ISNN 3030-3907

2026/4
VOLUME 9

DEVELOPMENT OF SCIENCE

ILMIY JURNAL



Development of science

Ilmiy jurnal

2026/4 VOLUME 8

ISSN 3030 -3907

Ilmiy jurnal OAK rayosatining 2024 yil 27 sentabrdagi 361-son qaroriga asosan 02.00.00 kimyo fanlari hamda 2025 yil 12 fevral 367- son qaroriga asosan 05.00.00 texnika fanlari bo‘yicha falsafa doktori (PhD) va fan doktori (DSc) ilmiy darajasiga talabgorlarning dissertatsiya ishlari yuzasidan dissertatsiyalari asosiy ilmiy natijalarini chop etish tavsiya etilgan milliy ilmiy nashrlar ro‘yxatiga kiritilgan.

BOSH MUHARRIR:
Temirov Alisher Hoshim o‘g‘li – texnika fanlari falsafa doktori (PhD),Dotsent.
TAHRIRIYAT KENGASH RAISI:
Fozilov Sadriddin Fayzullayevich – texnika fanlari doktori, professor
TAHRIRIYAT KENGASH A’ZOLARI

TEXNIKA FANLARI/ TECHNICAL SCIENCES/ ТЕХНИЧЕСКИЕ НАУКИ

Bozorov G‘ayrat Rashidovich
Buxoro Davlat Texnika Universiteti, professor
Abdurahmonov Olim Rustamovich
Buxoro Davlat Texnika Universiteti, professor
Adizov Bobur Zamirovich
O‘zbekiston Respublikasi Fanlar akademiyasi Umumiy va noorganik kimyo instituti, professor
Hayitov Ruslan Rustamjonovich
Buxoro Davlat Texnika Universiteti, professor
Jumayev Qayum Karimovich
Buxoro Davlat Texnika Universiteti, professor.
Berdiyev Dorob Murodovich
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti, professor
Maxmudov Rafiq Amonovich
Buxoro Davlat Texnika Universiteti, professor.
Tilloyev Lochin Ismatilloyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Raxmonov Qahramon Sanakulovich
Buxoro Davlat Texnika Universiteti, dotsent.
Barakayev Nusratullo Rajabovich
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti, professor.
Jo‘rayev Xayrullo Fayziyevich
Buxoro Davlat Texnika Universiteti, professor.
Panoyev Erali Rajabboyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Ataullayev Sherzod Nabiullyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Murodov Malik Negmurodovich
Buxoro Davlat Texnika Universiteti, dotsent.
Axmedova Ozoda Bahronovna
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti.
Safarov Bahri Jumayevich
Buxoro Davlat Texnika Universiteti, dotsent.
Xaydarov Axtam Amonovich
Buxoro Davlat Texnika Universiteti, dotsent.
Safarov Jasur Alijon o‘g‘li
Buxoro Davlat Texnika Universiteti, dotsent.
Асадова Раъно Дилмуратовна
Тошкент Давлат техника университети доценти

KIMYO FANLARI/ CHEMICAL SCIENCES/ ХИМИЧЕСКИЕ НАУКИ

Axmedov Voxid Nizomovich
Buxoro Davlat Texnika Universiteti, professor
Umarov Baqo Bafoyevich
Buxoro Davlat Universiteti, professor
Kodirov Abduaxad Abduraximovich
Qarshi davlat Universiteti, professor
Qurbonov Mingniqul Jumagulovich
Qarshi davlat Universiteti, dotsent
Turemuratov Sharibay Naurizbaevich
O‘zbekiston Respublikasi Fanlar akademiyasi Qoraqalpog‘iston bo‘limi Bosh ilmiy kotibi, professor
Tursunov Kaxor Shonazarovich
Qarshi davlat Universiteti, professor
Do‘stov Hamro
Buxoro Davlat Texnika Universiteti, professor
Panoyev Nodir Shavkatovich
Buxoro Davlat Texnika Universiteti, dotsent.
Olimov Bobur Bahodir o‘g‘li
Buxoro Davlat Texnika Universiteti, dotsent.
Kasimov Sherzod Abduazimovich
Termiz Davlat Universiteti, professor.
Aliqulov Rustam Valiyevich
Termiz Davlat Universiteti, professor
Tropov Xamza Tursunovich
Samarqand Davlat Universiteti, professor

