УДК 343.722
DOI 10.37468/2307-1400-2026-1-57-77

Технологии искусственного интеллекта в противодействии финансовым преступлениям: возможности и ограничения

Леонов Вячеслав Алексеевич [1]
Зайцев Александр Константинович [2]
Матвеев Владимир Владимирович [1]

[1] *Финансовый университет при Правительстве РФ (Санкт-Петербургский филиал), Санкт-Петербург, Россия*

[2] *Межрегиональное управление Федеральной службы по финансовому мониторингу по Северо-Западному федеральному округу, Санкт-Петербург, Россия*

Аннотация
Рассматриваются возможности применения технологий искусственного интеллекта в противодействии финансовым преступлениям как факторе обеспечения финансовой безопасности Российской Федерации. Показано, что противодействие легализации доходов, полученных преступным путем (ПОД/ФТ), и противодействие мошенничеству (антифрод-системы) образуют два различных класса задач, отличающихся объектом защиты, горизонтом анализа, правовой основой и доступностью размеченных данных, что определяет выбор методов. На основе обобщения нормативных признаков и материалов типологических исследований предложены сводные типологии схем легализации и мошеннических атак, каждая из которых соотнесена с наблюдаемыми признаками в транзакционных данных и применимыми методами машинного обучения. Обосновано, что в задачах противодействия легализации доходов, полученных преступным путем, приоритет принадлежит методам обучения без учителя и графовому анализу, тогда как в антифрод-системах эффективно обучение с учителем. Систематизированы ограничения применения искусственного интеллекта: дефицит и запаздывание разметки, границы наблюдаемости данных в периметре одной кредитной организации, проблема объяснимости решений, цена ошибки первого рода, адаптация схем к средствам контроля. Сделан вывод о роли искусственного интеллекта как инструмента приоритизации и сокращения пространства поиска для аналитика, а не автономного субъекта принятия решений.

Ключевые слова: финансовая безопасность, искусственный интеллект, машинное обучение, легализация преступных доходов, ПОД/ФТ, антифрод-система, графовая аналитика, финансовый мониторинг, транзакционный анализ.

Введение

Пункт 4 статьи 67 Стратегии национальной безопасности Российской Федерации определяет в качестве цели обеспечения экономической безопасности ускорение темпов прироста инвестиций в основной капитал, доступность долгосрочного кредитования, защиту и поощрение капиталовложений, стимулирование использования внутренних источников инвестиций [1]. Достижению этих целей препятствует ряд факторов, среди которых Стратегия экономической безопасности Российской Федерации на период до 2030 года выделяет нарастание геополитической нестабильности, обострение глобальной конкуренции и существенные изменения в международно-правовой и экономической областях [2]. Анализ мировых событий последних десятилетий позволяет сделать вывод о том, что мир в целом погружен в системный кризис, охватывающий все сферы жизнедеятельности как отдельных людей, так и социально-экономических систем, включая государства и их объединения [3].

В этих условиях самостоятельное значение приобретает противодействие финансовым преступлениям – легализации доходов, полученных преступным путем, и хищениям денежных средств с использованием цифровых технологий. Оба явления непосредственно затрагивают устойчивость национальной финансовой системы. Первое обеспечивает воспроизводство

преступной экономики и вывод капитала за пределы страны, второе подрывает доверие к безналичным расчетам и дистанционному банковскому обслуживанию.

Принципиальное затруднение состоит в несоизмеримости масштабов контролируемого потока и возможностей его ручной обработки. По данным Банка России, в стране совершается более 2,5 тысячи платежей и переводов ежесекундно [4]; объем розничного оборота по картам исчисляется десятками триллионов рублей в год [5]. Такой объем информации не может быть обработан вручную, что делает необходимым создание и использование информационно-аналитических систем [6].

Целью настоящей статьи является обоснование возможностей и определение ограничений применения технологий искусственного интеллекта (ИИ) в выявлении финансовых преступлений. Задачи работы: разграничить классы задач противодействия легализации доходов, полученных преступным путем и антифрод-систем; систематизировать типологии схем и их наблюдаемые признаки; соотнести признаки с применимыми методами машинного обучения; выявить принципиальные ограничения этих методов.

Эмпирическую основу исследования составили нормативные правовые акты Российской Федерации в сфере противодействия легализации преступных доходов и противодействия хищению денежных средств, публикуемые материалы Банка России и Росфинмониторинга, типологические исследования Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ, Financial Action Task Force)[2], а также научные публикации по применению методов машинного обучения в финансовом мониторинге.

Финансовые преступления как угроза финансовой безопасности Российской Федерации

Одной из значимых внутренних угроз российской экономики является отток капитала из страны, величина которого сопоставима с параметрами консолидированного государственного бюджета [7]. Существенную часть этого потока составляют операции, не имеющие очевидного экономического содержания.

Банк России фиксирует финансовые операции, входящие в стандартные категории: импорт товаров, инвестиции, погашение долга, оплата по исполнительным листам и другие. Наряду с ними в платежном балансе выделяется статья «чистые ошибки и пропуски», формально обозначаемая как статистическое расхождение. По данным, приводимым в открытых источниках, объем этой статьи в 2024 г. вырос примерно на треть по сравнению с 2023 г. и оказался наибольшим с 2012 г., приблизившись к уровням второй половины 1990-х гг. [8]. Динамика чистого оттока капитала представлена на Рисунке 1.

Отток капитала имеет несколько значений для национальной экономики. Во-первых, он сокращает объем денежной массы, обслуживающей внутренний оборот, что замедляет скорость обращения капитала и ограничивает объемы производимой продукции и услуг. Во-вторых, средства платежа в конвертируемой валюте, попадая за рубеж, фактически становятся инвестициями в экономику иностранного государства за счет средств резидентов страны-донора. В-третьих, эти средства могут возвращаться в страну происхождения уже в качестве портфельных инвестиций, но под высокий процент [9].

Следует признать, что капитал размещается там, где ниже риски и выше доходность. Однако принципиально важно различать легальный вывоз капитала и вывод средств, полученных преступным путем: первое является предметом валютного и инвестиционного регулирования, второе – предметом уголовно-правового и финансово-мониторингового реагирования. Соотношение форм капитала и способов его вывоза за границу представлено на Рисунке 2.

[2] **ФАТФ (Financial Action Task Force, FATF) –** международная межправительственная организация, которая разрабатывает стандарты противодействия отмыванию денег, финансированию терроризма и финансированию распространения оружия массового уничтожения (ПОД/ФТ/ФРОМУ), а также оценивает соответствие национальных систем этим стандартам.

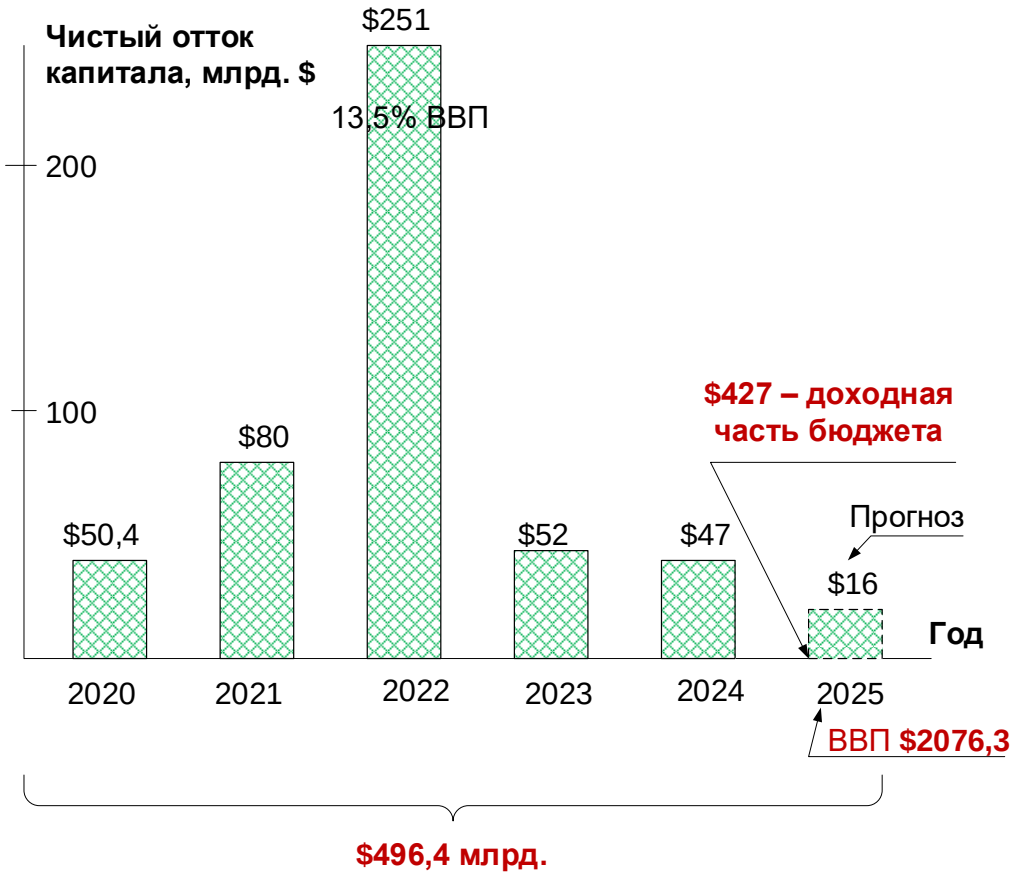

Рисунок 1 – Динамика чистого оттока капитала

Рисунок 2 – Формы капитала и сущность его вывоза за границу

Значительную часть криминального компонента оттока составляют денежные средства, полученные преступным путем, которые могут использоваться, в том числе, для финансирования терроризма и против интересов Российской Федерации [10].

