ОТЗЫВ
официального рецензента на диссертационную работу
Шайзат Медета Жанболатұлы на тему «Разработка методов и моделей машинного обучения для киберкриминалистического анализа Bitcoin-транзакций», предоставленную на соискание степени доктора философии (PhD)
по образовательной программе «8D06301 – Системы информационной безопасности»

№ п/п	Критерии	Соответствие критериям (подчеркнуть один из вариантов ответа)	Обоснование позиции официального рецензента (замечания выделить курсивом)
1.	Тема диссертации (на дату ее утверждения) соответствует направлениям развития науки и/или государственным программам	1.1 Соответствие приоритетным направлениям развития науки или государственным программам: 1) диссертация выполнена в рамках проекта или целевой программы, финансируемого(ой) из государственного бюджета (указать название и номер проекта или программы); 2) диссертация выполнена в рамках другой государственной программы (указать название программы); 3) диссертация соответствует приоритетному направлению развития науки, утвержденному Высшей научно-технической комиссией при Правительстве Республики Казахстан (указать направление).	Тема диссертации соответствует направлениям развития науки и выполнена в рамках проекта, финансируемых из государственного бюджета фундаментальных и прикладных научных исследований молодых ученых «Жас ғалым» на 2025-2027 годы (AP25793719 «Разработка системы анализа незаконных криптовалютных транзакций»). Диссертация и проект соответствуют приоритетному направлению развития науки «Национальная безопасность и оборона, биологическая безопасность», и специализированному научному направлению «Прикладные научные исследования. Обеспечение информационной безопасности».
2.	Важность для науки	Работа вносит/не вносит существенный вклад в науку, а ее важность хорошо раскрыта/не раскрыта.	Диссертационная работа вносит существенный вклад в науку в области развития методов и инструментов криминалистического анализа криптовалютных операций, а ее важность хорошо раскрыта. Ключевыми результатами работы, имеющими существенное значение для развития профильного научного направления, являются обоснование наборов дескрипторов Bitcoin-транзакций, создание модели

			выявления нелегальных операций на основе алгоритма CatBoost, а также обёрточный метод отбора признаков на основе генетического поиска. Предложенные соискателем существенно повышают точность и содержательную интерпретируемость криминалистического анализа финансовых операций в блокчейне.
3.	Принцип самостоятельности	Уровень самостоятельности: 1) высокий; 2) средний; 3) низкий; 4) самостоятельности нет.	Содержание работы позволяет оценить уровень самостоятельности соискателя как высокий. Показано умение автора проводить научный поиск и анализ данных, провести все этапы исследований от постановки проблемы, формализации, сбора данных и отбора дескрипторов, построения моделей машинного обучения и реализации веб-приложения для криминалистического анализа криптовалютных операций до интерпретации результатов и подготовки научных статей.
4.	Принцип внутреннего единства	4.1 Обоснование актуальности диссертации: 1) обоснована; 2) частично обоснована; 3) не обоснована.	Актуальность темы диссертационного исследования всесторонне обоснована как на национальном уровне – в связи с требованиями Закона РК «О цифровых активах» и потребностями финансового мониторинга, так и на международном – с учетом масштабов незаконного оборота криптовалют и сложности имплементации стандартов FATF. Актуальность тематики исследований связана с недостаточностью методов выявления нелегальных Bitcoin-транзакций с сохранением смысловой интерпретируемости результатов для аналитиков и правоохранительных органов.
		4.2 Содержание диссертации отражает тему диссертации: 1) отражает;	Содержание диссертационной работы полностью отражает её тему, что подтверждается четкой и логичной структурой из 4-х разделов, последовательно раскрывающих все этапы

