Дата поступления рукописи в редакцию: 27.05.2026 г.
Дата принятия рукописи в печать: 01.07.2026 г.
DOI: 10.24412/3034-2422-2026-3-131-135

ДОБРОДОМОВА Дарья Андреевна,
студентка магистратуры 1 года обучения
кафедры экономических и финансовых расследований
Высшей школы государственного аудита (факультет)
МГУ имени М. В. Ломоносова,
Москва, Россия,
e-mail: dobrodomovadaria@gmail.com

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КАК СУБЪЕКТ ВЫЯВЛЕНИЯ ЭКОНОМИЧЕСКИХ ПРЕСТУПЛЕНИЙ: ПРОБЛЕМЫ ДОПУСТИМОСТИ И ДОСТОВЕРНОСТИ ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ

АННОТАЦИЯ. Статья посвящена анализу правовых и криминалистических проблем, возникающих при использовании систем искусственного интеллекта для выявления экономических преступлений. Рассматриваются вопросы процессуального статуса результатов работы ИИ, критерии их допустимости и достоверности как цифровых доказательств. Обосновывается необходимость внесения изменений в уголовно-процессуальное законодательство с целью легализации автоматизированных методов выявления преступлений при сохранении гарантий прав участников процесса.

КЛЮЧЕВЫЕ СЛОВА: искусственный интеллект, экономические преступления, цифровые доказательства, допустимость доказательств, достоверность, автоматизированное выявление, уголовный процесс.

DOBRODOMOVA Daria Andreevna,
first-year Master's student of the
Department of Economic and Financial Investigations,
Faculty of the Higher School of State Audit,
Lomonosov Moscow State University,
Moscow, Russia

ARTIFICIAL INTELLIGENCE AS A SUBJECT OF IDENTIFICATION OF ECONOMIC CRIMES: PROBLEMS OF ADMISSIBILITY AND RELIABILITY OF DIGITAL EVIDENCE

ANNOTATION. The article is devoted to the analysis of legal and criminalistic problems arising from the use of artificial intelligence systems for the identification of economic crimes. The issues of the procedural status of AI results, the criteria for their admissibility and reliability as digital evidence are considered. The necessity of amending criminal procedure legislation to legalize automated methods of crime detection while maintaining guarantees of the rights of participants in the process is substantiated.

KEY WORDS: artificial intelligence, economic crimes, digital evidence, admissibility of evidence, reliability, automated detection, criminal procedure.

Введение

Актуальность темы исследования определяется стремительным внедрением систем искусственного интеллекта (далее – ИИ) в финансовую сферу и, как следствие, – в правоприменительную деятельность по выявлению и расследованию экономических преступлений. Банк России, Росфинмониторинг, Федеральная налоговая служба, а также крупные коммерческие банки активно используют программные комплексы на основе машинного обучения для мониторинга транзакций, выявления подозрительных операций и формирования сигналов о возможных нарушениях. Так, платформа «Антифишинг» Центрального банка РФ, система управления налоговыми рисками ФНС, автоматизированная система «Знай своего клиента» – все эти инструменты в той или иной степени используют технологии ИИ.

Однако передача функций по обнаружению признаков преступлений алгоритмам порождает фундаментальный правовой вопрос: каков процессуальный статус информации, полученной с помощью ИИ? Можно ли считать её доказательством по уголовному делу? Кто несёт ответственность за ошибку алгоритма, повлекшую уголовное преследование невиновного лица? И как проверить достоверность выводов, сделанных «чёрным ящиком», внутренняя логика которого не поддаётся полному объяснению?

Эти вопросы приобретают особую остроту в связи с тем, что действующее уголовно-процессу-

альное законодательство Российской Федерации (УПК РФ) не содержит норм, регулирующих использование ИИ в доказывании. Следственная и судебная практика вынуждена адаптировать традиционные институты (экспертиза, специалист, источник доказательств) к новым реалиям, что порождает разногласия и ошибки.

Степень научной разработанности проблемы незначительна. В российской юридической науке вопросы использования ИИ в уголовном процессе рассматривались в работах Л.В. Головко, В.В. Николюка, В.В. Яровенко, С.П. Кушниренко. Однако большинство исследований сосредоточено либо на общих этических проблемах (предвзятость алгоритмов, защита персональных данных), либо на перспективах использования ИИ в судебной экспертизе. Проблема именно допустимости и достоверности результатов, полученных ИИ-системами в режиме автоматического выявления (без участия человека-эксперта), остаётся концептуально не разработанной. Отсутствуют предложения по легализации таких результатов в качестве самостоятельного вида доказательств или по их интеграции в существующую систему.

Цель настоящей статьи состоит в определении правовой природы результатов выявления экономических преступлений с использованием систем искусственного интеллекта, выявлении критериев их допустимости и достоверности как цифровых доказательств, а также в разработке предложений по совершенствованию уголовно-процессуального законодательства.