Статистика Министерства внутренних дел Российской Федерации указывает, что среди преступлений экономической направленности значительное место занимают деяния, связанные с легализацией (отмыванием) денежных средств или иного имущества, приобретенных преступным путем (Таблица 1).

Таблица 1 – Показатели расследования преступлений экономической направленности в 2024 г. [11]

Показатель	Всего	Изменение к предыдущему году, %
Предварительно расследовано преступлений	77 571	−0,2
в том числе лица, установленные сотрудниками ОВД	63 982	−1,2
в том числе уголовные дела, направленные в суд	63 962	+1,6
Выявлено лиц, уголовные дела о которых направлены в суд	39 305	+5,3
в том числе установлено сотрудниками ОВД	33 018	+4,1

Приведенные данные характеризуют лишь выявленную часть противоправной деятельности. Латентность рассматриваемой категории преступлений традиционно высока, что дополнительно обосновывает необходимость совершенствования инструментов их выявления.

Задачи противодействия финансовым преступлениям

Применение ИИ в противодействии финансовым преступлениям предполагает различие двух классов задач, которые и определяют и выбор технологий ИИ и оценку качества их работы.

Противодействие легализации доходов, полученных преступным путем, направлено на защиту публичного интереса, т.е. устойчивости финансовой системы государства. Нарушителем здесь выступает сам клиент кредитной организации, действующий осознанно и, как правило, в составе организованной группы. Признаки противоправности проявляются не в отдельной операции, а в их совокупности на горизонте от нескольких недель до нескольких месяцев и в структуре связей между участниками расчетов. Правовую основу составляет Федеральный закон от 07.08.2001 № 115-ФЗ, подзаконные акты Банка России, а также рекомендации ФАТФ.

AML (Anti-Money Laundering, «противодействие отмыванию денег») – комплекс процедур финансового мониторинга, который организации обязаны проводить для выявления, предотвращения и сообщения о попытках легализовать доходы преступного происхождения [12]. В России регулируется № 115-ФЗ. Применяется банками, микрофинансовыми организациями, страховщиками, брокерами, операторами цифровых финансовых активов и другими организациями, работающими с деньгами или имуществом. AML в российском праве = ПОД/ФТ (противодействие легализации доходов и финансированию терроризма), в соответствии с базовым законом № 115-ФЗ от 07.08.2001.

Антифрод-система решает противоположную по конфигурации задачу – защиту средств клиента и банка от третьего лица, действующего против воли владельца счета. Горизонт анализа измеряется секундами, объектом оценки является единичная операция или сессия [13], а правовую основу образует законодательство о национальной платежной системе в редакции, установившей признаки осуществления перевода денежных средств без добровольного согласия клиента [14].

Различие этих задач имеет прямое методическое следствие – различную доступность размеченных данных.

В антифрод-системе разметка формируется быстро и почти автоматически, когда клиент оспаривает операцию, кредитная организация фиксирует факт хищения, и обучающая выборка пополняется достоверно определенным классом. Это создает благоприятные условия для обучения с учителем, т.к. модель располагает достаточным множеством подтвержденных примеров и может регулярно переобучаться.

В задачах AML-систем ситуация принципиально иная. Достоверным подтверждением факта легализации является вступивший в силу обвинительный приговор, отделенный от самой операции интервалом в несколько лет. Доля подтвержденных случаев в общем массиве операций очень мала, а сведения о результатах рассмотрения направленных сообщений возвращаются в кредитную организацию не в полном объеме. Следствием является нехватка и временная задержка получения разметки данных, а также крайняя несбалансированность классов. Поэтому центр тяжести смещается к методам, не требующим размеченной выборки, таким как обнаружение аномалий, кластеризация, а также к графовому анализу, для которого признаком выступает не свойство отдельной операции, а конфигурация связей между счетами.

Отсюда следует, что перенос решений, доказавших результативность в антифрод-системе, в контур AML-систем без пересмотра методической основы в целом нереализуем. При внешнем сходстве входных данных эти задачи опираются на разные типы обучения. Сопоставление двух классов задач приведено в Таблице 2.

Таблица 2 – Сопоставление задач ПОД/ФТ и антифрод-систем

Критерий	AML-система (ПОД/ФТ)	Антифрод-система
Защищаемый интерес	Устойчивость финансовой системы	Средства клиента и кредитной организации
Источник угрозы	Клиент, действующий осознанно	Третье лицо, действующее против воли клиента
Горизонт анализа	Недели и месяцы	Секунды
Единица наблюдения	Совокупность операций, структура связей	Операция, сессия
Правовая основа	№ 115-ФЗ, акты Банка России	Законодательство о национальной платежной системе
Доступность разметки	Низкая, с задержкой на годы	Высокая, в пределах дней
Преобладающие методы	Обучение без учителя, графовый анализ	Обучение с учителем
Цена ошибки первого рода	Ограничение доступа к обслуживанию	Повторная аутентификация

При этом обе задачи не изолированы, а образуют связанную систему [15]. Антифрод-системы выявляют счета, открытые по похищенным или синтетическим идентификационным данным, и учетные записи, используемые для транзитного перемещения средств; именно они образуют нижний уровень схем обналичивания, исследуемых в ПОД/ФТ. В обратном направлении сети, раскрытые в ходе финансового расследования, пополняют перечни повышенного риска, применяемые при операционном контроле.

Типология схем отмывания и наблюдаемые признаки

Легализация денежных средств, полученных преступным путем, описывается трехфазной моделью, включающей размещение, расслоение и интеграцию (Рисунок 3).

Одной из наиболее распространенных схем является последовательность операций, начинающаяся с внесения на банковские счета или вклады наличных денежных средств в объемах, не превышающих установленный порог обязательного контроля, с последующим снятием внесенных средств в форме высоколиквидной наличности. Данная техника, известная

как «слоение» (structuring, smurfing), позволяет обходить автоматизированные системы контроля, создавая видимость фрагментированных низкорисковых транзакций [16].

