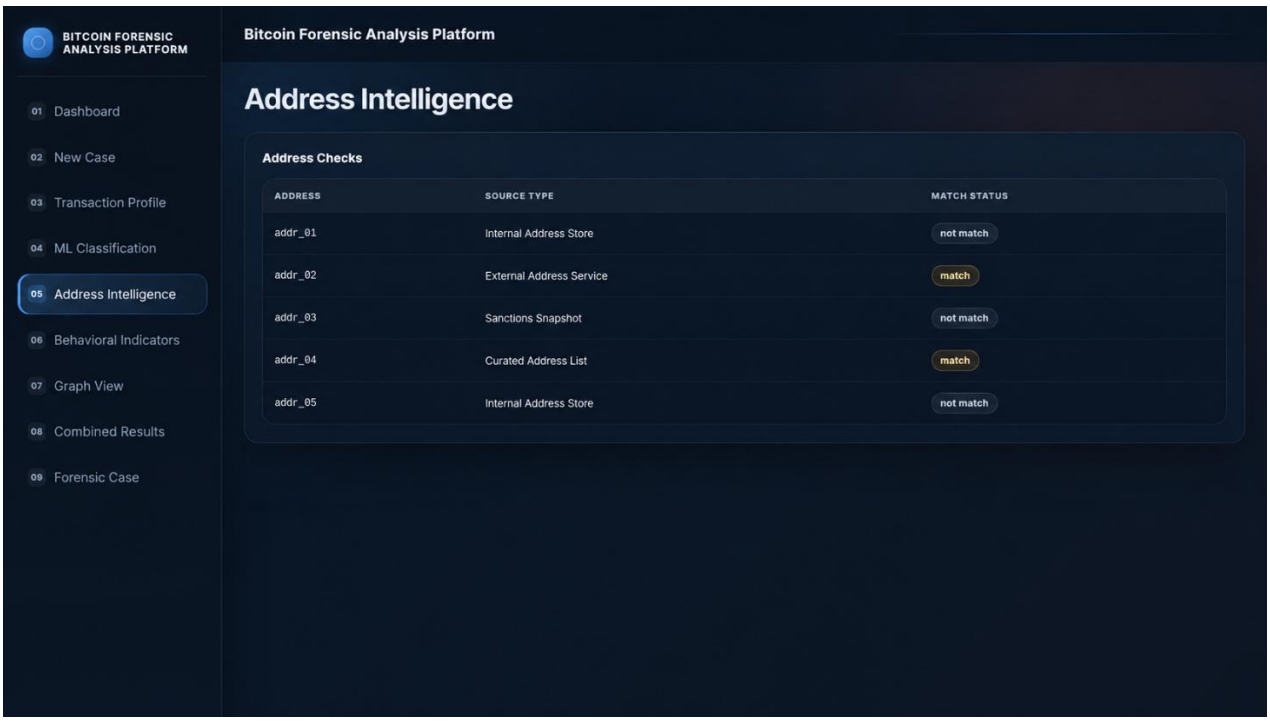


Рисунок 4.10 – Результат адресной проверки

Для каждого адреса указываются источник сведений и результат проверки: «совпадение обнаружено» или «совпадение не обнаружено».

Результаты поведенческого анализа представлены на рисунке 4.11. Для каждого индикатора указывается статус «выявлен» или «не выявлен».

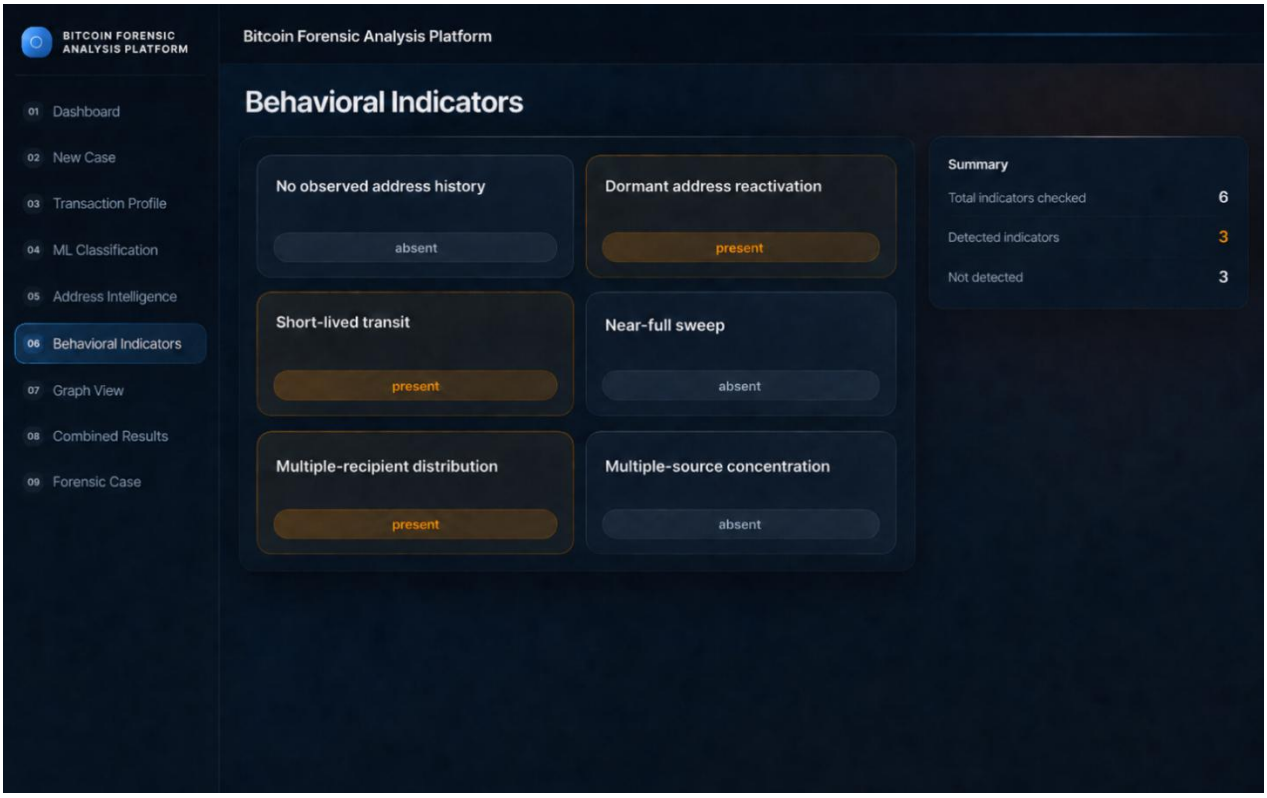


Рисунок 4.11 – Поведенческие индикаторы адреса

Для просмотра движения средств используется модуль локального графа, который показан на рисунке 4.12.