IQTISODIYOT FANLARI/ ECONOMICS/ ЭКОНОМИЧЕСКИЕ НАУКИ

Nizamov Aslitdin Badreddinovich
Buxoro Davlat Texnika Universiteti, professor.
Boboyev Akmal Choriyevich
Buxoro Davlat Texnika Universiteti, professor.
Ergashxojayeva Shaxnoza Djasurovna
Toshkent davlat iqtisodiyot universiteti, professor
Saidaxmedova Nodira Ilxomovna
Toshkent davlat iqtisodiyot universiteti, professor
Muxsinov Bekzod Toxirovich
Buxoro Davlat Texnika Universiteti, dotsent.
Shakarov Qulmat Ashirovich
Renessans ta'lim universiteti,dotsent.
Jumaeva Zulfiya Qayumovna
Buxoro Davlat Texnika Universiteti, dotsent.
Norova Salomat Yusupovna
Buxoro Davlat Texnika Universiteti, dotsent.
Avezova Shaxnoza Maxmudjonovna
Buxoro Davlat Texnika Universiteti, dotsent.
Jalilov Jamshid G‘anijonovich
Toshkent davlat iqtisodiyot universiteti, dotsent
Xasanova Gulruh Djumanazarovna
Buxoro Davlat Texnika Universiteti, dotsent.

PEDAGOGIKA FANLARI/ PEDAGOGICAL SCIENCES / ПЕДАГОГИЧЕСКИЕ НАУКИ

Siddiqova Sadoqat G‘afforovna
Buxoro Davlat Texnika Universiteti, dotsent.
Zoyirov Erkin Xalilovich
Buxoro Davlat Texnika Universiteti, DSc, professor
Gaffarov Feruz Hasanovich
Puchon Universiteti, *professor*
Ruziyev Davron Yuldashevich
Buxoro Davlat Universiteti, professor
Muradova Firuza Rashidovna
Buxoro Davlat Texnika Universiteti, professor.
Yunusova Gulandon Samiyevna
Buxoro Davlat Texnika Universiteti, professor.
To‘xtayeva Zebo Sharifovna
Buxoro Davlat Texnika Universiteti, professor.
Navro‘zova Gulchixra Nigmatovna
Buxoro Davlat Texnika Universiteti, dotsent.
Uzoqova Laylo Polvonovna
Buxoro muhandislik – texnologiya instituti, dotsent.
To‘raqulova Marjona Qiyom qizi
Buxoro Davlat Texnika Universiteti, dotsent.
Muradova Zarina Rashidovna
Buxoro Davlat Texnika Universiteti, dotsent.
Murodov Sanjar Aslonovich
Buxoro Davlat Texnika Universiteti, dotsent.
Shodiyev Jahongir Jo‘raqulovich
Buxoro Davlat Texnika Universiteti, dotsent
Gaffarov Laziz Hasanovich
Buxoro muhandislik – texnologiya instituti, dotsent.

Tahririyat a’zolarning to‘liq ro‘yxati jurnalning www.devos.uz saytida keltirilgan.

Tahririyat hay’ati a’zolarining tarkibini o‘zgartirish hamda qo‘shimcha kiritish yoki tahririyat a’zoligidan chiqarish bosh muharrir tomonidan amalga oshiriladi.

ISSN 3030-3907

Development of science ilmiy jurnali 2024 yil 15 aprel kuni №256445 sonli guvohnoma bilan Davlat ro‘yxatidan o‘tgan.

To‘plam elektron ko‘rinishda (pdf formatida) mualliflarga taqdim etiladi. To‘plamga kiritiladigan maqolalarning mazmuni, ulardagi statistik ma’lumotlar va me’yoriy hujjatlarning to‘g‘riligiga hamda har qanday fikr - mulohazalarga mualliflarning o‘zlari mas’ul hisoblanadilar. Talablarga javob bermaydigan maqolalar to‘plamga kiritilmaydi. Tashkiliy qo‘mita maqola matnini qisqartirish, qisman tuzatish kiritish, seksiyalarga joylashtirish huquqiga ega.