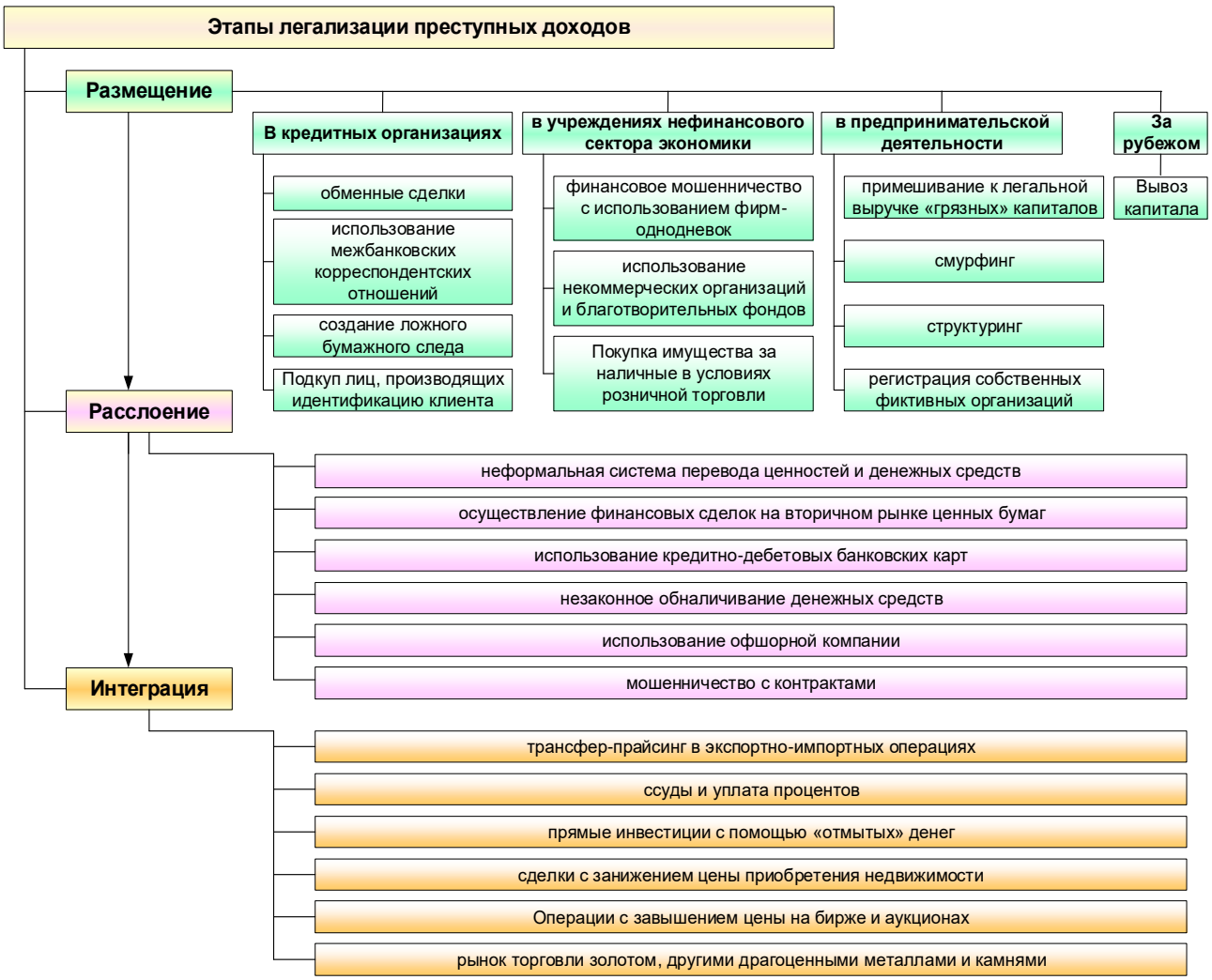

Рисунок 3 – Трехфазная модель отмывания преступных доходов

Технологии обналичивания денежных средств многообразны. Первый вариант заключается в переводе денежных средств на счета специализированных фирм, которые затем снимают наличные; риски таких операций распределяются между участниками. По другой технологии используются каскадные переводы между физическими лицами: перевод осуществляется от одного субъекта к другому несколько раз, и последний субъект цепочки снимает наличные денежные средства. В этом случае сложно проследить всю цепочку и установить источник происхождения транзакций. Еще более сложной для мониторинга является технология, при которой используются корпоративные структуры, имитирующие банковские трансферы по организации бизнес-проектов с последующим обналичиванием значительных сумм.

Многообразие таких технологий означает, что проблема носит системный характер, а выявление противоправных действий требует квалифицированной аналитической деятельности, опирающейся на несколько взаимодополняющих критериев.

Первый критерий – установление соответствия между заявленными в уставных документах кодами Общероссийского классификатора видов экономической деятельности (ОКВЭД) и фактическим содержанием транзакций. Для верификации правомерности операций проводится

сопоставление финансовой документации: договоров, актов выполненных работ, платежных поручений, счетов на оплату, счетов-фактур, товарно-транспортных накладных и иных первичных учетных документов. Только такое сопоставление позволяет обосновать экономическую целесообразность каждого перечисления.

Второй критерий основывается на обосновании экономической необходимости именно наличной формы расчетов. Клиент должен документально подтвердить, почему снятие наличных существенно для его операционной деятельности, с учетом специфики рынка, сезонных факторов или обстоятельств непреодолимой силы. Без такого обоснования операции квалифицируются как высокорисковые.

Третий критерий заключается в макроэкономической оценке сегментации целевого рынка клиента. Необходимо сформировать картину цепочки создания ценности, включая поставщиков, дистрибьюторов и конечных потребителей, а также показатели конкурентоспособности предприятия – долю рынка, рентабельность, динамику выручки.

Четвертый критерий – анализ документов: налоговых деклараций по налогу на добавленную стоимость, налогу на прибыль и налогу на доходы физических лиц; платежных поручений на перечисление налоговых платежей и страховых взносов; документов о выплате заработной платы. Анализ такого пакета документов позволяет с высокой вероятностью подтвердить или опровергнуть легитимность деятельности клиента.

Обобщение нормативных признаков, указывающих на необычный характер сделки[3], а также материалов отчетов ФАТФ и Росфинмониторинга позволяет выделить девять устойчивых типологий схем легализации преступных доходов (Таблица 3).

Таблица 3 – Типология схем легализации преступных доходов и их наблюдаемые признаки

№	Типология	Механизм	Фаза	Наблюдаемые признаки в данных	Применимый метод ИИ
1	Структурирование (дробление)	Разбиение суммы на операции ниже порога обязательного контроля	Размещение	Серии однотипных зачислений или переводов, в совокупности превышающих порог; устойчивая периодичность; суммы, тяготеющие к границе порога	Анализ временных рядов; признаки скорости операций; кумулятивная агрегация в скользящем окне
2	Транзитные операции юридических лиц	Кратковременное прохождение средств через счет без экономического содержания	Расслоение	Нулевые или незначительные остатки при значительных оборотах; совпадение сумм входящих и исходящих платежей; малый интервал между зачислением и списанием	Графовый анализ (транзитные узлы, центральность); правила соотношения оборота и остатка
3	Обналичивание через физических лиц	Веерное распределение средств на счета физических лиц с	Размещение, расслоение	Множественные переводы одному отправителю разным получателям; снятие наличных в тот же	Выявление сообществ в графе; кластеризация по поведенческим векторам

[3] См. Приложение к Положению Банка России от 18 июня 2025 года N 860-П "О требованиях к правилам внутреннего контроля кредитной организации, филиала иностранного банка, через который иностранный банк осуществляет деятельность на территории Российской Федерации, в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и экстремистской деятельности"

№	Типология	Механизм	Фаза	Наблюдаемые признаки в данных	Применимый метод ИИ
		последующим снятием		операционный день; совпадение подразделения обслуживания; прекращение операций после цикла	
4	Фиктивная хозяйственная деятельность	Имитация оборота, не соответствующего заявленному виду деятельности	Расслоение	Расхождение назначений платежей с кодами ОКВЭД; отсутствие сопутствующих платежей (заработная плата, налоги, взносы, аренда); широкий спектр несвязанных товарных позиций	Классификация назначений платежа (NLP); сопоставление с реестрами; выявление отсутствующих признаков
5	Использование номинальных структур	Создание юридических лиц под ограниченный цикл операций	Расслоение	Малый срок с даты регистрации до начала операций; совпадение адресов, учредителей, бенефициаров, контактных данных; резкое прекращение деятельности	Связывание сущностей; графовый анализ по общим атрибутам
6	Трансграничные схемы	Вывод средств под видом внешнеторговых или инвестиционных расчетов	Расслоение, интеграция	Расчеты с контрагентами в юрисдикциях повышенного риска; несоответствие условий контракта рыночным; авансовые платежи без последующей поставки; возврат средств в виде инвестиций	Анализ атрибутов контрагента; выявление циклов в графе расчетов
7	Операции с ценными бумагами и векселями	Придание правомерного вида через инструменты фондового рынка	Расслоение, интеграция	Приобретение ценных бумаг на предъявителя сразу после поступления средств; расчеты по индоссаменту с последующим обналичиванием; внесение наличных в кассу профессионального участника	Выявление последовательностей операций; сопоставление с профилем клиента
8	Схемы в отраслях с высоким наличным оборотом	Смешение преступных доходов с легальной наличной выручкой	Размещение	Доля наличной выручки, не соответствующая отраслевым и сезонным ориентирам; резкий рост инкассации без изменения масштаба деятельности	Обнаружение аномалий относительно отраслевой группы; сегментация

№	Типология	Механизм	Фаза	Наблюдаемые признаки в данных	Применимый метод ИИ
9	Синтетические и похищенные идентификационные данные	Открытие счетов по комбинированным или чужим персональным данным	Размещение	Частичные совпадения идентификационных атрибутов между клиентами; несоответствие поведения заявленному профилю; аномалии на этапе идентификации	Связывание сущностей; нечеткое сопоставление; графовый анализ пересечений атрибутов

Развернутый перечень признаков, указывающих на необычный характер сделки, приведен в приложении к соответствующему положению Банка России и в настоящей работе не воспроизводится.

Приведенные типологии не являются взаимоисключающими. Реальные схемы, как правило, комбинируют несколько из них, что и обусловливает преимущество графовых методов [17]. Наличие признака не является доказательством противоправности и служит основанием для дополнительной проверки. В случае выявления подозрительной деятельности обслуживающая кредитная организация вправе истребовать документы, подтверждающие заявленную функциональную деятельность клиента.

Типология мошеннических атак и их признаки

Второй класс задач связан с противодействием хищениям денежных средств, совершаемым третьими лицами. Признаки осуществления перевода денежных средств без добровольного согласия клиента установлены нормативно [18] и дополняются типологиями, сложившимися в практике противодействия мошенничеству (Таблица 4).