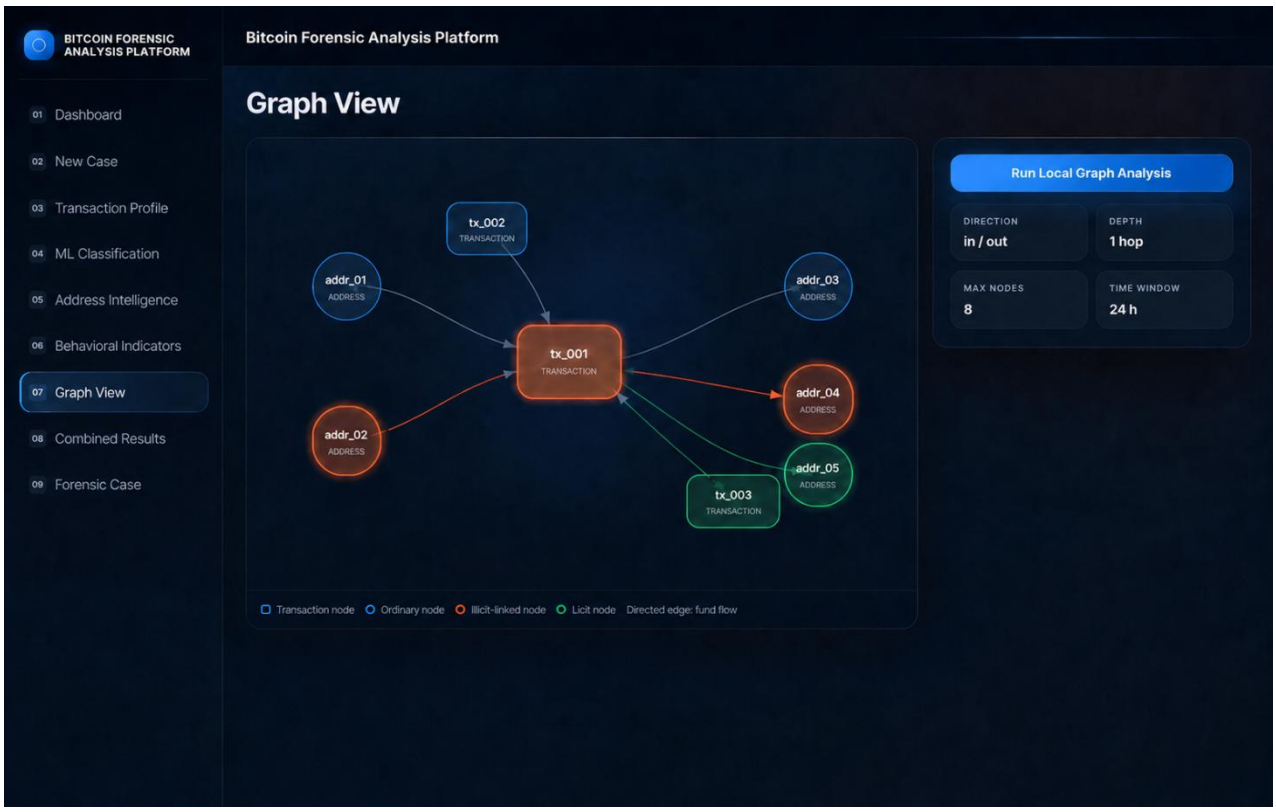


Рисунок 4.12 – Локальное графовое окружение транзакции

В центре графа находится анализируемая транзакция, вокруг нее расположены адреса и соседние транзакции. Направленные ребра показывают поток средств. Пользователь может задать направление анализа, глубину, временное окно и максимальное число узлов. Изменение временного окна локального графа используется только для дополнительного анализа окружения и не влияет на признаки модельной ветви. Если в заданном окружении найдено подтвержденное совпадение, модуль фиксирует графовый сигнал и сохраняет связанный узел, направление связи и число переходов до исследуемой транзакции.

На сводной странице, показанной на рисунке 4.13, отображаются объединенные результаты всех модулей: результат классификации, адресные совпадения, поведенческие индикаторы и графовый сигнал.