		2) частично отражает; 3) не отражает.	выполнения исследовательских задач – от анализа существующих подходов и разработки метода отбора признаков на основе генетического алгоритма до формирования интерпретируемых дескрипторов, построения моделей машинного обучения и их программной реализации.
		4.3. Цель и задачи соответствуют теме диссертации: 1) соответствуют; 2) частично соответствуют; 3) не соответствуют.	Сформулированная цель по разработке методов формирования интерпретируемых признаков и моделей машинного обучения напрямую вытекает из темы диссертационной работы и фокусируется на решении её ключевой проблемы. Восемь декомпозированных задач образуют полный цикл исследований – от обзора существующих подходов, формирования наборов данных до практической оценки алгоритмов машинного обучения, реализации программной системы, анализа и интерпретации результатов.
		4.4 Все разделы и положения диссертации логически взаимосвязаны: 1) полностью взаимосвязаны; 2) взаимосвязь частичная; 3) взаимосвязь отсутствует.	Все разделы диссертационной работы логически взаимосвязаны и объединены методологией последовательного исследования: каждый последующий раздел и этап исследований основан на результатах предшествующих шагов. Все положения, выносимые на защиту, представлены в главах диссертационной работы, кроме первого обзорного раздела.
		4.5 Предложенные автором новые решения (принципы, методы) аргументированы и оценены по сравнению с известными решениями: 1) критический анализ есть; 2) анализ частичный;	В диссертации приведены результаты сравнительной оценки предложенных методов с существующими аналогами и базовыми бенчмарками в строгой метрической аргументации. В частности, эффективность обёрточного метода отбора признаков подтверждается явным превосходством над опубликованными показателями

		3) анализ представляет собой не собственные мнения, а цитаты других авторов; 4) анализ отсутствует.	модели RF+GCN (повышение метрик Precision, Recall и F1-score). Ценность системы из 61 интерпретируемого дескриптора и модели CatBoost доказана результатами анализа и ростом ключевых показателей качества (PR-AUC, F1-score) для всех сравниваемых моделей.
5.	Принцип научной новизны	5.1 Научные результаты и положения являются новыми? 1) полностью новые; 2) частично новые (новыми являются 25-75%); 3) не новые (новыми являются менее 25%).	Все научные результаты и положения, выносимые на защиту, обладают высокой научной новизной, в частности: - система из 61 криминалистически интерпретируемого дескриптора Bitcoin-транзакций, впервые формализующая паттерны локального отклонения, динамики расходования и истории транзакций; -модель выявления нелегальных транзакций на основе CatBoost, обученная на наборе данных с полностью раскрытой семантикой признаков вместо анонимизированных; -обёрточный метод отбора признаков на базе генетического поиска и оценки Random Forest, сокративший признаковое пространство Elliptic со 166 до 53 признаков с превосходством над базовым бенчмарком (RF+GCN). Обоснованность и корректность научных результатов, положений подтверждаются их апробацией на международных научных конференциях и публикацией результатов в рецензируемых изданиях, включая журналы, индексируемые в базе Scopus и рекомендованные КОКСНВО МНВО РК.
		5.2 Выводы диссертации являются новыми? 1) полностью новые; 2) частично новые (новыми являются 25-75%); 3) не новые (новыми являются менее	Выводы диссертационной работы являются полностью новые и подтверждены теоретически и экспериментально через абляционный анализ и сравнение с существующими моделями. Сформулированные заключения раскрывают закономерности потоков средств в транзакционных графах и доказывают эффективность перехода от

		25%).	анонимизированных признаков к интерпретируемым дескрипторам и алгоритмам машинного обучения.
		5.3 Технические, технологические, экономические или управленческие решения являются новыми и обоснованными:	В качестве нового технического и технологического решения сосикателем разработана гибридная архитектура и полнофункциональная система криминалистического анализа Bitcoin-транзакций. Данное решение реализовано в виде веб-приложения, включающего серверную часть, базу данных, модули загрузки данных блокчейна, REST API, блоки машинного обучения, а также функционал поведенческого и графового анализа.
		1) полностью новые;	
		2) частично новые (новыми являются 25-75%);	
		3) не новые (новыми являются менее 25%).	
6.	Обоснованность основных выводов	Все основные выводы основаны/не основаны на весомых с научной точки зрения доказательствах либо достаточно хорошо обоснованы (для qualitative research (куолитатив ресеч) и направлений подготовки по искусству и гуманитарным наукам).	Все основные выводы и заключения диссертационного исследования являются хорошо обоснованными. Достоверность полученных результатов подтверждается использованием репрезентативных выборок реальных данных публичного блокчейна Bitcoin (наборы Elliptic и Elliptic++), применением корректного математического аппарата и алгоритмов машинного обучения (CatBoost, Random Forest, генетический алгоритм), а также проведением абляционного анализа. Высокая точность, воспроизводимость и статистическая значимость выводов аргументированы превосходством метрик качества (PR-AUC, F1-score) над существующими аналогами и апробацией в международных рецензируемых изданиях.
7.	Основные положения, выносимые на защиту	Необходимо ответить на следующие вопросы по каждому положению в отдельности:	Положение №1 – система криминалистически интерпретируемых признаков Bitcoin-транзакций, формализующая криминалистические гипотезы, повышает качество выявления нелегальных транзакций. Положение доказано на основе проведения серии контрольных экспериментов и абляционного анализа на репрезентативных наборах данных, продемонстрировав
		7.1 Доказано ли положение?	
		1) доказано;	
		2) скорее доказано;	
		3) скорее не доказано;	