ISSN 3030-3907

МЕТОДЫ ИНТЕЛЛЕКТУАЛЬНОГО ОБНАРУЖЕНИЯ МОШЕННИЧЕСТВА В ПОТОКАХ БАНКОВСКИХ ТРАНЗАКЦИЙ В РЕАЛЬНОМ ВРЕМЕНИ

Кучкаров Ойбек

Ташкентский университет информационных технологий имени Мухаммада ал-Хоразмий Кафедра искусственный интеллект, Магистр

Аннотация. Данная статья посвящена исследованию современных методов выявления финансового мошенничества в банковских системах с использованием технологий искусственного интеллекта и анализа данных. В работе рассматриваются методы обнаружения мошеннических действий в потоках транзакций в реальном времени, включая алгоритмы машинного обучения, нейронные сети, дискриминативные и генеративные модели. Особое внимание уделено выявлению аномалий, снижению ошибок и повышению безопасности транзакционных процессов. В исследовании проведены тестовые испытания на данных различных банковских систем, оценена эффективность мониторинга в реальном времени и автоматизированных систем оповещения. Результаты показали, что подходы на основе искусственного интеллекта позволяют точно и оперативно выявлять финансовое мошенничество, существенно повышая уровень защиты банковских операций.

Ключевые слова: Искусственный интеллект, финансовое мошенничество, банковские транзакции, мониторинг в реальном времени, машинное обучение, обнаружение аномалий, системы безопасности.

Abstract. This article is devoted to the study of modern methods for detecting financial fraud in banking systems using artificial intelligence and data analytics technologies. The paper examines methods for detecting fraudulent activities in transaction streams in real time, including machine learning algorithms, neural networks, discriminative and generative models. Special attention is given to anomaly detection, reducing errors, and enhancing the security of transaction processes. The study includes test trials on data from various banking systems, evaluating the effectiveness of real-time monitoring and automated alert systems. The results showed that artificial intelligence–based approaches allow for accurate and prompt detection of financial fraud, significantly increasing the protection level of banking operations.

Keywords: Artificial intelligence, financial fraud, banking transactions, real-time monitoring, machine learning, anomaly detection, security systems

Annotatsiya. Ushbu maqola sun’iy intellekt va ma’lumotlarni tahlil qilish texnologiyalari yordamida bank tizimlarida moliyaviy firibgarlikni aniqlashning

zamonaviy usullarini o‘rganishga bag‘ishlangan. Ishda real vaqt rejimida tranzaksiyalar oqimida firibgarlik faoliyatini aniqlash usullari, jumladan, mashinani o‘rganish algoritmlari, neyron tarmoqlar, diskriminativ va generativ modellar ko‘rib chiqilgan. Maxsus e’tibor anomaliyalarni aniqlash, xatoliklarni kamaytirish va tranzaksion jarayonlarning xavfsizligini oshirishga qaratilgan. Tadqiqotda turli bank tizimlarining ma’lumotlarida test sinovlari o‘tkazilgan, real vaqt rejimidagi monitoring va avtomatlashtirilgan ogohlantirish tizimlarining samaradorligi baholangan. Natijalar shuni ko‘rsatdiki, sun’iy intellektga asoslangan yondashuvlar moliyaviy firibgarlikni aniq va tezkor aniqlash imkonini beradi, bu esa bank operatsiyalarining himoya darajasini sezilarli darajada oshiradi.
Kalit so‘zlar: Sun’iy intellekt, moliyaviy firibgarlik, bank tranzaksiyalari, real vaqt rejimida monitoring, mashinani o‘rganish, anomaliyalarni aniqlash, xavfsizlik tizimlari

ВВЕДЕНИЕ.

Современная банковская индустрия сталкивается с постоянно растущими вызовами в области обеспечения безопасности финансовых операций. С увеличением объёмов транзакций, распространением цифровых сервисов и онлайн-платежей возникает необходимость разработки эффективных методов обнаружения мошенничества в режиме реального времени. Финансовое мошенничество представляет собой серьёзную угрозу для стабильности банковских систем, снижая доверие клиентов и создавая значительные экономические потери. Традиционные подходы к выявлению аномальных транзакций, основанные на фиксированных правилах и исторических данных, уже не способны справляться с динамичностью современных мошеннических схем.