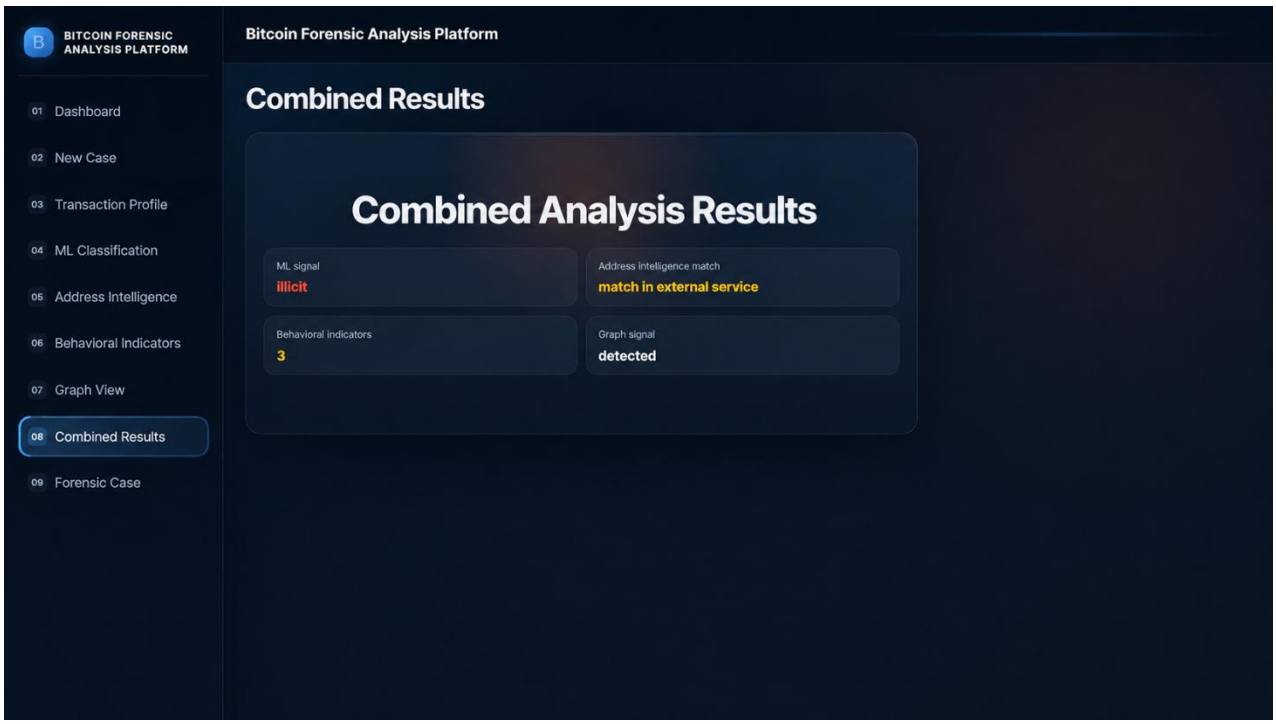


Рисунок 4.13 – Объединение результатов анализа

После завершения анализа формируется карточка кейса, представленная на рисунке 4.14. Она содержит сведения о кейсе и транзакции, дату анализа, результаты всех проверок и итоговый вывод. Отчет можно экспортировать в форматах PDF и JSON.

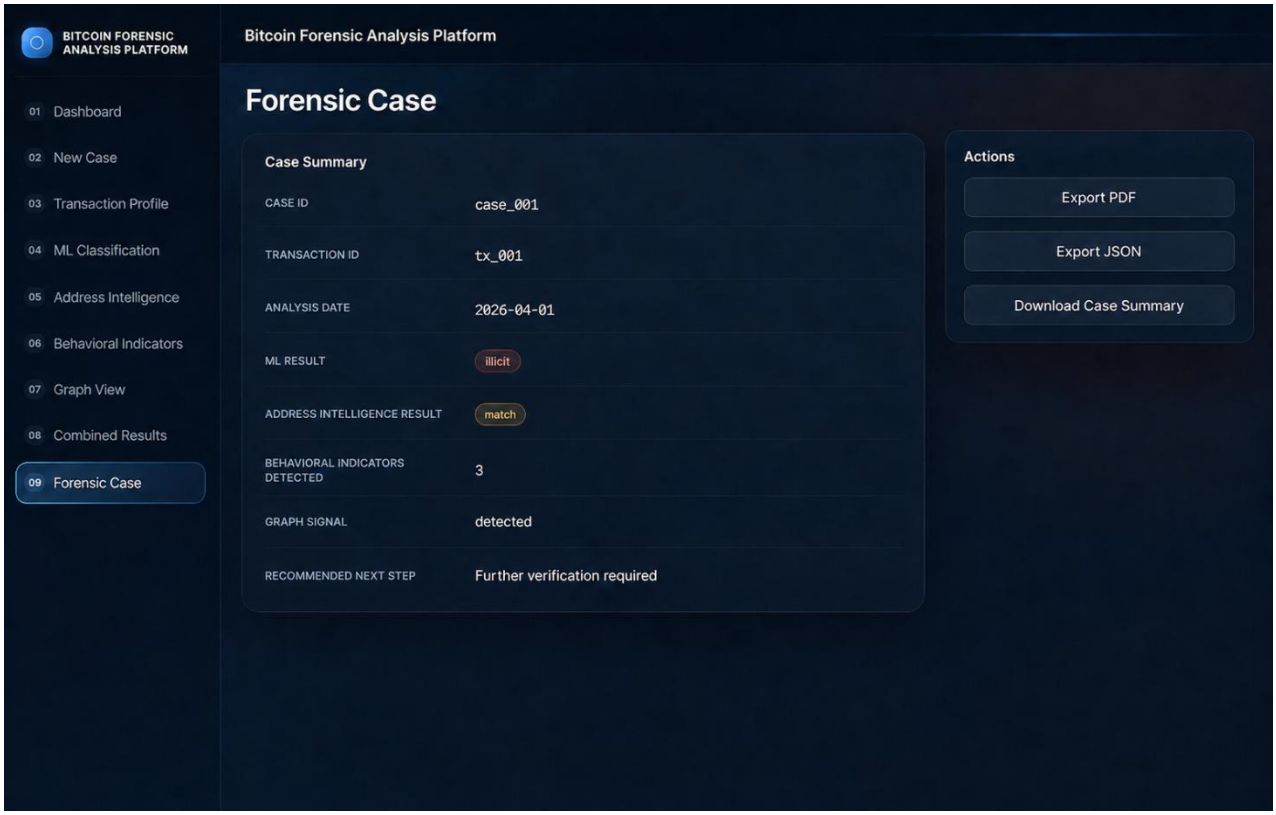


Рисунок 4.14 – Формирование криминалистического кейса

4.5 Выводы по разделу 4

В главе предложена гибридная архитектура анализа Bitcoin-транзакций, включающая классификацию транзакции, проверку связанных адресов, изучение их активности, поведенческих признаков и ближайшего графового окружения. Результаты каждого модуля сохраняются отдельно и используются при решении о дальнейшей проверке.

При анализе адресов приоритет отдается официальным сведениям. Данные из внешних источников, история активности и поведенческие признаки учитываются как дополнительная информация.

Система реализована в виде веб-приложения, которое сохраняет данные транзакции и результаты анализа. Оно помогает аналитику изучить транзакцию, но не устанавливает ее правовой статус и не заменяет экспертную оценку.

ЗАКЛЮЧЕНИЕ

В ходе выполнения диссертационной работы решена актуальная научно-техническая задача, заключающаяся в разработке методов и моделей машинного обучения для киберкриминалистического анализа Bitcoin-транзакций на основе открытых данных блокчейна. Разработанные методы обеспечивают выявление транзакций с признаками нелегальной активности и формирование интерпретируемых результатов.

Анализ существующих подходов показал, что качество выявления нелегальных Bitcoin-транзакций определяется не только алгоритмом классификации, но и достоверностью разметки, составом признаков, способом построения графа и протоколом эксперимента. Основными ограничениями опубликованных методов являются недостаточная интерпретируемость признаков и невозможность их непосредственного расчета для новых Bitcoin-транзакций, что затрудняет практическое применение построенных на них моделей.