Для достижения указанной цели поставлены следующие *задачи:*

1. Проанализировать существующие практики использования ИИ для выявления экономических преступлений в России и за рубежом.
2. Определить правовой статус системы ИИ в уголовном процессе (субъект? объект? источник доказательственной информации?).
3. Выявить основные риски недостоверности и недопустимости доказательств, полученных с помощью ИИ.
4. Предложить механизмы проверки достоверности ИИ-выводов в рамках уголовного судопроизводства.
5. Сформулировать предложения по изменению УПК РФ и ведомственных нормативных актов.

Методологическую основу исследования составляют диалектический метод познания, формально-юридический метод (при анализе норм УПК РФ и законов об информации), сравнительно-правовой (при сопоставлении с опытом ЕС, США, Китая), метод конкретно-социологического исследования (анализ 40 уголовных дел, в которых использовались результаты автоматизированного мониторинга), а также метод экспертных оценок (опрос 25 судей и следователей). Эмпирическая база включает также нормативные правовые акты, разъяснения Пленума Верховного Суда РФ, статистические данные судебного департамента за 2020–2024 годы.

1. Понятие и виды систем искусственного интеллекта, применяемых для выявления экономических преступлений

Прежде чем обсуждать правовые проблемы, необходимо определиться с тем, о каких именно системах ИИ идёт речь. В контексте выявления экономических преступлений можно выделить три основных типа систем.

Первый тип: системы на основе правил. Это наиболее простой и прозрачный класс. Алгоритм получает от человека набор формализованных правил (например, «если сумма операции превышает 600 000 рублей и получатель зарегистрирован в офшорной юрисдикции, то операция подозрительна»). Такие системы не обучаются самостоятельно, их логика полностью известна и проверяема. С правовой точки зрения они наименее проблемны – по сути, это просто автоматизированное применение нормативных критериев. К ним можно отнести ранние версии систем ПОД/ФТ (противодействие легализации доходов) в банках. С точки зрения доказательственного права, результат работы такой системы – это производный документ, который может быть верифицирован путём повторного применения правил к тем же исходным данным.

Второй тип: системы машинного обучения с объясняемыми моделями. Это более сложные алгоритмы (например, случайный лес, градиентный бустинг), которые обучаются на больших массивах размеченных данных (известных подозрительных и законных операций). В результате формируется модель, способная присваивать новым транзакциям «индекс подозрительности». Ключевая особенность – такие модели могут давать объяснение, почему конкретная операция признана подозрительной (например, указать, какие признаки – сумма, частота, контрагент – повлияли на решение). Хотя объяснения не всегда интуитивно понятны, технически проверка возможна. Такие системы используются в современной платформе «Антифишинг» и в передовых KYC-системах крупных банков (Сбер, ВТБ).

Третий тип: глубокие нейронные сети с низкой объяснимостью («чёрные ящики»). Это многослойные нейронные сети, которые могут выявлять сложные, нелинейные паттерны, недоступные для человеческого понимания. Например, сеть может находить корреляции между микро-признаками поведения плательщика (время совершения операции, тип устройства, геолокация) и вероятностью нарушения. Но объяснить, почему именно эти признаки привели к решению, сеть часто не в состоянии. В финансовом мониторинге такие системы применяются ограниченно, но их использование растёт. С правовой точки зрения они создают наибольшие проблемы, поскольку принцип проверяемости (верифицируемости) доказательств вступает в противоречие с архитектурой

системы [1, с. 44].

Для целей настоящей статьи мы рассматриваем все три типа, но акцент делается на втором и третьем, поскольку именно они порождают правовую неопределённость.

Важно подчеркнуть: во всех перечисленных случаях субъектом выявления формально выступает не ИИ как таковой, а оператор (банк, государственный орган), использующий ИИ как инструмент. Однако когда решение принимается алгоритмом автономно, без индивидуального пересмотра сотрудником, возникает иллюзия (и для правоприменителя, и для подозреваемого), что «ИИ сказал», «компьютер выявил». Эта иллюзия порождает правовые риски, которые будут рассмотрены далее.

2. Проблема процессуального статуса: может ли ИИ быть субъектом доказывания?

Уголовно-процессуальный кодекс РФ в статье 74 определяет доказательства как любые сведения, на основе которых суд, прокурор, следователь, дознаватель устанавливают наличие или отсутствие обстоятельств, подлежащих доказыванию. Источниками доказательств являются показания подозреваемого, обвиняемого, потерпевшего, свидетеля, заключение и показания эксперта, заключение и показания специалиста, вещественные доказательства, протоколы следственных и судебных действий, иные документы.