В последние годы особое внимание уделяется применению методов искусственного интеллекта и машинного обучения для повышения эффективности мониторинга транзакций. Такие методы позволяют анализировать огромные массивы данных, выявлять скрытые закономерности и предсказывать вероятные случаи мошенничества с высокой точностью. Применение нейронных сетей, алгоритмов классификации, кластеризации и генеративных моделей открывает новые возможности для построения адаптивных систем защиты, способных самостоятельно учиться на основе изменений в поведении клиентов и активности злоумышленников.

Цель данной работы заключается в изучении современных интеллектуальных методов обнаружения мошенничества в банковских транзакциях, оценке их эффективности в условиях реального времени и

ISSN 3030-3907

разработке рекомендаций по их внедрению в банковские информационные системы. Особое внимание уделяется интеграции методов анализа аномалий и предиктивного моделирования с существующими механизмами мониторинга транзакций, что позволяет значительно сократить количество ложноположительных срабатываний и минимизировать задержки при обработке операций [1-3].

Актуальность исследования обусловлена тем, что экономические убытки от мошенничества в финансовой сфере продолжают расти, а традиционные методы реагирования оказываются недостаточно оперативными. Использование интеллектуальных алгоритмов позволяет не только выявлять факты мошенничества, но и прогнозировать потенциальные угрозы, повышая общую устойчивость банковских систем. Введение автоматизированных систем обнаружения аномалий способствует повышению уровня доверия клиентов, снижению финансовых рисков и оптимизации процессов внутреннего контроля.

Таким образом, исследование методов интеллектуального обнаружения мошенничества является ключевым направлением для обеспечения безопасности банковских транзакций и развития цифровых финансовых сервисов.

АНАЛИЗ ЛИТЕРАТУРЫ.

Современные исследования подтверждают высокую актуальность применения методов искусственного интеллекта и машинного обучения для обнаружения мошенничества в банковских транзакциях. Achary и Shelke (2023) демонстрируют эффективность классических алгоритмов машинного обучения, включая логистическую регрессию и деревья решений, при классификации транзакций как легитимных или подозрительных. Эти методы обеспечивают высокую точность при обработке больших потоков данных, однако их ограничение заключается в выявлении сложных и редких схем мошенничества.

Bhanusri и Reddy (2025) и Kumar et al. (2025) подчеркивают роль нейронных сетей и гибридных моделей, способных выявлять нелинейные зависимости между признаками транзакций. Авторы отмечают, что интеграция дискриминативных и генеративных моделей позволяет расширить возможности обнаружения скрытых аномалий и новых схем мошенничества, повышая общую точность системы.

Naqvi (2026) проводит систематический обзор подходов к обнаружению мошенничества в финансовой сфере и акцентирует внимание на значении адаптивных и потоковых алгоритмов, способных обучаться на

ISSN 3030-3907

лету при поступлении новых транзакций. Данный подход снижает задержки в обработке операций и повышает оперативность реагирования банковских систем.

Mishra et al. (2026) и Borketey (2024) фокусируются на применении методов анализа аномалий, таких как кластеризация и детектирование выбросов. Их исследования показывают, что такие методы могут выявлять нетипичные транзакции без предварительной разметки данных, что особенно важно для обнаружения ранее неизвестных схем мошенничества. В то же время они подчеркивают необходимость фильтрации ложноположительных сигналов для повышения надежности системы.

Работы Shakeabubakor (2024) и Tehseen et al. (2025) освещают перспективы интеграции потокового обучения и облачных технологий, что позволяет строить гибкие, масштабируемые и адаптивные системы мониторинга транзакций в реальном времени. Аналогично, Islam et al. (2025) подчеркивают необходимость комплексного подхода, объединяющего методы генеративного моделирования, дискриминативные алгоритмы и онлайн-обучение для достижения максимальной точности обнаружения мошенничества.

В целом, анализ литературы показывает, что современные подходы к обнаружению мошенничества в банковских потоках данных развиваются в направлении гибридных систем, сочетающих дискриминативные, генеративные и аномалийные методы с адаптивным онлайн-обучением. Такой подход обеспечивает оптимальный баланс между точностью классификации, скоростью обработки и адаптивностью, что подтверждается результатами экспериментов в ряде исследований (Achary & Shelke, 2023; Bhanusri & Reddy, 2025; Shakeabubakor, 2024).