Таблица 4 – Типология мошеннических атак и их наблюдаемые признаки

№	Типология	Механизм	Наблюдаемые признаки в данных	Применимый метод ИИ
1	Социальная инженерия	Клиент под воздействием обмана самостоятельно совершает перевод	Нехарактерные для клиента получатель и сумма при штатной аутентификации; аномальный темп взаимодействия с интерфейсом; длительная пауза перед подтверждением	Поведенческая биометрия; модели последовательностей действий в сессии
2	Компрометация учетной записи	Получение доступа к дистанционному обслуживанию помимо воли клиента	Вход с нового устройства или из нетипичной геолокации; смена контактных данных непосредственно перед операцией; несовпадение параметров устройства с историческим профилем	Идентификация устройства; обнаружение аномалий относительно индивидуального профиля
3	Компрометация платежной карты	Использование реквизитов без физического носителя	Серии операций малых сумм в разных торговых точках; несоответствие страны операции и страны эмитента; высокая частота авторизаций	Обучение с учителем на подтвержденных случаях; признаки скорости операций
4	Вредоносное программное обеспечение и	Управление устройством клиента третьим лицом	Признаки удаленного управления в характеристиках сессии; аномалии ввода,	Классификация характеристик сессии; эвристический анализ во

№	Типология	Механизм	Наблюдаемые признаки в данных	Применимый метод ИИ
	средства удаленного доступа		несовместимые с ручным взаимодействием; расхождение параметров среды исполнения	взаимодействии со средствами защиты конечных устройств
5	Компрометация канала подтверждения	Перехват средств подтверждения операции	Замена абонентского устройства незадолго до операции; несовпадение канала подтверждения с историческим; операции сразу после изменения реквизитов доступа	Анализ последовательности событий; правила временной близости изменений и операций
6	Мошенничество при оформлении продукта	Получение банковского продукта по чужим или комбинированным данным	Частичные совпадения идентификационных атрибутов между заявителями; несоответствие заявленных сведений внешним источникам; аномалии заполнения заявки	Связывание сущностей; нечеткое сопоставление; графовый анализ пересечений атрибутов
7	Инфраструктура вывода похищенных средств	Использование счетов подставных лиц для приема и обналичивания	Прием средств от множества несвязанных отправителей; снятие наличных в тот же операционный день; краткий жизненный цикл счета	Выявление сообществ в графе; кластеризация по поведенческим векторам

Типология 7 совпадает по наблюдаемым признакам и методам с типологией 3 Таблицы 3. Это совпадение не случайно, т.к. похищенные средства и преступные доходы выводятся через одну и ту же инфраструктуру подставных счетов, что обосновывает целесообразность объединения методов противодействия.

Достоверные сведения о клиенте в сочетании с набором поведенческих параметров обычно укладываются в типичные шаблоны для добросовестных клиентов. Это служит основой работы современных антифрод-систем, они опираются на эталонные паттерны поведения при принятии решений. В систему включается широкий спектр факторов – от частоты авторизаций и способа ввода данных до географической истории и параметров устройства. На их основе в реальном времени рассчитывается оценка риска.

Классическими примерами аномалий являются следующие:

- внезапная трата нехарактерной суммы клиентом, обычно совершающим операции существенно меньшего масштаба, без предшествующих индикаторов;
- серия платежей с одного счета разным получателям с идентичными суммами, часто маскирующая проверку похищенных реквизитов; резкое изменение географии операций за интервал, исключающий физическое перемещение;
- краткие сессии без прохождения дополнительной аутентификации.

Методы машинного обучения и технологии ИИ при решении задач противодействия финансовых преступлений

Современные системы противодействия финансовым преступлениям используют широкий набор методов машинного обучения и технологий ИИ, причем каждая нацелена на решение конкретных задач выявления угроз.

Текстовая аналитика опирается на алгоритмы поиска по ключевым словам, контекстной категоризации и извлечения именованных сущностей (NER). Эти инструменты позволяют анализировать текстовые поля транзакций, назначения платежей и описания операций [19].

В задачах ПОД/ФТ текстовая аналитика применяется прежде всего для сопоставления назначения платежа с заявленными кодами ОКВЭД – операции, которая при ручном исполнении требует значительных трудозатрат.

Анализ разрывов (gap-анализ) направлен на поиск пропусков в последовательности операций. Отсутствие в цепочке ожидаемого шага, например, платежей, сопутствующих реальной хозяйственной деятельности, воспринимается как сигнал повышенного риска [20]. Существенно, что здесь диагностическим является не наличие признака, а его отсутствие, что делает метод плохо заменимым правилами.

Расчет статистических показателей (средних, дисперсий, стандартизованных отклонений) выступает базовым инструментом обнаружения отклонений в поведении клиента. Резкий рост сумм или частоты операций рассматривается как сигнал возможной компрометации счета либо изменения характера деятельности.

Анализ временных рядов с использованием рекуррентных архитектур (в частности, моделей типа LSTM) позволяет выявлять закономерности в поведении переводов: повторяющиеся циклы платежей между счетами, внезапные всплески объемов, периодичность, характерную для структурирования. Именно этот класс методов наиболее применим к типологии 1 Таблицы 3, где признак проявляется только в совокупности операций.

Сетевая (графовая) аналитика моделирует связи между счетами, устройствами и адресами. Применяются алгоритмы выявления сообществ, оценки центральности узлов, а также графовые нейронные сети. Этот подход позволяет выявлять группы связанных участников и аномальные кластеры, включая сети подставных счетов. Для задач ПОД/ФТ графовая аналитика имеет ключевое значение: отмывание по своей природе является свойством сети операций, а не отдельной транзакции [21]. Метод раскрывает схемы с участием номинальных структур с общими бенефициарами и прослеживает путь средств от первичного счета через цепочку переводов к финальному обналичиванию.

Обучение с учителем строится на исторических данных, где случаи противоправных операций заранее размечены. Такие модели эффективно распознают повторяющиеся шаблоны. Например, серии микроплатежей, используемые для проверки похищенных реквизитов, или многократные попытки авторизации с одинаковыми параметрами. Как было отмечено выше, условия для применения этого класса методов существенно благоприятнее в антифрод-системе.

Обучение без учителя работает с неразмеченными данными и выявляет структуры и аномалии самостоятельно. Методы кластеризации (k-means, DBSCAN, HDBSCAN) и автокодировщики помогают обнаруживать необычные группы транзакций и сигнатуры, не встречавшиеся ранее [22]. Сегментация клиентов по поведенческим векторам позволяет выявлять выбросы. Например, субъект малого предпринимательства с оборотами, характерными для крупной организации. Обнаружение редких событий строится на моделях одноклассовой классификации.

Обогащение данных представляет собой автоматическую агрегацию разнородных источников: истории операций клиента, идентификационных сведений, географических данных и внешних информационных ресурсов [23]. Формируемый таким образом консолидированный профиль повышает полноту исходных данных для последующего анализа.

Скоринг предупреждений реализуется через байесовские алгоритмы, проводящие сравнительное ранжирование объектов мониторинга по вероятности противоправного характера операции, что позволяет приоритизировать поток срабатываний для аналитика [24, 25].

Оценка клиентских рисков опирается, в том числе, на логистическую регрессию, эмпирически рассчитывающую вероятность отнесения клиента к группе повышенного риска [26]:

$$P(y = 1 \mid X) = \frac{1}{\left(1+e^{-(b_0+b_1X_1+\cdots)}\right)},$$

где X – вектор признаков (частота снятия наличных, соответствие операций кодам ОКВЭД, параметры оборота), $b_0 \ldots b_n$ – оцениваемые коэффициенты, y – бинарная переменная отнесения к группе риска.

Автоматизированная разработка сценариев использует деревья решений и их ансамбли (Random Forest, градиентный бустинг) для генерации логики обнаружения по правилам вида «если доля снятия наличных превышает установленное значение оборота при отсутствии сопутствующих платежей, то операция направляется на проверку» [27, 28]. Преимущество ансамблевых методов заключается в способности выявлять взаимодействия признаков, не заданные аналитиком явно.

Распознавание образов задействует сверточные архитектуры в сочетании с оптическим распознаванием символов для классификации товарно-сопроводительных документов: извлечения данных из счетов-фактур и накладных, проверки их комплектности и непротиворечивости [29].

Сопоставление наблюдаемых признаков, методов и присущих им ограничений приведено в Таблице 5.