Для наборов данных с анонимизированными признаками предложен оберточный метод отбора на основе генетического алгоритма и Random Forest. На наборе Elliptic число признаков сокращено со 166 до 53. Модель с отобранными признаками достигла Precision 99,37%, Recall 73,13% и F1-score 84,26%. Значение F1-score превысило результат Random Forest на полном наборе признаков на 1,36 п. п., а результат SelectKBest при том же количестве признаков – на 5,49 п. п. Сопоставление с опубликованными Weber et al. результатами модели Random Forest с GCN-эмбеддингами показало более высокие значения Precision, Recall и F1-score – соответственно на 2,27, 5,63 и 4,66 п. п.

Сформирован набор данных, включающий 48 239 размеченных Bitcoin-транзакций, сопоставленных с открытыми данными блокчейна. Разработана система из 61 криминалистически интерпретируемого дескриптора, объединенных в три группы: признаки локального отклонения от окружения, временные признаки последующего расходования и признаки предшествующей транзакционной истории. Добавление этих дескрипторов к базовому набору из 26 транзакционных и структурно-графовых признаков повысило качество всех восьми исследованных моделей: средний прирост PR-AUC составил 3,97 п. п., а F1-score – 4,26 п. п. Абляционный анализ показал, что наибольший вклад внесли признаки локального отклонения от окружения и предшествующей транзакционной истории.

На основе разработанной системы признаков построена модель выявления нелегальных Bitcoin-транзакций с использованием алгоритма CatBoost. При оценке на сформированном наборе данных модель достигла значений PR-AUC 90,27%, Recall 81,11% и F1-score 83,90%.

В работе предложен подход, объединяющий классификацию транзакции, проверку адресов, анализ поведенческих признаков и ближайшего графового окружения. Все этапы реализованы в веб-приложении, которое формирует структурированный отчет по каждому аналитическому случаю.

Разработанный инструментарий может применяться подразделениями финансового мониторинга, правоохранительными органами, криптовалютными биржами и организациями, занимающимися противодействием отмыванию доходов и расследованием преступлений, связанных с использованием криптовалют. Метод отбора признаков на основе генетического алгоритма может использоваться при работе с наборами, содержащими анонимизированные признаки.

Для проведения анализа необходимы блокчейн-данные, позволяющие описать характеристики транзакции и восстановить ее графовое окружение. Объем и глубина анализа определяются поставленной задачей, доступностью данных и вычислительными ресурсами.

Вычислительная эффективность решения оценена количественно. Экономическая эффективность не рассчитывалась из-за отсутствия данных о затратах.

Разработанное приложение позволяет сократить объем ручной работы и упростить анализ Bitcoin-транзакций.

Научное отличие работы состоит в разработке семантически открытых признаков, рассчитываемых непосредственно по данным блокчейна, проведении экспериментов по воспроизводимой схеме и объединении модельной классификации с дополнительными видами киберкриминалистического анализа. В рамках принятого экспериментального протокола полученные результаты демонстрируют конкурентоспособность предложенного подхода. Таким образом, задачи исследования выполнены, а поставленная цель достигнута. Полнота решения подтверждается аналитическими, методическими, экспериментальными и программными результатами, представленными в работе.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 О цифровых активах в Республике Казахстан: Закон Республики Казахстан от 6 февраля 2023 года № 193-VII ЗРК [Электронный ресурс]. – URL: https://adilet.zan.kz/rus/docs/Z2300000193 – Дата обращения: 15.03.2026.

2 Financial Action Task Force (FATF). Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers [Электронный ресурс]. – Paris: FATF, 2025. – URL: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2025.html – Дата обращения: 15.03.2026.

3 Chainalysis Team. Crypto Crime Reaches Record High in 2025 as Nation-State Sanctions Evasion Moves On-Chain at Scale [Электронный ресурс]. – 2026. – URL: https://www.chainalysis.com/blog/2026-crypto-crime-report-introduction/ – Дата обращения: 15.03.2026.

4 Meiklejohn S., Pomarole M., Jordan G., Levchenko K., McCoy D., Voelker G. M., Savage S. A Fistful of Bitcoins: Characterizing Payments Among Men with No Names // Communications of the ACM. – 2016. – Vol. 59, No. 4. – P. 86–93. – DOI: 10.1145/2896384.

5 Fröwis M., Gottschalk T., Haslhofer B., Rückert C., Pesch P. Safeguarding the Evidential Value of Forensic Cryptocurrency Investigations // Forensic Science International: Digital Investigation. – 2020. – Vol. 33. – Art. 200902. – DOI: 10.1016/j.fsidi.2019.200902.

6 Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System [Электронный ресурс]. – 2008. – URL: https://bitcoin.org/bitcoin.pdf – Дата обращения: 15.03.2026.

7 Schnoering H., Vazirgiannis M. Bitcoin Research with a Transaction Graph Dataset // Scientific Data. – 2025. – Vol. 12. – Art. 404. – DOI: 10.1038/s41597-025-04684-8.

8 Reid F., Harrigan M. An Analysis of Anonymity in the Bitcoin System // Security and Privacy in Social Networks / ed. by Y. Altshuler, Y. Elovici, A. B. Cremers, N. Aharony, A. Pentland. – New York: Springer, 2013. – P. 197–223. – DOI: 10.1007/978-1-4614-4139-7_10.

9 Wu J., Liu J., Zhao Y., Zheng Z. Analysis of Cryptocurrency Transactions from a Network Perspective: An Overview // Journal of Network and Computer Applications. – 2021. – Vol. 190. – Art. 103139. – DOI: 10.1016/j.jnca.2021.103139.

10 Thomas T., Edwards T., Baggili I. BlockQuery: Toward Forensically Sound Cryptocurrency Investigation // Forensic Science International: Digital Investigation. – 2022. – Vol. 40. – Art. 301340. – DOI: 10.1016/j.fsidi.2022.301340.

11 Narayanan A., Bonneau J., Felten E., Miller A., Goldfeder S. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. – Princeton: Princeton University Press, 2016.

12 Financial Action Task Force (FATF). Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing [Электронный ресурс]. – Paris: FATF, 2020. – URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-Assets-Red-Flag-Indicators.pdf – Дата обращения: 16.03.2026.