		4) не доказано; 5) в текущей формулировке проверить доказанность положения невозможно. 7.2 Является ли тривиальным? 1) да; 2) нет; 3) в текущей формулировке проверить тривиальность положения невозможно. 7.3 Является ли новым? 1) да; 2) нет; 3) в текущей формулировке проверить новизну положения невозможно. 7.4 Уровень для применения: 1) узкий; 2) средний; 3) широкий; 4) в текущей формулировке проверить уровень применения положения невозможно. 7.5 Доказано ли в статье? 1) да; 2) нет; 3) в текущей формулировке проверить доказанность положения в статье невозможно.	устойчивый рост метрик качества (PR-AUC, F1-score) для всех тестируемых алгоритмов при добавлении 61 разработанного дескриптора. Не является тривиальным, так как формализация экспертных криминалистических гипотез в виде 61 количественного признака (динамика последующего расходования, локальные графовые отклонения и др.) представляет собой сложную научно-прикладную задачу, ранее не имевшую строгой математической интерпретации. Положения является новым, предложенный подход впервые объединяет транзакционные, временные и графовые параметры с целью обеспечения содержательной криминалистической интерпретируемости. Уровень для применения: широкий, так как сформированная система интерпретируемых признаков универсальна для блокчейна Bitcoin и может применяться в подразделениях финансового мониторинга, правоохранительных органах. Доказано в [M.Shaizat, Sh. Mussiraliyeva, I.Tereikovskyi, "Forensically Interpretable Graph Descriptors for Improved Illicit Bitcoin Transaction Detection", International Journal of Computer Network and Information Security, Vol.18, No.3, pp. 63-84, 2026.]. Положение №2 – модель выявления нелегальных Bitcoin-транзакций на основе алгоритма CatBoost, обученная на сформированном наборе данных с семантически открытыми транзакционными, структурно-графовыми и криминалистически интерпретируемыми признаками. Положение доказано, высокие значения целевых метрик (PR-AUC 90.27%, F1-score 83.90%, Recall 81.11%) на восстановленных реальных транзакционных данных подтверждают работоспособность и корректность предложенной модели CatBoost. Положение не является тривиальным, так как реконструкция публичных

			идентификаторов транзакций из анонимизированного бенчмарка Elliptic и эффективное адаптивное обучение модели CatBoost на 87 семантически открытых признаках требуют сложных процедур. Является новым, впервые предложена модель, преодолевающая ключевое ограничение популярных анонимизированных наборов данных и позволяющая проводить первичный анализ реальных Bitcoin-транзакций в практических условиях. Уровень для применения широкий, так как предлагаемая модель может быть интегрирована в системы мониторинга криптовалютных транзакций и инструментарий экспертов-криминалистов для оперативного анализа цифровых активов. Доказано в [M.Shaizat, Sh. Mussiraliyeva, I.Tereikovskyi, "Forensically Interpretable Graph Descriptors for Improved Illicit Bitcoin Transaction Detection", International Journal of Computer Network and Information Security, Vol.18, No.3, pp. 63-84, 2026.] Положение № 3 – метод отбора признаков для блокчейн-наборов данных с анонимизированными признаками, основанный на генетическом поиске и оберточной оценке моделью Random Forest. Доказательность подтверждается прямым сравнительным экспериментом, где сокращение признакового пространства со 166 до 53 не только не снизило, но и статистически значимо повысило точность классификации по сравнению с бенчмарком RF+GCN. Положение не является ли тривиальным, так как использование генетического поиска, адаптированного строго под временные срезы блокчейн-данных без риска утечки информации является оригинальным техническим и математическим решением. Положение является новым, впервые предложен обёрточный метод отбора анонимизированных признаков для графовых блокчейн-