Таблица 5 – Соотношение признаков, методов ИИ и их ограничений

Признак в данных	Класс задачи	Метод	Основание применимости	Ограничение
Дробление сумм под порог обязательного контроля	AML	Анализ временных рядов; признаки скорости операций	Улавливает периодичность и кумулятивный эффект, невидимые в отдельной операции	Схема адаптируется под известное окно агрегации
Транзитный характер операций	AML	Графовый анализ, оценка центральности	Транзит проявляется в структуре связей, а не в атрибутах платежа	Ограничен периметром одной кредитной организации
Цепочки переводов через подставные счета	AML	Выявление сообществ, графовые нейронные сети	Отмывание – свойство сети, а не транзакции	Требует данных нескольких организаций
Расхождение операций с кодами ОКВЭД	AML	Классификация назначений платежа (NLP)	Автоматизирует ручную аналитическую процедуру	Назначение платежа заполняется произвольно, высок уровень шума
Отсутствие сопутствующих платежей	AML	Gap-анализ	Диагностическим является отсутствие признака	Возможны законные причины отсутствия
Несоответствие оборота отраслевому профилю	AML	Сегментация, обнаружение выбросов	Не требует разметки	Гетерогенность отраслевых групп снижает точность
Синтетические идентификационные данные	Оба класса	Связывание сущностей, нечеткое сопоставление	Фрагменты данных пересекаются между профилями	Ложные совпадения у родственников и однофамильцев
Отклонение от индивидуального поведенческого профиля	Антифрод	Кластеризация, обнаружение аномалий	Не требует разметки, выявляет ранее не встречавшееся	Естественный дрейф поведения клиента
Признаки перевода под влиянием социальной инженерии	Антифрод	Поведенческая биометрия, модели сессии	Атака оставляет след в способе взаимодействия, а не в реквизитах	Наиболее чувствительно к ошибкам первого рода

Признак в данных	Класс задачи	Метод	Основание применимости	Ограничение
Несоответствие устройства и геолокации	Антифрод	Признаки устройства и геолокации в скоринговых моделях	Быстрый сигнал в реальном времени	Обходится техническими средствами
Серии операций малых сумм	Антифрод	Обучение с учителем, признаки скорости	Разметка доступна и своевременна	Требует регулярного переобучения
Аномалии на этапе оформления продукта	Антифрод	Классификация, графовый анализ атрибутов	Признаки доступны до совершения операции	Ограниченность внешних источников верификации

Графовая аналитика применительно к выявлению связанных сетей подставных счетов иллюстрируется на Рисунке 4.

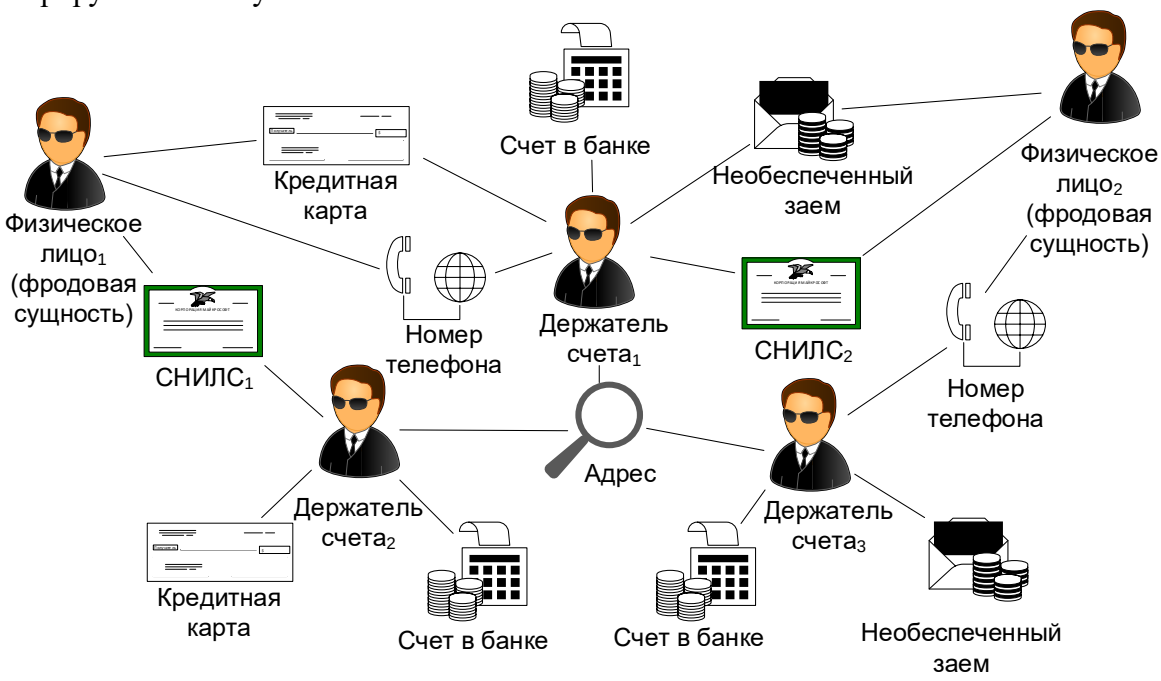

Рисунок 4 – Графовая аналитика выявления преступных транзакций (сети с синтетическими учетными записями)

Архитектура интегрированной системы мониторинга финансовых операций

Рассмотренные технологии предлагается реализовывать в рамках единого контура, функционирующего в непрерывном режиме без четко выраженных начальной и конечной фаз (Рисунок 5).

Алгоритм процесса мониторинга включает следующие этапы: выявление и анализ всех входящих транзакций для сбора данных; идентификация подозрительных операций и паттернов риска; принятие решения о приостановлении операции либо направлении ее на дополнительную проверку; последующее машинное обучение на полученной информации с расширением базы данных в целях повышения точности при последующих проверках. Цикл работы системы представлен на Рисунке 6.

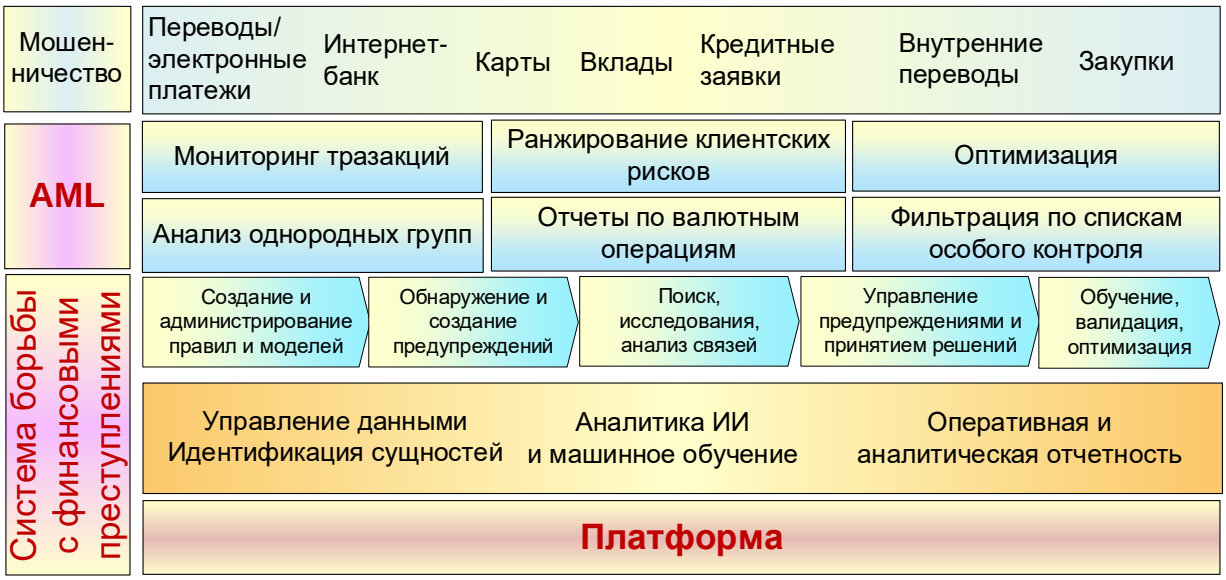

Рисунок 5 – Принцип работы системы мониторинга финансовых операций

Рисунок 6 – Цикл работы системы противодействия финансовым преступлениям

Анализ проводится по следующим критериям: контроль суммы платежа на предмет превышения установленного лимита; проверка адресов плательщика и получателя с учетом появления ранее не встречавшихся связей; распознавание новых моделей клиентского поведения; нестандартно быстрый вывод средств после зачисления; получение массовых платежей на счета физических лиц без надлежащего оформления; запутанные операции, лишенные очевидного экономического смысла.

Операции классифицируются по уровням риска и визуализируются в цветах светофора [30]: зеленый означает низкую вероятность противоправного характера операции; желтый свидетельствует об уровне риска выше среднего и требует дополнительной проверки; красный указывает на высокую вероятность и требует документального подтверждения.

Совместное использование аналитических систем и технологий обработки больших данных реализует принцип «знай своего клиента» (KYC – Know Your Customer). Система позволяет анализировать операции, выявляя подозрительные отклонения и фиксируя рискованные операции [31]. Основные функции данного контура включают в себя: выявление подозрительных транзакций; валидация, позволяющая автоматизировать процесс обновления моделей машинного обучения; сигнализация о необходимости ручной проверки и расследования с участием человека в сложных случаях, в частности при расследовании цепочек с участием международных преступных организаций (Рисунок 7).