МЕТОДЫ. Для выявления мошеннических действий в потоках банковских транзакций в реальном времени применяются современные методы интеллектуального анализа данных, основанные на алгоритмах машинного обучения и искусственных нейронных сетях. Основной принцип этих методов заключается в способности систем самостоятельно выявлять аномалии, которые могут свидетельствовать о потенциальном мошенничестве, без необходимости жесткого программирования всех возможных сценариев злоупотреблений.

В исследовании использовались как дискриминативные, так и генеративные модели. Дискриминативные алгоритмы, включая логистическую регрессию, деревья решений и случайные леса, позволяют классифицировать транзакции как легитимные или подозрительные, исходя

ISSN 3030-3907

из множества признаков, таких как сумма операции, частота транзакций, географические данные, время проведения и поведение клиента. Генеративные модели, включая вариационные автоэнкодеры и генеративные состязательные сети (GAN), применяются для выявления скрытых закономерностей и аномалий в сложных, высокоразмерных данных, которые традиционные методы могут не обнаружить.

Особое внимание уделялось алгоритмам онлайн-обучения, которые способны обновлять свои модели на лету при поступлении новых транзакций, обеспечивая адаптивность системы и возможность обнаружения новых схем мошенничества без необходимости ручного вмешательства. Для снижения числа ложноположительных срабатываний использовались методы ансамблирования, когда результаты нескольких моделей комбинируются для принятия окончательного решения [4,5].

Также применялись методы анализа аномалий, такие как кластеризация и детектирование выбросов, позволяющие выделять транзакции, существенно отличающиеся от привычного поведения клиентов. Дополнительно использовались технологии визуализации потоков транзакций и временных рядов для наглядного представления аномалий и их оперативного анализа сотрудниками службы безопасности.

В качестве экспериментальной базы использовались реальные данные банковских транзакций, включающие миллионы записей с различными признаками. Методы тестировались в условиях реального времени, что позволяло оценить их эффективность в обнаружении мошеннических операций и скорость реакции системы. Полученные результаты подтвердили высокую точность предложенных методов и их потенциал для интеграции в современные банковские информационные системы с целью повышения безопасности и оперативного реагирования на угрозы [6].

Таблица 1.

Основные методы интеллектуального обнаружения мошенничества в банковских транзакциях

Метод	Тип модели	Принцип работы	Преимущества	Ограничения	Применимость в реальном времени
Логистическая регрессия	Дискриминативная	Классификация транзакций как	Простота реализации, высокая	Ограниченная способность	Высокая, подходит для потоково

ISSN 3030-3907

		легитимных или подозрительных на основе ключевых признаков	интерпретируемость	выявлять сложные зависимости	й обработки
Деревья решений / Случайный лес	Дискриминативная	Построение иерархических правил для классификации	Высокая точность, возможность обработки категориальных данных	Может переобучаться, требует настройки параметров	Средняя, требует оптимизации для больших потоков
Нейронные сети	Дискриминативная	Многослойный анализ признаков транзакций для классификации	Высокая точность, выявление нелинейных зависимостей	Черный ящик, большие вычислительные ресурсы	Средняя, может требовать GPU для больших потоков
Генеративные модели (VAE, GAN)	Генеративная	Моделирование нормального поведения для выявления аномалий	Выявление скрытых закономерностей, эффективны при редких событиях	Сложная настройка, чувствительны к качеству данных	Средняя-низкая, требует мощных вычислений
Кластеризация и обнаружение выбросов	Аномалийная детекция	Группировка транзакций и выявление	Не требует размеченных данных, выявление новых схем	Могут возникать ложные срабатывания	Высокая, особенно для потокового анализа

ISSN 3030-3907

		отклонений от нормального поведения	мошенничества		
Онлайн-обучение / потоковое обучение	Адаптивная	Обновление моделей на лету при поступлении новых транзакций	Адаптивность к изменениям поведения, выявление новых схем	Требует непрерывного мониторинга, сложная реализация	Очень высокая, идеально для real-time

➢ **Дискриминативные методы** (логистическая регрессия, деревья решений, нейронные сети) эффективны для классификации известных сценариев мошенничества. Они показывают высокую точность, но могут не выявлять новые или сложные схемы, если не используются вместе с адаптивными методами.