			данных, превосходящий по качеству сложные гибридные графовые нейросети (GCN). Уровень для применения - средний, так как метод ориентирован на оптимизацию работы с датасетами, что актуально для исследователей и разработчиков специализированного ПО с импользованием моделей машинного обучения. Доказано в [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.]
8.	Принцип достоверности.	8.1 Выбор методологии - обоснован или методология достаточно подробно описана:	Выбор методологии исследования полностью обоснован логикой решения поставленной научной проблемы и предметной областью. В работе подробно описан системный и сравнительный анализ, генетический алгоритм, методы машинного обучения (CatBoost, Random Forest), а также способы построения и анализа транзакционных графов.
	Достоверность источников и предоставляемой информации	1) да;	
		2) нет.	
		8.2 Результаты диссертационной работы получены с использованием современных методов научных исследований и методик обработки и интерпретации данных с применением компьютерных технологий:	Диссертационное исследование выполнено на высоком современном технологическом уровне. В процессе работы соискатель использовал методы машинного обучения, графового анализа и интерпретируемого ИИ. Сбор, очистка, агрегация данных блокчейна, обучение моделей и анализ графов реализованы с помощью современного программного стека и оформлены в виде полноценного веб-приложения с REST API.
		1) да;	
		2) нет.	

		8.3 Теоретические выводы, модели, выявленные взаимосвязи и закономерности доказаны и подтверждены экспериментальным исследованием (для направлений подготовки по педагогическим наукам результаты доказаны на основе педагогического эксперимента):	Все теоретические положения, предложенные дескрипторы и модели классификации подтверждены вычислительными экспериментами. Эффективность системы из 61 признака доказана ростом метрик качества классификации (PR-AUC и F1-score) для всей линейки проверенных моделей, а преимущество метода отбора признаков подтверждено экспериментальным сопоставлением с результатами базового бенчмарка RF+GCN на данных Elliptic и Elliptic++.
		1) да;	
		2) нет.	
		8.4 Важные утверждения подтверждены/частично подтверждены/не подтверждены ссылками на актуальную и достоверную научную литературу.	Важные утверждения, теоретические предпосылки, статистика противодействия нелегальных криптовалютных транзакций средств (FATF, Chainalysis) и критический анализ существующих подходов в полной мере подтверждены ссылками на современную научную литературу и нормативные акты.
		8.5 Использованные источники литературы достаточны/не достаточны для литературного обзора.	Использованные источники литературы достаточны для литературного обзора: список использованной литературы включает 104 наименования, в том числе фундаментальные и современные публикации в области кибербезопасности, анализа блокчейн-сетей и машинного обучения.
9	Принцип практической ценности	9.1 Диссертация имеет теоретическое значение:	Диссертация имеет теоретическое значение, которое заключается в развитии научно-методических основ интерпретируемого криминалистического анализа блокчейн-сетей и транзакций в ней. Соискатель систематизировал и математически формализовал признаки локального отклонения от графового окружения, динамики последующего движения средств и истории транзакций, предложил модели машинного обучения для выявления нелегальных транзакций.
		1) да;	
		2) нет.	