Рисунок 7 – Процессы AML-систем (ПОД/ФТ), в которых используются технологии ИИ

Ключевым свойством такой архитектуры является взаимный обмен признаками между данными системами (контурами): сведения о компрометации счетов и о счетах подставных лиц, формируемые в антифрод-системе, поступают в контур AML-систем (ПОД/ФТ) как входные признаки, а выявленные в ходе финансовых расследований сети пополняют перечни повышенного риска, применяемые при операционном контроле. Ни одно узкоспециализированное решение не способно самостоятельно обеспечить выполнение требований законодательства в полном объеме, что обусловливает необходимость системного подхода.

Ограничения и риски применения ИИ

Оценка возможностей ИИ была бы неполной без анализа ограничений, часть которых носит принципиальный характер и не преодолевается наращиванием вычислительных мощностей или объема данных.

Дефицит и запаздывание разметки. Достоверное подтверждение факта легализации отделено от операции значительным временным интервалом, а доля подтвержденных случаев сравнительно мала. Это ограничивает применимость обучения с учителем и означает, что заявляемые в литературе показатели качества классификации нередко получены на выборках, где в качестве целевой переменной используется не приговор, а факт направления сообщения в уполномоченный орган. Такая подмена может систематически завышать оценки результативности.

Границы наблюдаемости данных. Схемы легализации по своей природе распределены между несколькими кредитными организациями, тогда как каждая из них наблюдает лишь принадлежащий ей фрагмент графа расчетов. Возможности графового анализа тем самым ограничены границей одной организации. Расширение границы упирается в требования законодательства о персональных данных и о банковской тайне. Технологии распределенного обучения, при которых модели обмениваются параметрами без передачи исходных данных, снимают проблему лишь частично, т.к. они позволяют согласовать модели, но не восстанавливают связность графа.

Объяснимость и правовые последствия решения. Решение, принятое на основании модели, влечет для клиента ограничение распоряжения средствами, а при систематическом характере существенные затруднения в доступе к банковскому обслуживанию. При этом наиболее результативные методы (ансамблевые и графовые нейросетевые модели) не обеспечивают интерпретируемого обоснования [32]. Возникает противоречие между точностью и возможностью мотивировать решение перед клиентом, надзорным органом и судом.

Цена ошибки первого рода. Ложное срабатывание в антифрод-системе оборачивается неудобством и повторной аутентификацией. В контуре AML-систем (ПОД/ФТ) последствия для добросовестного клиента, прежде всего для субъекта малого предпринимательства, несоизмеримо тяжелее. Снижение доли ложных срабатываний имеет здесь не только экономическое, но и социальное измерение, а оценка модели исключительно по показателям полноты обнаружения методически некорректна без одновременного указания уровня ошибок первого рода.

Адаптация схем к средствам контроля. Противодействие финансовым преступлениям представляет собой антагонистическую среду. Параметры контроля, ставшие известными, немедленно учитываются при построении схем. Пороговые значения, окна агрегации и правила выявления дробления перестают работать вскоре после того, как становятся предсказуемыми. Устойчивость модели во времени является самостоятельным критерием ее качества, а необходимость периодического переобучения – конструктивным требованием, а не эксплуатационным неудобством.

Дрейф данных. Изменение платежного поведения под влиянием регуляторных, технологических и внешнеэкономических факторов приводит к деградации моделей, обученных на предшествующих периодах, что требует организации постоянного контроля их качества в промышленной эксплуатации.

Отдельную группу образуют ограничения, специфичные для антифрод-систем.

Легитимность операции при социальной инженерии. В случаях, когда клиент под воздействием обмана самостоятельно инициирует перевод, операция технически безупречна. Как правило, она совершается с доверенного устройства, из привычной геолокации, с корректным прохождением аутентификации. Признаки компрометации отсутствуют, поскольку компрометации не было, т.к. воздействие было оказано на волю клиента, а не на канал. Модель вынуждена опираться на косвенные поведенческие индикаторы, надежность которых существенно ниже. Это ограничение носит принципиальный характер и не устраняется совершенствованием алгоритмов идентификации.

Адаптация к средствам биометрической верификации. Развитие средств синтеза изображения и голоса снижает надежность соответствующих модальностей быстрее, чем совершенствуются методы их проверки. Устойчивость обеспечивается не отдельной модальностью, а их сочетанием и совместным использованием с поведенческими признаками, что удорожает решение и увеличивает время отклика.

Риск автоматизационной предвзятости. По мере роста доверия к автоматизированным оценкам снижается критичность их проверки аналитиком, что при систематической ошибке модели ведет к воспроизводству этой ошибки в масштабе всей организации. Сохранение содержательного участия человека в принятии итогового решения остается необходимым элементом интегрированной системы мониторинга финансовых операций.

Заключение

Проведенное исследование позволяет сформулировать следующие выводы.

Противодействие легализации преступных доходов и противодействие мошенничеству, несмотря на общность используемых данных и технологической базы, образуют два различных класса задач. Они различаются защищаемым интересом, источником угрозы, горизонтом анализа, правовой основой и ценой ошибки первого рода. Ключевым для выбора методов является различие в доступности размеченных данных. В антифрод-системе подтверждение

противоправного характера операции поступает в течение дней, в задачах AML-систем (ПОД/ФТ) с задержкой в несколько лет. Отсюда следует методическое разграничение: в антифрод-системе эффективно обучение с учителем, в AML-системе (ПОД/ФТ) приоритет принадлежит обучению без учителя и графовому анализу. Смешение этих классов, распространенное в отраслевой литературе, приводит к некорректному переносу решений и завышенным ожиданиям от их результативности.

Систематизация типологий обоих классов и их сопоставление с наблюдаемыми признаками в транзакционных данных позволяют перейти от перечисления технологий к обоснованному выбору метода под конкретный признак. Предложенные в работе Таблицы 3–5 реализуют такое сопоставление и могут использоваться при проектировании систем.

Оба процесса целесообразно рассматривать как связанную систему. Инфраструктура подставных счетов, обслуживающая вывод похищенных средств, совпадает с нижним уровнем схем обналичивания преступных доходов, что делает обмен признаками между контурами источником дополнительной аналитической ценности.

Возможности ИИ в рассматриваемой области существенно ограничены. Дефицит и запаздывание разметки, ограниченность наблюдаемого фрагмента графа расчетов периметром одной организации, проблема объяснимости решений, влекущих правовые последствия для клиента, и адаптация схем к ставшим известными параметрам контроля представляют собой принципиальные, а не технические препятствия. Это определяет роль ИИ как инструмента приоритизации и сокращения пространства поиска для аналитика, а не автономного субъекта принятия решений.

Направлениями дальнейших исследований представляются: разработка методов оценки качества моделей AML-систем (ПОД/ФТ) в условиях запаздывающей и неполной разметки; исследование правовых и организационных механизмов межбанковского обмена признаками, совместимых с требованиями законодательства о персональных данных и банковской тайне.

Список литературы

1. Стратегия национальной безопасности Российской Федерации: Указ Президента Российской Федерации от 02.07.2021 № 400. URL: http://www.kremlin.ru/acts/bank/47046.

2. Стратегия экономической безопасности Российской Федерации на период до 2030 года: Указ Президента Российской Федерации от 13.05.2017 № 208. URL: https://base.garant.ru/71672608/.

3. *Матвеев В.В.* Процесс трансформации системы глобального управления. Роль России в создании нового мирового порядка // Национальная безопасность и стратегическое планирование. – 2024. – № 3(47). – С. 25–54. – DOI 10.37468/2307-1400-2024-3-25-54.

4. ЦБ России: количество переводов, совершаемое в России каждую секунду. URL: https://1prime.ru/20230217/839836188.html.

5. Объем транзакций по картам в России стремится к рекордным значениям. URL: https://www.penza.kp.ru/online/news/5460668/.

6. *Антонов А.Е., Матвеев В.В.* Обеспечение экономической безопасности с использованием DLP-системы (искусственного интеллекта) // Теоретические и прикладные вопросы комплексной безопасности: Материалы V Международной научно-практической конференции, Санкт-Петербург, 23 марта 2022 года. – Санкт-Петербург, 2022. – С. 251–257.

7. *Маслов Д.М., Матвеев В.В.* Отток капитала из России в современный период: причины и последствия // Современные вызовы экономики и систем управления в России в условиях многополярного мира: Сборник статей V Международной научно-практической конференции, Санкт-Петербург, 24–25 апреля 2024 года. – Санкт-Петербург: Скифия-принт, 2025. – С. 130–142.

8. Отток замедлился: как население продолжает выводить деньги из России. URL: https://www.forbes.ru/investicii/508062-ottok-zamedlilsa-kak-naselenie-prodolzaet-vyvodit-den-gi-iz-rossii.

9. *Гаджиахмедова Э.М., Ячменева Г.Е., Матвеев В.В.* Обеспечение экономической безопасности России в условиях глобализации и фритредерства // Национальная безопасность и стратегическое планирование. – 2019. – № 4(28). – С. 56–69.