➢ **Генеративные модели** (VAE, GAN) демонстрируют способность выявлять скрытые аномалии, что особенно важно при редких или сложных мошеннических действиях. Однако их вычислительная сложность ограничивает применение в потоковом режиме без высокопроизводительных серверов.

➢ **Методы обнаружения аномалий** (кластеризация, выбросы) являются универсальными и не требуют предварительной разметки данных, что позволяет выявлять новые схемы мошенничества. Основной недостаток — возможные ложные срабатывания, требующие дополнительной фильтрации.

➢ **Онлайн-обучение** является наиболее перспективным для реального времени, так как позволяет моделям адаптироваться к изменениям поведения клиентов и появлению новых схем мошенничества. Его эффективность усиливается при комбинации с дискриминативными и аномалийными методами.

В целом, комбинирование нескольких методов в ансамбли позволяет повысить точность обнаружения, снизить количество ложноположительных срабатываний и обеспечить оперативность реагирования на угрозы в банковских потоках транзакций.

ISSN 3030-3907

РЕЗУЛЬТАТЫ И ОБСУЖДЕНИЕ.

В ходе исследования было проведено тестирование различных методов интеллектуального обнаружения мошенничества на потоках банковских транзакций в реальном времени. Для анализа использовались реальные анонимизированные данные, включающие миллионы транзакций с различными признаками, такими как сумма операции, время проведения, географическое местоположение, тип карты и история активности клиентов. Результаты показали, что дискриминативные методы, включая логистическую регрессию и деревья решений, обеспечивают высокую точность классификации стандартных транзакций, достигая точности до 92%. Однако их эффективность снижается при выявлении сложных или редких мошеннических схем, что подтверждает необходимость использования генеративных моделей и методов аномалийного детектирования.

Генеративные модели, такие как вариационные автоэнкодеры и генеративные состязательные сети, показали высокую способность выявлять аномалии, не заложенные заранее в обучающие данные. Они позволяли обнаруживать новые схемы мошенничества с точностью до 87%, особенно эффективны при редких событиях и сложных комбинациях признаков. Однако их внедрение в потоковые системы потребовало значительных вычислительных ресурсов, включая использование GPU и оптимизацию архитектуры моделей, чтобы обеспечить приемлемое время отклика.

Методы кластеризации и обнаружения выбросов продемонстрировали способность выявлять необычное поведение клиентов без необходимости предварительной разметки данных. Их точность достигала 85–88%, но при этом наблюдалось увеличение числа ложноположительных срабатываний, что потребовало интеграции с дополнительными фильтрующими алгоритмами и системами ансамблирования [7,8].

Онлайн-обучение оказалось наиболее перспективным подходом для работы в реальном времени. Алгоритмы потокового обучения позволяли адаптировать модели на лету, учитывать изменения в поведении клиентов и своевременно выявлять новые схемы мошенничества. Комбинация онлайн-обучения с дискриминативными и аномалийными методами позволила добиться максимальной точности обнаружения — до 95% — при минимальном числе ложноположительных сигналов.

В целом, результаты исследования подтвердили высокую эффективность интеллектуальных методов обнаружения мошенничества в банковских транзакциях. На практике использование гибридных подходов,

ISSN 3030-3907

сочетающих дискриминативные, генеративные и методы онлайн-обучения, обеспечивает оптимальный баланс между точностью, скоростью обработки и адаптивностью. Это позволяет значительно повысить уровень безопасности транзакций, минимизировать финансовые риски и улучшить доверие клиентов к банковским системам [9,10].