13 Arnold N. A., Zhong P., Ba C. T., Steer B., Mondragon R., Cuadrado F., Lambiotte R., Clegg R. G. Insights and Caveats from Mining Local and Global Temporal Motifs in Cryptocurrency Transaction Networks // Scientific Reports. – 2024. – Vol. 14. – Art. 26569. – DOI: 10.1038/s41598-024-75348-7.

14 Ranshous S., Joslyn C. A., Kreyling S., Nowak K., Samatova N. F., West C. L., Winters S. Exchange Pattern Mining in the Bitcoin Transaction Directed Hypergraph // Financial Cryptography and Data Security. FC 2017. Lecture Notes in Computer Science. – Cham: Springer, 2017. – Vol. 10323. – P. 248–263. – DOI: 10.1007/978-3-319-70278-0_16.

15 Coquidé C., Cazabet R. A Temporal Graph Dataset of Bitcoin Entity-Entity Transactions // Scientific Data. – 2025. – Vol. 12. – Art. 337. – DOI: 10.1038/s41597-025-04595-8.

16 Ramos Tubino R., Robardet C., Cazabet R. Towards a Better Identification of Bitcoin Actors by Supervised Learning // Data & Knowledge Engineering. – 2022. – Vol. 142. – Art. 102094. – DOI: 10.1016/j.datak.2022.102094.

17 Tironsakkul T., Maarek M., Eross A., Just M. Context Matters: Methods for Bitcoin Tracking // Forensic Science International: Digital Investigation. – 2022. – Vol. 42–43. – Art. 301475. – DOI: 10.1016/j.fsidi.2022.301475.

18 Huang D. Y., Aliapoulios M. M., Li V. G., Invernizzi L., McRoberts K., Bursztein E., Levin J., Levchenko K., Snoeren A. C., McCoy D. Tracking Ransomware End-to-End // 2018 IEEE Symposium on Security and Privacy. – 2018. – P. 618–631. – DOI: 10.1109/SP.2018.00047.

19 Hu X., Gui M., Cheng G., Li R., Wu H. Multi-Class Bitcoin Mixing Service Identification Based on Graph Classification // Digital Communications and Networks. – 2024. – Vol. 10, No. 6. – P. 1881–1893. – DOI: 10.1016/j.dcan.2024.08.010.

20 dos Reis E. F., Teytelboym A., ElBahrawy A., De Loizaga I., Baronchelli A. Identifying Key Players in Dark Web Marketplaces through Bitcoin Transaction Networks // Scientific Reports. – 2024. – Vol. 14. – Art. 2385. – DOI: 10.1038/s41598-023-50409-5.

21 Elmougy Y., Liu L. Demystifying Fraudulent Transactions and Illicit Nodes in the Bitcoin Network for Financial Forensics // Proceedings of the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining. – 2023. – P. 3979–3990. – DOI: 10.1145/3580305.3599803.

22 Bartoletti M., Pes B., Serusi S. Data Mining for Detecting Bitcoin Ponzi Schemes // 2018 Crypto Valley Conference on Blockchain Technology. – 2018. – P. 75–84. – DOI: 10.1109/CVCBT.2018.00014.

23 Chandola V., Banerjee A., Kumar V. Anomaly Detection: A Survey // ACM Computing Surveys. – 2009. – Vol. 41, No. 3. – Art. 15. – DOI: 10.1145/1541880.1541882.

24 Ma X., Wu J., Xue S., Yang J., Zhou C., Sheng Q. Z., Xiong H., Akoglu L. A Comprehensive Survey on Graph Anomaly Detection with Deep Learning // IEEE Transactions on Knowledge and Data Engineering. – 2023. – Vol. 35, No. 12. – P. 12012–12038. – DOI: 10.1109/TKDE.2021.3118815.

25 Pocher N., Zichichi M., Merizzi F., Shafiq M. Z., Ferretti S. Detecting Anomalous Cryptocurrency Transactions: An AML/CFT Application of Machine Learning-Based Forensics // Electronic Markets. – 2023. – Vol. 33. – Art. 37. – DOI: 10.1007/s12525-023-00654-3.

26 Weber M., Domeniconi G., Chen J., Weidele D. K. I., Bellei C., Robinson T., Leiserson C. E. Anti-Money Laundering in Bitcoin: Experimenting with Graph Convolutional Networks for Financial Forensics // KDD '19 Workshop on Anomaly Detection in Finance. – 2019. – DOI: 10.48550/arXiv.1908.02591.

27 Alarab I., Prakoonwit S., Nacer M. I. Comparative Analysis Using Supervised Learning Methods for Anti-Money Laundering in Bitcoin // Proceedings of the 2020 5th International Conference on Machine Learning Technologies. – 2020. – P. 11–17. – DOI: 10.1145/3409073.3409078.

28 Guyon I., Elisseeff A. An Introduction to Variable and Feature Selection // Journal of Machine Learning Research. – 2003. – Vol. 3. – P. 1157–1182.

29 Vlahavas G., Karasavvas K., Vakali A. Unsupervised Clustering of Bitcoin Transactions // Financial Innovation. – 2024. – Vol. 10. – Art. 25. – DOI: 10.1186/s40854-023-00525-y.

30 Liu F. T., Ting K. M., Zhou Z.-H. Isolation Forest // Proceedings of the 2008 Eighth IEEE International Conference on Data Mining. – 2008. – P. 413–422. – DOI: 10.1109/ICDM.2008.17.

31 Schölkopf B., Platt J. C., Shawe-Taylor J., Smola A. J., Williamson R. C. Estimating the Support of a High-Dimensional Distribution // Neural Computation. – 2001. – Vol. 13, No. 7. – P. 1443–1471. – DOI: 10.1162/089976601750264965.

32 Sakurada M., Yairi T. Anomaly Detection Using Autoencoders with Nonlinear Dimensionality Reduction // Proceedings of the 2nd Workshop on Machine Learning for Sensory Data Analysis. – 2014. – P. 4–11. – DOI: 10.1145/2689746.2689747.

33 Zhou D., Bousquet O., Lal T. N., Weston J., Schölkopf B. Learning with Local and Global Consistency // Advances in Neural Information Processing Systems. – 2004. – Vol. 16. – P. 321–328.

34 Li M., Jia L., Su X. Global-Local Graph Attention with Cyclic Pseudo-Labels for Bitcoin Anti-Money Laundering Detection // Scientific Reports. – 2025. – Vol. 15. – Art. 22668. – DOI: 10.1038/s41598-025-08365-9.