10. *Зайцев А.К., Матвеев В.В.* Экономические преступления с использованием цифровых технологий // Национальная безопасность и стратегическое планирование. – 2022. – № 1(37). – С. 63–81. – DOI 10.37468/2307-1400-2022-1-63-81.

11. Комплексный анализ состояния преступности в Российской Федерации по итогам 2024 года и ожидаемые тенденции ее развития : аналитический обзор / М. В. Гончарова, М. М. Бабаев, С. А. Невский, Р. В. Черкасов, Г. Ф. Коимшиди, Г. Э. Бицадзе, К. С. Насуев, Е. М. Тимошина, Н. А. Ведешкин. – Москва: ВНИИ МВД России, 2025. – 87 с.

12. *Chen Z. et al.* Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: a review //Knowledge and Information Systems. – 2018. – V. 57. – №. 2. – P. 245-285. – DOI https://doi.org/10.1007/s10115-017-1144-z

13. *Li F., Chen Z.* Dynamic quantification anti-fraud machine learning model for real-time transaction fraud detection in banking // Discover Computing. – 2025. – V. 28. – №. 1. – P. 59. – DOI https://doi.org/10.1007/s10791-025-09549-7

14. О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия хищению денежных средств: Федеральный закон от 27.06.2018 № 167-ФЗ. URL: https://www.zakonrf.info/doc-35332077/

15. *Zita K.L.N. et al.* Anti-Fraud and Anti-Money Laundering: Proactive Detection Using Artificial Neural Networks with the Fraud Hexagon Approach to Strengthen the Stability of Indonesia's Financial Ecosystem //Indonesian Economic Review. – 2026. – V. 6. – №. 1. – P. 260-269. – DOI https://doi.org/10.53787/iconev.v6i1.105

16. *Calafos M. W., Dimitoglou G*. Cyber laundering: Money laundering from fiat money to cryptocurrency // Principles and Practice of Blockchains. – Cham: Springer International Publishing, 2022. – P. 271-300. – DOI https://doi.org/10.1007/978-3-031-10507-4_12

17. *Cheng D. et al.* Anti-money laundering by group-aware deep graph learning // IEEE Transactions on Knowledge and Data Engineering. – 2023. – V. 35. – №. 12. – P. 12444-12457. – DOI https://doi.org/10.1109/TKDE.2023.3272396

18. Обзор систем противодействия банковскому мошенничеству (антифрод). URL: https://www.anti-malware.ru/analytics/Market_Analysis/anti-fraud-Bank-systems.

19. *Das S. R.* Text and context: Language analytics in finance //Foundations and Trends® in Finance. – 2014. – V. 8. – №. 3. – P. 145-261. – DOI https://doi.org/10.1561/0500000045

20. *Divya D. et al.* Bridging financial and operational gaps in supply chain finance: An information processing theory perspective //Journal of Risk and Financial Management. – 2025. – V. 18. – №. 9. – P. 479. – DOI https://doi.org/10.3390/jrfm18090479

21. *Pocher N. et al.* Detecting anomalous cryptocurrency transactions: An AML/CFT application of machine learning-based forensics // Electronic Markets. – 2023. – V. 33. – №. 1. – P. 37. – DOI https://doi.org/10.1007/s12525-023-00654-3

22. *Cholevas C. et al*. Anomaly detection in blockchain networks using unsupervised learning: A survey // Algorithms. – 2024. – V. 17. – №. 5. – P. 201. – DOI https://doi.org/10.3390/a17050201

23. *Kunadi S.K.* AI-Driven Data Enrichment and Golden Record Creation for Enterprise Customer Data Platforms // International Journal of Research and Applied Innovations. – 2026. – V. 9. – №. 1. – P. 13630-13640. – DOI https://doi.org/10.15662/IJRAI.2026.0901016

24. *Khan N. S. et al.* A Bayesian approach for suspicious financial activity reporting //International Journal of Computers and Applications. – 2013. – V. 35. – №. 4. – P. 181-187.

25. *Zuo Z. et al.* A Bayesian-Optimized XGBoost Approach for Money Laundering Risk Prediction in Financial Transactions //Information. – 2026. – V. 17. – №. 4. – P. 324. – DOI https://doi.org/10.3390/info17040324

26. *Сорокин А.С.* Построение скоринговых карт с использованием модели логистической регрессии // Вестник евразийской науки. – 2014. – №. 2 (21). – С. 82.

27. *Vassallo D., Vella V., Ellul J.* Application of gradient boosting algorithms for anti-money laundering in cryptocurrencies // SN Computer Science. – 2021. – V. 2. – №. 3. – P. 143. – DOI https://doi.org/10.1007/s42979-021-00558-z

28. *Pratama S.F., Wahid A.M.* Fraudulent transaction detection in online systems using random forest and gradient boosting //Journal of Cyber Law. – 2025. – V. 1. – №. 1. – P. 88-115. – DOI https://doi.org/10.63913/jcl.v1i1.16

29. *Yu C. H. et al.* Machine Learning-Enhanced Automation for Invoice Reconciliation: OCR-Based Solutions for Accuracy and Efficiency in Logistics Industry //Intelligent Systems Conference. – Cham: Springer Nature Switzerland, 2024. – P. 325-336. – DOI https://doi.org/10.1007/978-3-031-66336-9_23

30. *Berndsen R., Heijmans R.* Risk indicators for financial market infrastructure: from high frequency transaction data to a traffic light signal // De Nederlandsche Bank Working Paper. – No. 557. – URL: https://ssrn.com/abstract=2985412

31. *Islam S.* Machine Learning–Based AML/KYC Transaction Monitoring for Suspicious Activity Detection and Compliance Risk Reduction in Digital Banking // ASRC Procedia: Global Perspectives in Science and Scholarship. – 2025. – V. 1. – №. 01. – P. 1740-1775. – DOI https://doi.org/10.63125/r9c8q813

32. *Матвеев А.В.* Сравнительный анализ методов интерпретируемости моделей искусственного интеллекта в процессах принятия решений // Современные наукоемкие технологии. – 2026. – № 5. – С. 131-138. – DOI 10.17513/snt.40785.

Статья поступила в редакцию 24 февраля 2026 г.
Принята к публикации 17 марта 2026 г.

Ссылка для цитирования: Леонов В. А., Зайцев А. К., Матвеев В. В. Технологии искусственного интеллекта в противодействии финансовым преступлениям: возможности и ограничения // Национальная безопасность и стратегическое планирование. 2026. № 1(53). С. 57-77. DOI: https://doi.org/10.37468/2307-1400-2026-1-57-77

Artificial intelligence technologies in countering financial crime: opportunities and limitations

***Leonov Viacheslav A.*[1]**
***Zaytsev Alexander K.*[2]**
***Matveev Vladimir V.*[1]**

[1] *Financial University under the Government of the Russian Federation (St. Petersburg branch), St. Petersburg, Russia*

[2] *Interregional Office of the Federal Service for Financial Monitoring for the Northwestern Federal District, St. Petersburg, Russia*

Abstract

The paper examines the application of artificial intelligence technologies to countering financial crime as a factor of the financial security of the Russian Federation. It is shown that anti-money laundering (AML) and anti-fraud constitute two distinct classes of tasks differing in the protected interest, the analytical horizon, the legal framework and the availability of labelled data. Drawing on regulatory indicators and typological studies, the paper proposes consolidated typologies of laundering schemes and fraud attacks, each mapped to observable features in transaction data and to applicable machine learning methods. It is argued that AML tasks favour unsupervised learning and graph analysis, whereas anti-fraud tasks favour supervised learning. The limitations of artificial intelligence are systematised: scarcity and latency of labels, the boundaries of data observability within a single credit institution, the explainability of decisions, the cost of false positives, and the adaptation of schemes to control mechanisms. The paper concludes that artificial intelligence serves as a tool for prioritisation and search-space reduction rather than an autonomous decision-making agent.

Keywords: financial security, artificial intelligence, machine learning, money laundering, AML, anti-fraud, graph analytics, financial monitoring, transaction analysis.

References

1. National Security Strategy of the Russian Federation: Decree of the President of the Russian Federation of July 2, 2021, No. 400. Available at: http://www.kremlin.ru/acts/bank/47046.

2. Economic Security Strategy of the Russian Federation through 2030: Decree of the President of the Russian Federation of May 13, 2017, No. 208. Available at: https://base.garant.ru/71672608/.

3. *Matveev V.V.* The Process of Transformation of the Global Governance System. Russia's Role in Creating a New World Order // National Security and Strategic Planning. - 2024. - No. 3 (47). - pp. 25–54. - DOI 10.37468/2307-1400-2024-3-25-54.

4. The Central Bank of Russia: The number of transfers made in Russia every second. URL: https://1prime.ru/20230217/839836188.html.

5. The volume of card transactions in Russia is approaching record levels. URL: https://www.penza.kp.ru/online/news/5460668/.