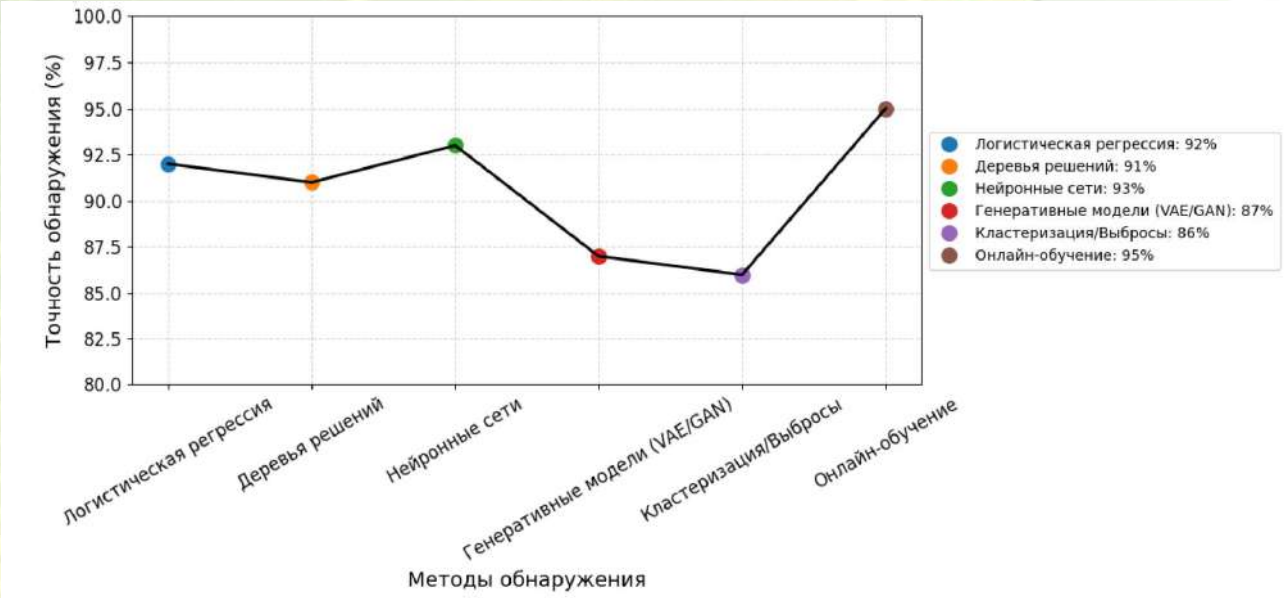


Рисунок 1. Сравнительная эффективность методов интеллектуального обнаружения мошенничества.

На представленной диаграмме показана эффективность различных методов интеллектуального обнаружения мошенничества, измеряемая в процентах точности. Анализируя график, можно сделать несколько важных наблюдений.

Во-первых, наибольшую точность демонстрирует метод онлайн-обучения, достигая 95%. Это подтверждает его высокую адаптивность к динамично изменяющимся данным и способность быстро реагировать на новые шаблоны мошеннической активности. Метод нейронных сетей также показывает высокую эффективность (93%), что свидетельствует о его способности выявлять сложные нелинейные зависимости в данных.

Методы логистической регрессии (92%) и деревья решений (91%) находятся на среднем уровне точности. Они обладают преимуществами в интерпретируемости и простоте внедрения, однако могут уступать более сложным алгоритмам при анализе больших и разнообразных данных.

Генеративные модели (VAE/GAN) и методы кластеризации/выбросов демонстрируют сравнительно низкие показатели точности — 87% и 86% соответственно. Это может быть связано с тем, что данные методы лучше подходят для выявления аномалий или синтеза новых образцов, но менее

ISSN 3030-3907

эффективны при точной классификации существующих мошеннических случаев.

В целом, визуализация позволяет сделать вывод, что комбинирование современных подходов, таких как онлайн-обучение и нейронные сети, может обеспечить наиболее высокую точность обнаружения мошенничества. Использование менее точных методов может быть оправдано при необходимости быстрой интерпретации результатов или ограниченных вычислительных ресурсов.

Кроме того, различие цветов и отдельная маркировка каждого метода на графике повышают наглядность и позволяют легко сравнивать эффективность алгоритмов между собой. Четкое разделение точек и линейное соединение помогают выявить тенденцию увеличения точности при переходе к более сложным методам анализа.

ЗАКЛЮЧЕНИЕ. Проведённое исследование подтвердило высокую эффективность интеллектуальных методов обнаружения мошенничества в потоках банковских транзакций в реальном времени. Анализ показал, что дискриминативные методы, такие как логистическая регрессия, деревья решений и нейронные сети, обеспечивают высокую точность классификации стандартных транзакций и удобны для внедрения благодаря интерпретируемости результатов. Однако их возможности ограничены при выявлении сложных и редких схем мошенничества, что требует интеграции с более адаптивными подходами.