35 Lo W. W., Kulatilleke G. K., Sarhan M., Layeghy S., Portmann M. Inspection-L: Self-Supervised GNN Node Embeddings for Money Laundering Detection in Bitcoin // Applied Intelligence. – 2023. – Vol. 53, No. 16. – P. 19406–19417. – DOI: 10.1007/s10489-023-04504-9.

36 Veličković P., Fedus W., Hamilton W. L., Liò P., Bengio Y., Hjelm R. D. Deep Graph Infomax // Proceedings of the International Conference on Learning Representations. – 2019.

37 Liang Y., Wu W., Liang R., Chen Y., Lei K., Zhong G., Zhang J., Gan Q., Huang J. A Plug-and-Play Data-Driven Approach for Anti-Money Laundering in Bitcoin // Expert Systems with Applications. – 2025. – Vol. 266. – Art. 126072. – DOI: 10.1016/j.eswa.2024.126072.

38 Kipf T. N., Welling M. Semi-Supervised Classification with Graph Convolutional Networks // International Conference on Learning Representations. – 2017. – DOI: 10.48550/arXiv.1609.02907.

39 Veličković P., Cucurull G., Casanova A., Romero A., Liò P., Bengio Y. Graph Attention Networks // International Conference on Learning Representations. – 2018. – DOI: 10.48550/arXiv.1710.10903.

40 Xu K., Hu W., Leskovec J., Jegelka S. How Powerful Are Graph Neural Networks? // International Conference on Learning Representations. – 2019. – DOI: 10.48550/arXiv.1810.00826.

41 Lundberg S. M., Lee S.-I. A Unified Approach to Interpreting Model Predictions // Advances in Neural Information Processing Systems. – 2017. – Vol. 30. – P. 4765–4774.

42 Ying Z., Bourgeois D., You J., Zitnik M., Leskovec J. GNNExplainer: Generating Explanations for Graph Neural Networks // Advances in Neural Information Processing Systems. – 2019. – Vol. 32. – P. 9240–9251.

43 Bellei C., Xu M., Phillips R., Robinson T., Weber M., Kaler T., Leiserson C. E., Arvind, Chen J. The Shape of Money Laundering: Subgraph Representation Learning on the Blockchain with the Elliptic2 Dataset [Электронный ресурс]. – 2024. – arXiv:2404.19109. – DOI: 10.48550/arXiv.2404.19109. – URL: https://arxiv.org/abs/2404.19109 – Дата обращения: 16.03.2026.

44 Akcora C. G., Li Y., Gel Y. R., Kantarcioglu M. BitcoinHeist: Topological Data Analysis for Ransomware Prediction on the Bitcoin Blockchain // Proceedings of the Twenty-Ninth International Joint Conference on Artificial Intelligence (IJCAI-20). – 2020. – P. 4439–4445. – DOI: 10.24963/ijcai.2020/612.

45 Xiang Y., Lei Y., Bao D., Li T., Yang Q., Liu W., Ren W., Choo K.-K. R. BABD: A Bitcoin Address Behavior Dataset for Pattern Analysis // IEEE Transactions on Information Forensics and Security. – 2024. – Vol. 19. – P. 2171–2185. – DOI: 10.1109/TIFS.2023.3347894.

46 Robinson T. The Elliptic Data Set: Working with the Community to Combat Financial Crime in Cryptocurrencies [Электронный ресурс] // Elliptic Blog. – 2019. – 12 Aug. – URL: https://www.elliptic.co/blog/elliptic-dataset-cryptocurrency-financial-crime – Дата обращения: 16.03.2026.

47 Breiman L. Random Forests // Machine Learning. – 2001. – Vol. 45, No. 1. – P. 5–32. – DOI: 10.1023/A:1010933404324.

48 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. – DOI: 10.15587/1729-4061.2025.335630.

49 Hamilton W. L., Ying R., Leskovec J. Inductive Representation Learning on Large Graphs // Advances in Neural Information Processing Systems. – 2017. – Vol. 30. – P. 1024–1034.

50 Li Y., Tarlow D., Brockschmidt M., Zemel R. Gated Graph Sequence Neural Networks // International Conference on Learning Representations. – 2016. – DOI: 10.48550/arXiv.1511.05493.

51 Xu K., Li C., Tian Y., Sonobe T., Kawarabayashi K., Jegelka S. Representation Learning on Graphs with Jumping Knowledge Networks // Proceedings of the 35th International Conference on Machine Learning. Proceedings of Machine Learning Research. – 2018. – Vol. 80. – P. 5453–5462.

52 Klicpera J., Bojchevski A., Günnemann S. Predict Then Propagate: Graph Neural Networks Meet Personalized PageRank // International Conference on Learning Representations. – 2019. – DOI: 10.48550/arXiv.1810.05997.

53 Wu F., Souza A., Zhang T., Fifty C., Yu T., Weinberger K. Simplifying Graph Convolutional Networks // Proceedings of the 36th International Conference on Machine Learning. Proceedings of Machine Learning Research. – 2019. – Vol. 97. – P. 6861–6871.

54 Chen M., Wei Z., Huang Z., Ding B., Li Y. Simple and Deep Graph Convolutional Networks // Proceedings of the 37th International Conference on Machine Learning. Proceedings of Machine Learning Research. – 2020. – Vol. 119. – P. 1725–1735.

55 Corso G., Cavalleri L., Beaini D., Liò P., Veličković P. Principal Neighbourhood Aggregation for Graph Nets // Advances in Neural Information Processing Systems. – 2020. – Vol. 33. – P. 13260–13271. – DOI: 10.48550/arXiv.2004.05718.

56 Goldberg D. E. Genetic Algorithms in Search, Optimization, and Machine Learning. – Reading, MA: Addison-Wesley, 1989.

57 Katoch S., Chauhan S. S., Kumar V. A Review on Genetic Algorithm: Past, Present, and Future // Multimedia Tools and Applications. – 2021. – Vol. 80. – P. 8091–8126. – DOI: 10.1007/s11042-020-10139-6.

58 Kohavi R., John G. H. Wrappers for Feature Subset Selection // Artificial Intelligence. – 1997. – Vol. 97, No. 1–2. – P. 273–324. – DOI: 10.1016/S0004-3702(97)00043-X.

59 Alarab I., Prakoonwit S., Nacer M. I. Competence of Graph Convolutional Networks for Anti-Money Laundering in Bitcoin Blockchain // Proceedings of the 2020 5th International Conference on Machine Learning Technologies. – 2020. – P. 23–27. – DOI: 10.1145/3409073.3409080.