		9.2 Диссертация имеет практическое значение и существует высокая вероятность применения полученных результатов на практике: 1) да; 2) нет.	Практическая ценность работы подтверждается созданием готового программно-аналитического комплекса для выявления и классификации подозрительных Bitcoin-транзакций. Имеет высокий потенциал внедрения разработанного инструментария в деятельность подразделений финансового мониторинга, правоохранительных органов, криптовалютных бирж и организаций, осуществляющих противодействие отмыванию нелегальных доходов.
		9.3 Предложения для практики являются новыми: 1) полностью новые; 2) частично новые (новыми являются 25-75%); 3) не новые (новыми являются менее 25%).	Новизна практических предложений заключается в замене анонимизированных признаков полностью прозрачной системой из 61 интерпретируемого дескриптора и прикладной модели CatBoost на основе 87 открытых признаков. Разработанная гибридная архитектура веб-приложения с REST API и модулями графового и поведенческого анализа предоставляет экспертам-криминалистам качественно новый инструментарий анализа реальных блокчейн-транзакций.
10.	Качество написания и оформления	Качество академического письма: 1) высокое; 2) среднее; 3) ниже среднего; 4) низкое.	Качество академического письма в диссертационной работе оценивается как высокое. Текст отличается строгим научным стилем, четкостью и логической последовательностью изложения. Представленная диссертационная работа полностью соответствует установленным требованиям к оформлению и содержанию исследований на соискание степени доктора философии (PhD).
11.	Замечания к диссертации	Имеются следующие замечания и рекомендации по представленной работе: 1. В названии и в тексте диссертационной работы используется словосочетание «киберкриминалистический анализ». В международной и отечественной практике более общепринятыми и установившимися являются термины «цифровая криминалистика» (Digital Forensics) или «компьютерно-техническая экспертиза». Требуется разъяснение термина. 2. Подраздел 3.3 содержит содержательный анализ практических кейсов, но связь каждого рассмотренного случая с конкретными разработанными признаками распределена по тексту.	

		Наглядность раздела повысила бы итоговая таблица, сопоставляющая кейсы, наблюдаемые схемы движения средств и соответствующие группы дескрипторов. 3. В работе не приведено свидетельство о государственной регистрации прав на объект авторского права на программу для ЭВМ. В качестве рекомендации предлагается юридически закрепить авторские права на веб-приложение для анализа Bitcoin-транзакций, что также облегчит процесс его практического внедрения в деятельность правоохранительных органов и структур финансового мониторинга. Указанные замечания и рекомендация не снижают общей высокой научной и практической ценности диссертационной работы и не влияют на положительную оценку исследования в целом.
12.	Научный уровень статей докторанта по теме исследования (в случае защиты диссертации в форме серии статей официальные рецензенты комментируют научный уровень каждой статьи докторанта по теме исследования)	Результаты диссертации по теме исследования были опубликованы в двух изданиях, индексируемых в базе данных Scopus, две статьи были опубликованы в изданиях, рекомендованных Комитетом по обеспечению качества в области образования и науки Министерства образования Республики Казахстан, одна работа статей была опубликована в сборнике материалов международной научной конференции. Высокий процентиль международных журналов (вплоть до 72-го процентиля Scopus) и прохождение апробации в виде независимого международного рецензирования подтверждают высокую научную новизну, методологическую строгой корректность и практическую значимость результатов, вынесенных соискателем на защиту.
13.	Решение официального рецензента (согласно пункту 28 настоящего Типового положения)	На основании вышеизложенного, диссертационная работа Шайзат Медета Жанболатұлы на тему «Разработка методов и моделей машинного обучения для киберкриминалистического анализа Bitcoin-транзакций» является завершенным научным исследованием, выполнена на высоком научно-методологическом уровне, полностью соответствует требованиям к диссертационным работам, а ее автор Шайзат Медет Жанболатұлы заслуживает присуждения степени доктора философии (PhD) по образовательной программе «8D06301 – Системы информационной безопасности».

Официальный рецензент,
к.ф.-м.н., профессор,
директор НИИ информационной
безопасности и криптологии
НАО «Евразийский национальный
университет имени Л.Н. Гумилева» **Сатыбалдина Д.Ж.**

ҚОЛЫН КУӘЛАНДЫРАМЫН
«Л.Н. Гумилев атындағы Еуразия ұлттық университеті» КеАҚ
ҚЫЗМЕТКЕРЛЕР БАСҚАРМАСЫ
«5» 08 2026 ж.
қолы