6. *Antonov A.E., Matveev V.V.* Ensuring economic security using a DLP system (artificial intelligence) // Theoretical and Applied Issues of Integrated Security: Proceedings of the V International Scientific and Practical Conference, St. Petersburg, March 23, 2022. – St. Petersburg, 2022. – pp. 251–257.

7. *Maslov D.M., Matveev V.V.* Capital Outflow from Russia in the Modern Period: Causes and Consequences // Modern Challenges of the Economy and Management Systems in Russia in a Multipolar World: Collection of Articles from the V International Scientific and Practical Conference, St. Petersburg, April 24–25, 2024. – St. Petersburg: Skifia-print, 2025. – Pp. 130–142.

8. The Outflow Has Slowed Down: How the Population Continues to Take Money Out of Russia. URL: https://www.forbes.ru/investicii/508062-ottok-zamedlilsa-kak-naselenie-prodolzaet-vyvodit-den-gi-iz-rossii.

9. *Gadzhiakhmedova E.M., Yachmeneva G.E., Matveev V.V.* Ensuring Russia's Economic Security in the Context of Globalization and Free Trade // National Security and Strategic Planning. – 2019. – No. 4(28). – P. 56–69.

10. *Zaitsev A.K., Matveev V.V.* Economic crimes using digital technologies // National security and strategic planning. – 2022. – No. 1(37). – P. 63–81. – DOI 10.37468/2307-1400-2022-1-63-81.

11. Comprehensive analysis of the state of crime in the Russian Federation by the end of 2024 and expected trends in its development: an analytical review / M. V. Goncharova, M. M. Babaev, S. A. Nevsky, R. V. Cherkasov, G. F. Koimshidi, G. E. Bitsadze, K. S. Nasuev, E. M. Timoshina, N. A. Vedeshkin. - Moscow: VNII MVD of Russia, 2025. - 87 p.

12. *Chen Z. et al.* Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: a review //Knowledge and Information Systems. – 2018. – V. 57. – №. 2. – P. 245-285. – DOI https://doi.org/10.1007/s10115-017-1144-z

13. *Li F., Chen Z.* Dynamic quantification anti-fraud machine learning model for real-time transaction fraud detection in banking // Discover Computing. – 2025. – V. 28. – №. 1. – P. 59. – DOI https://doi.org/10.1007/s10791-025-09549-7

14. On Amendments to Certain Legislative Acts of the Russian Federation in Terms of Combating the Theft of Funds: Federal Law of June 27, 2018 No. 167-FZ. URL: https://www.zakonrf.info/doc-35332077/

15. *Zita K. L. N. et al.* Anti-Fraud and Anti-Money Laundering: Proactive Detection Using Artificial Neural Networks with the Fraud Hexagon Approach to Strengthen the Stability of Indonesia's Financial Ecosystem //Indonesian Economic Review. – 2026. – V. 6. – №. 1. – P. 260-269. – DOI https://doi.org/10.53787/iconev.v6i1.105

16. *Calafos M. W., Dimitoglou G.* Cyber laundering: Money laundering from fiat money to cryptocurrency // Principles and Practice of Blockchains. – Cham: Springer International Publishing, 2022. – P. 271-300. – DOI https://doi.org/10.1007/978-3-031-10507-4_12

17. *Cheng D. et al.* Anti-money laundering by group-aware deep graph learning // IEEE Transactions on Knowledge and Data Engineering. – 2023. – V. 35. – №. 12. – P. 12444-12457. – DOI https://doi.org/10.1109/TKDE.2023.3272396

18. Review of anti-fraud systems for banking (antifraud). URL: https://www.anti-malware.ru/analytics/Market_Analysis/anti-fraud-Bank-systems.

19. *Das S.R.* Text and context: Language analytics in finance //Foundations and Trends® in Finance. – 2014. – V. 8. – №. 3. – P. 145-261. – DOI https://doi.org/10.1561/0500000045

20. *Divya D. et al.* Bridging financial and operational gaps in supply chain finance: An information processing theory perspective //Journal of Risk and Financial Management. – 2025. – V. 18. – №. 9. – P. 479. – DOI https://doi.org/10.3390/jrfm18090479

21. *Pocher N. et al.* Detecting anomalous cryptocurrency transactions: An AML/CFT application of machine learning-based forensics // Electronic Markets. – 2023. – V. 33. – №. 1. – P. 37. – DOI https://doi.org/10.1007/s12525-023-00654-3

22. *Cholevas C. et al.* Anomaly detection in blockchain networks using unsupervised learning: A survey // Algorithms. – 2024. – V. 17. – №. 5. – P. 201. – DOI https://doi.org/10.3390/a17050201

23. *Kunadi S.K.* AI-Driven Data Enrichment and Golden Record Creation for Enterprise Customer Data Platforms // International Journal of Research and Applied Innovations. – 2026. – V. 9. – №. 1. – P. 13630-13640. – DOI https://doi.org/10.15662/IJRAI.2026.0901016

24. *Khan N. S. et al.* A Bayesian approach for suspicious financial activity reporting //International Journal of Computers and Applications. – 2013. – V. 35. – №. 4. – P. 181-187.

25. *Zuo Z. et al.* A Bayesian-Optimized XGBoost Approach for Money Laundering Risk Prediction in Financial Transactions //Information. – 2026. – V. 17. – №. 4. – P. 324. – DOI https://doi.org/10.3390/info17040324

26. *Sorokin A.S.* Construction of scorecards using the logistic regression model // Bulletin of Eurasian Science. – 2014. – No. 2 (21). – P. 82.

27. *Vassallo D., Vella V., Ellul J.* Application of gradient boosting algorithms for anti-money laundering in cryptocurrencies // SN Computer Science. – 2021. – V. 2. – №. 3. – P. 143. – DOI https://doi.org/10.1007/s42979-021-00558-z

28. *Pratama S.F., Wahid A.M.* Fraudulent transaction detection in online systems using random forest and gradient boosting //Journal of Cyber Law. – 2025. – V. 1. – №. 1. – P. 88-115. – DOI https://doi.org/10.63913/jcl.v1i1.16

29. *Yu C. H. et al.* Machine Learning-Enhanced Automation for Invoice Reconciliation: OCR-Based Solutions for Accuracy and Efficiency in Logistics Industry //Intelligent Systems Conference. – Cham: Springer Nature Switzerland, 2024. – P. 325-336. – DOI https://doi.org/10.1007/978-3-031-66336-9_23

30. *Berndsen R., Heijmans R.* Risk indicators for financial market infrastructure: from high frequency transaction data to a traffic light signal // De Nederlandsche Bank Working Paper. – No. 557. – URL: https://ssrn.com/abstract=2985412

31. *Islam S.* Machine Learning–Based AML/KYC Transaction Monitoring for Suspicious Activity Detection and Compliance Risk Reduction in Digital Banking // ASRC Procedia: Global Perspectives in Science and Scholarship. – 2025. – V. 1. – №. 01. – P. 1740-1775. – DOI https://doi.org/10.63125/r9c8q813

32. *Matveev A.V.* Comparative analysis of methods of interpretability of artificial intelligence models in decision-making processes // Modern science-intensive technologies. – 2026. – No. 5. – P. 131–138. – DOI 10.17513/snt.40785.

For citation: Leonov V. A., Zaytsev A. K., Matveev V. V. Artificial intelligence technologies in countering financial crime: opportunities and limitations // National security and strategic planning. 2026. № 1(53). pp. 57-77. DOI: https://doi.org/10.37468/2307-1400-2026-1-57-77

Сведения об авторах:

Леонов Вячеслав Алексеевич – кафедра экономики и финансов Санкт-Петербургского филиала Финансового университета при Правительстве Российской Федерации, г. Санкт-Петербург, Россия

Зайцев Александр Константинович – заместитель начальника аналитического отдела Межрегионального управления Федеральной службы по финансовому мониторингу по Северо-Западному федеральному округу, г. Санкт-Петербург, Россия
SPIN-код: 6389-1380
e-mail: alexanderzaitsev619@gmail.com

Матвеев Владимир Владимирович – доктор технических наук, профессор, профессор кафедры экономики и финансов, Финансовый университет при Правительстве РФ (Санкт-Петербургский филиал), г. Санкт-Петербург, Россия
SPIN-код: 6680-9575
e-mail: 070355mvv@gmail.com

Information about authors:

Leonov Viacheslav A. – Department of Economics and Finance, St. Petersburg Branch of the Financial University under the Government of the Russian Federation, St. Petersburg, Russia

Zaytsev Alexander K. – Deputy Head of the Analytical Department of the Interregional Office of the Federal Service for Financial Monitoring for the Northwestern Federal District, St. Petersburg, Russia
SPIN: 6389-1380
e-mail: alexanderzaitsev619@gmail.com

Matveev Vladimir V. – Doctor in Engineering, Professor, Professor of the Economics and Finance Department, Financial University under the Government of the Russian Federation (St. Petersburg branch), St. Petersburg, Russia
SPIN: 6680-9575
e-mail: 070355mvv@gmail.com