60 Lorenz J., Silva M. I., Aparício D., Ascensão J. T., Bizarro P. Machine Learning Methods to Detect Money Laundering in the Bitcoin Blockchain in the Presence of Label Scarcity // Proceedings of the First ACM International Conference on AI in Finance. – 2020. – P. 1–8. – DOI: 10.1145/3383455.3422549.

61 Benzik A. Deanonymized 99.5 pct of Elliptic Transactions: Kaggle Dataset [Электронный ресурс]. – URL: https://www.kaggle.com/datasets/alexbenzik/deanonymized-995-pct-of-elliptic-transactions – Дата обращения: 20.03.2024.

62 Blockchair. Blockchair API Documentation [Электронный ресурс]. – URL: https://blockchair.com/api/docs – Дата обращения: 20.03.2024.

63 Crystal Intelligence. Blockchain Intelligence for Crime Detection, Investigation and Compliance [Электронный ресурс]. – URL: https://crystalintelligence.com/ – Дата обращения: 20.03.2024.

64 Page L., Brin S., Motwani R., Winograd T. The PageRank Citation Ranking: Bringing Order to the Web: Technical Report No. 1999-66 [Электронный ресурс]. – Stanford: Stanford InfoLab, 1999. – URL: http://ilpubs.stanford.edu:8090/422/1/1999-66.pdf – Дата обращения: 18.03.2026.

65 Kleinberg J. M. Authoritative Sources in a Hyperlinked Environment // Journal of the ACM. – 1999. – Vol. 46, No. 5. – P. 604–632. – DOI: 10.1145/324133.324140.

66 Newman M. E. J. Networks: An Introduction. – Oxford: Oxford University Press, 2010.

67 Bonacich P. Factoring and Weighting Approaches to Status Scores and Clique Identification // The Journal of Mathematical Sociology. – 1972. – Vol. 2, No. 1. – P. 113–120. – DOI: 10.1080/0022250X.1972.9989806.

68 Seidman S. B. Network Structure and Minimum Degree // Social Networks. – 1983. – Vol. 5, No. 3. – P. 269–287. – DOI: 10.1016/0378-8733(83)90028-X.

69 Turner A. B., McCombie S., Uhlmann A. J. Analysis Techniques for Illicit Bitcoin Transactions // Frontiers in Computer Science. – 2020. – Vol. 2. – Art. 600596. – DOI: 10.3389/fcomp.2020.600596.

70 Reuters. Japan’s Tech Bureau Says About $60 Mln Stolen in Crypto Hack [Электронный ресурс]. – 2018. – URL: https://www.reuters.com/article/crypto-currencies-japan-cybercrime/japans-tech-bureau-says-about-60-mln-stolen-in-crypto-hack-idUKL3N1W5692/ – Дата обращения: 18.03.2026.

71 CoinDesk. Crypto Exchange Zaif Hacked in $60 Million Bitcoin Theft [Электронный ресурс]. – 2018. – URL: https://www.coindesk.com/markets/2018/09/20/crypto-exchange-zaif-hacked-in-60-million-bitcoin-theft – Дата обращения: 18.03.2026.

72 Federal Bureau of Investigation, Department of Defense Cyber Crime Center, National Police Agency of Japan. FBI, DC3, and NPA Identification of North Korean Cyber Actors, Tracked as TraderTraitor, Responsible for Theft of $308 Million USD from Bitcoin.DMM.com [Электронный ресурс]. – 2024. – URL: https://www.fbi.gov/news/press-releases/fbi-dc3-and-npa-identification-of-north-korean-cyber-actors-tracked-as-tradertraitor-responsible-for-theft-of-308-million-from-bitcoindmmcom – Дата обращения: 18.03.2026.

73 Elliptic. DMM Bitcoin Loses $308 Million in “Unauthorized Leak” [Электронный ресурс]. – 2024. – URL: https://www.elliptic.co/blog/dmm-bitcoin-loses-308-million-in-unauthorized-leak – Дата обращения: 18.03.2026.

74 U.S. Department of Justice. Bitfinex Hacker Sentenced in Money Laundering Conspiracy Involving Billions in Stolen Cryptocurrency [Электронный ресурс]. – 2024. – URL: https://www.justice.gov/archives/opa/pr/bitfinex-hacker-sentenced-money-laundering-conspiracy-involving-billions-stolen – Дата обращения: 18.03.2026.

75 Elliptic. New York Husband and Wife Arrested for Laundering Bitcoin [Электронный ресурс]. – 2022. – URL: https://www.elliptic.co/blog/elliptic-analysis-new-york-husband-and-wife-arrested-for-laundering-5-billion-in-bitcoin-stolen-from-bitfinex-in-2016 – Дата обращения: 19.03.2026.

76 U.S. Department of Justice. Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists DarkSide [Электронный ресурс]. – 2021. – URL: https://www.justice.gov/archives/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside – Дата обращения: 19.03.2026.

77 Chainalysis Team. Chainalysis in Action: How FBI Investigators Traced DarkSide's Funds Following the Colonial Pipeline Ransomware Attack [Электронный ресурс]. – 2022. – URL: https://www.chainalysis.com/blog/darkside-colonial-pipeline-ransomware-seizure-case-study/ – Дата обращения: 19.03.2026.

78 Elliptic. Elliptic Follows Bitcoin Ransoms Paid by Ransomware Victims [Электронный ресурс]. – 2021. – URL: https://www.elliptic.co/blog/elliptic-follows-bitcoin-ransoms-paid-by-darkside-ransomware-victims – Дата обращения: 19.03.2026.

79 U.S. Department of Justice. Ohio Resident Pleads Guilty to Operating Darknet-Based Bitcoin Mixer "Helix" [Электронный ресурс]. – 2021. – URL: https://www.justice.gov/archives/opa/pr/ohio-resident-pleads-guilty-operating-darknet-based-bitcoin-mixer-laundered-over-300-million – Дата обращения: 19.03.2026.

80 U.S. Department of Justice. Justice Department Investigation Leads to Takedown of Darknet Cryptocurrency Mixer That Processed over $3 Billion of Unlawful Transactions [Электронный ресурс]. – 2023. – URL: https://www.justice.gov/usao-edpa/pr/justice-department-investigation-leads-takedown-darknet-cryptocurrency-mixer-processed – Дата обращения: 20.03.2026.