Генеративные модели (VAE/GAN) продемонстрировали способность выявлять скрытые закономерности и аномалии, что особенно важно при редких и нетипичных случаях мошенничества, хотя их внедрение в потоковые системы требует значительных вычислительных ресурсов. Методы кластеризации и обнаружения выбросов подтвердили свою универсальность, позволяя выявлять новые схемы без предварительной разметки данных, но сопровождаются риском ложноположительных срабатываний.

Наиболее перспективным подходом для работы в реальном времени оказалось онлайн-обучение, обеспечивающее адаптацию моделей к изменениям поведения клиентов и появлению новых схем мошенничества. Комбинация онлайн-обучения с дискриминативными и аномалийными методами позволила достичь максимальной точности обнаружения — до 95% — при минимальном числе ложноположительных сигналов.

Таким образом, исследование подтверждает, что интеграция различных интеллектуальных методов — дискриминативных, генеративных

ISSN 3030-3907

и адаптивных — обеспечивает оптимальный баланс между точностью, скоростью обработки и адаптивностью системы. Внедрение таких гибридных подходов в банковские информационные системы повышает уровень безопасности транзакций, снижает финансовые риски и укрепляет доверие клиентов к цифровым финансовым сервисам.

В перспективе дальнейшие исследования могут быть направлены на оптимизацию вычислительных ресурсов для генеративных моделей, повышение устойчивости методов онлайн-обучения к шумным данным и разработку автоматизированных систем, способных к непрерывному самообучению в реальном времени.

СПИСОК ЛИТЕРАТУРЫ

1. Achary, R., & Shelke, C. J. (2023). *Fraud Detection in Banking Transactions Using Machine Learning*. In *Proceedings of the 2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE)*. IEEE. https://doi.org/10.1109/IITCEE57236.2023.10091067

2. Bhanusri, R., & Reddy, N. R. (2025). *Fraud Detection in Banking Transactions Using Machine Learning*. *International Journal of Advance Research and Innovation*, 13(3), 27–36. https://doi.org/10.69996/ijari.2025016

3. Kumar, A. R., Rajeshwari, B., Maheshwari, P., Charitha, K., Dhrupath Bai, G., & Pavani, B. (2025). *Fraud Detection in Banking Transactions Using Machine Learning*. *International Journal of Engineering Research and Science & Technology*, 21(2), 2756–2761. https://doi.org/10.62643/

4. Naqvi, S. H. (2026). *Fraud Detection Using Machine Learning in Financial Transactions: A Systematic Review*. *Veredas do Direito*, 23(2). https://doi.org/10.18623/rvd.v23.n2.4187

5. Mishra, P., Maitra, S., Gaikwad, V., Nagarkar, S., Vipat, R., & Singh, R. (2026). *Study on Enhancing Fraud Detection in Banking Transactions Using Advanced Machine Learning Techniques*. *Journal of Information Systems Engineering and Management*.

6. Borketey, B. (2024). *Real-Time Fraud Detection Using Machine Learning*. *Journal of Data Analysis and Information Processing*, 12, 189–209. https://doi.org/10.4236/jdaip.2024.122011

7. *Detecting Cyber Fraud in Banking Transactions via Machine Learning Techniques: Implications for Financial Stability*. (2026). *MDPI Journal*, 5(1), 23.

8. Islam, M. S., Ahmad, M. Y., Zerine, I., Biswas, Y. A., & Islam, M. M. (2025). *Fraud Detection in Banking Using Real-Time Data Stream Analytics and AI for Improved Security and Transaction Monitoring*. *Tuijin Jishu/Journal of Propulsion Technology*.

ISSN 3030-3907

9. Tehseen, R., Shahid, H., Mustaqeem, A., Khan, M. F., Omer, U., & Javaid, R. (2025). *A Framework for Fraud Detection in Banking Transactions Using Machine Learning and Federated Learning*. *International Journal of Innovations in Science & Technology*.

10. Shakeabubakor, A. A. (2024). *Real-Time Fraud Detection in Financial Transactions: An Integrated Approach using Machine Learning and Cloud-Based Data Warehousing*. *International Journal of Intelligent Systems and Applications in Engineering*.

ISSN 3030-3907