81 U.S. Department of Justice. Bitcoin Fog Operator Sentenced for Money Laundering Conspiracy [Электронный ресурс]. – 2024. – URL: https://www.justice.gov/archives/opa/pr/bitcoin-fog-operator-sentenced-money-laundering-conspiracy – Дата обращения: 20.03.2026.

82 U.S. Attorney's Office, Southern District of New York. Founders of Samourai Wallet Cryptocurrency Mixing Service Plead Guilty [Электронный ресурс]. – 2025. – URL: https://www.justice.gov/usao-sdny/pr/founders-samourai-wallet-cryptocurrency-mixing-service-plead-guilty – Дата обращения: 20.03.2026.

83 U.S. Department of Justice. Russian National and Bitcoin Exchange Charged in 21-Count Indictment for Operating Alleged International Money Laundering Scheme and Allegedly Laundering Funds from Hack of Mt. Gox [Электронный ресурс]. – 2017. – URL: https://www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged – Дата обращения: 21.03.2026.

84 Goldsmith D., Grauer K., Shmalo Y. Analyzing Hack Subnetworks in the Bitcoin Transaction Graph [Электронный ресурс]. – 2019. – arXiv:1910.13415. – DOI: 10.48550/arXiv.1910.13415. – URL: https://arxiv.org/abs/1910.13415 – Дата обращения: 21.03.2026.

85 Paquet-Clouston M., Haslhofer B., Dupont B. Ransomware Payments in the Bitcoin Ecosystem // Journal of Cybersecurity. – 2019. – Vol. 5, No. 1. – Art. tyz003. – DOI: 10.1093/cybsec/tyz003.

86 Wu J., Liu J., Chen W., Huang H., Zheng Z., Zhang Y. Detecting Mixing Services via Mining Bitcoin Transaction Network with Hybrid Motifs [Электронный ресурс]. – 2020. – arXiv:2001.05233. – DOI: 10.48550/arXiv.2001.05233. – URL: https://arxiv.org/abs/2001.05233 – Дата обращения: 21.03.2026.

87 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. – DOI: https://doi.org/10.5815/ijcnis.2026.03.04.

88 Huber P. J., Ronchetti E. M. Robust Statistics. – 2nd ed. – Hoboken: Wiley, 2009. – DOI: 10.1002/9780470434697.

89 Shuman D. I., Narang S. K., Frossard P., Ortega A., Vandergheynst P. The Emerging Field of Signal Processing on Graphs // IEEE Signal Processing Magazine. – 2013. – Vol. 30, No. 3. – P. 83–98. – DOI: 10.1109/MSP.2012.2235192.

90 Hoerl A. E., Kennard R. W. Ridge Regression: Biased Estimation for Nonorthogonal Problems // Technometrics. – 1970. – Vol. 12, No. 1. – P. 55–67. – DOI: 10.1080/00401706.1970.10488634.

91 Boyd S., Vandenberghe L. Convex Optimization. – Cambridge: Cambridge University Press, 2004. – 716 p. – DOI: 10.1017/CBO9780511804441.

92 Prokhorenkova L., Gusev G., Vorobev A., Dorogush A. V., Gulin A. CatBoost: Unbiased Boosting with Categorical Features // Advances in Neural Information Processing Systems. – 2018. – Vol. 31. – P. 6638–6648.

93 Ke G., Meng Q., Finley T., Wang T., Chen W., Ma W., Ye Q., Liu T.-Y. LightGBM: A Highly Efficient Gradient Boosting Decision Tree // Advances in Neural Information Processing Systems. – 2017. – Vol. 30. – P. 3146–3154.

94 Chen T., Guestrin C. XGBoost: A Scalable Tree Boosting System // Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. – 2016. – P. 785–794. – DOI: 10.1145/2939672.2939785.

95 U.S. Department of the Treasury, Office of Foreign Assets Control. Specially Designated Nationals and Blocked Persons List (SDN List) [Электронный ресурс]. – URL: https://sanctionslist.ofac.treas.gov/Home/SdnList – Дата обращения: 22.03.2026.

96 U.S. Department of the Treasury, Office of Foreign Assets Control. Sanctions List Service [Электронный ресурс]. – URL: https://ofac.treasury.gov/sanctions-list-service – Дата обращения: 22.03.2026.

97 U.S. Department of the Treasury, Office of Foreign Assets Control. Questions on Virtual Currency: FAQs 562 and 563 [Электронный ресурс]. – URL: https://ofac.treasury.gov/faqs/topic/1626 – Дата обращения: 22.03.2026.

98 Chainabuse. Screening Addresses: API Documentation [Электронный ресурс]. – URL: https://chainabuse.readme.io/docs/get-reports-parameters – Дата обращения: 23.03.2026.

99 BitcoinAbuse. Bitcoin Abuse Database [Электронный ресурс]. – URL: https://www.bitcoinabuse.com/ – Дата обращения: 23.03.2026.

100 WalletExplorer. WalletExplorer.com: Smart Bitcoin Block Explorer [Электронный ресурс]. – URL: https://www.walletexplorer.com/ – Дата обращения: 23.03.2026.

101 OpenSanctions. OpenSanctions: The Open Database of Sanctions, PEPs and Watchlists [Электронный ресурс]. – URL: https://www.opensanctions.org/ – Дата обращения: 23.03.2026.

102 Financial Crimes Enforcement Network (FinCEN). Advisory on Illicit Activity Involving Convertible Virtual Currency: FIN-2019-A003 [Электронный ресурс]. – 2019. – URL: https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2019-a003 – Дата обращения: 20.03.2026.

103 Мусиралиева Ш. Ж., Шайзат М. Ж., Бекетова А. К., Абайұлы Е., Манасова А. Б. О методе идентификации подозрительных транзакций в Биткоин сети // Известия Национальной академии наук Республики Казахстан. Серия физико-математическая. – 2023. – № 1 (345). – С. 154–169. – DOI: 10.32014/2023.2518-1726.175.

104 Мусиралиева Ш. Ж., Шайзат М. Ж., Бекетова А. К., Манасова А. Б. Идентификация подозрительных операций в сети биткоин: анализ, признаки и алгоритмы машинного обучения // Вестник Национальной инженерной академии Республики Казахстан. – 2023. – № 3 (89). – С. 87–96. – DOI: 10.47533/2023.1606-146X.20.