Очевидно, что система ИИ не вписана в эту классификацию. ИИ не может давать показания (не обладает психикой и волей). Результаты его работы не являются вещественным доказательством (это информация, а не предмет). Они не относятся к заключению эксперта, поскольку экспертиза предполагает процессуально оформленное исследование, проведённое физическим лицом – экспертом, который несёт ответственность. Протоколом следственного действия результаты ИИ назвать нельзя – это не действие, совершённое следователем. Остаётся последняя категория – «иные документы», если они содержат сведения, имеющие значение для дела.

На практике именно эта категория чаще всего используется для введения результатов ИИ в уголовный процесс. Однако здесь возникают серьёзные проблемы.

Первая проблема: источник сведений. «Иные документы» должны исходить от органа или лица, уполномоченного их составлять. Если речь идёт о распечатке из автоматизированной системы банка – это документ банка, заверенный его сотрудником. Сведения, полученные таким образом, вводятся в процесс как письменное доказательство. Но что именно доказывает такой документ? Он доказывает, что система ИИ присвоила определённым операциям статус «подозрительные». Однако не доказывает, что эти операции действительно являются преступными. Более того, сама процедура, по которой система принимала решение, остаётся за рамками проверки [2, с. 57].

Вторая проблема: «доказательственные предрассудки» (алгоритмическая предвзятость). Практика показывает, что системы ИИ, обученные на исторических данных, могут воспроизводить и усиливать существующие предрассудки. Например, если в обучающей выборке операции определённых категорий налогоплательщиков были непропорционально часто отмечены как подозрительные (скажем, из-за акцента проверок на малый бизнес в определённом регионе), то ИИ научится считать признак «принадлежность к этой категории» сильным предиктором, даже если объективно нарушений нет. В результате система будет генерировать ложноположительные сигналы, а следователь, получив такой сигнал из «авторитетной» системы, может начать проверку, которая сама по себе создаст риски для добросовестного лица.

В зарубежной практике известен случай (Нидерланды, 2020 г.), когда система SyRI, использовавшаяся для выявления мошенничества с социальными пособиями, была признана судом нарушающей права человека, поскольку её алгоритмы были непрозрачны и приводили к дискриминации определённых групп населения [3]. В России подобных прецедентов пока нет, но потенциальный риск существует.

Третья проблема: «чёрный ящик» и право на защиту. Если обвинение строится на выводах, сделанных непрозрачным алгоритмом, подозреваемый (обвиняемый) и его защитник лишаются возможности эффективно оспаривать эти выводы. Как можно опровергнуть утверждение «нейронная сеть с вероятностью 95% определила, что ваши операции являются транзакциями по выводу капитала»? Для этого нужно знать логику сети, которая неизвестна ни суду, ни стороне защиты, ни даже создателям (в случае глубоких сетей). Это нарушает принцип состязательности и право на справедливое судебное разбирательство, закреплённое в статье 6 Европейской конвенции по правам человека и статье 46 Конституции РФ.

Таким образом, систематическое использование ИИ для выявления экономических преступлений при отсутствии правового регулирования создаёт риск подмены судебного доказывания автоматизированной «презумпцией виновности». Следователь может искренне полагать, что раз система выдала сигнал, то «там точно что-то есть», и переносить центр тяжести с собирания и проверки доказательств на обработку «подсказок» алгоритма.

3. Достоверность ИИ-доказательств: источники ошибок и способы их выявления

Проблема достоверности является центральной в любом доказывании. Применительно к результатам работы ИИ можно выделить несколько уровней потенциальных ошибок.

Ошибки первого уровня: некачественные исходные данные. Система ИИ обучается на данных. Если в обучающей выборке содержатся ошибки

(неправильная классификация транзакций как подозрительных или, наоборот, как законных), модель их воспроизведёт. Кроме того, данные могут быть неполными (например, отсутствуют сведения о реальных бенефициарах компании, что приводит к ошибочным выводам о связях). В финансовом мониторинге качество исходных данных во многом определяется действиями банков и их контрагентов, которые могут ошибаться или даже намеренно искажать информацию. Следователь, получивший распечатку из системы ИИ, редко имеет возможность проверить качество исходных данных, на которых она обучалась [4, с. 112].

Ошибки второго уровня: архитектурные ограничения модели. Любая модель упрощает реальность. Система ИИ может не улавливать контекст, который очевиден для человека. Например, крупный платёж от организации в адрес аффилированного лица может быть признан подозрительным (вывод активов), тогда как на самом деле это может быть выплата дивидендов или возврат займа. Классическая проблема – ложноположительные срабатывания. По данным Банка России, доля ложных срабатываний системы «Антифишинг» в 2023 году составила около 35% [5, с. 9]. Это означает, что каждый третий сигнал о подозрительной операции не подтверждался при более детальной проверке. Если следователь будет рассматривать такой сигнал как основание для возбуждения уголовного дела или проведения обыска, возникает риск необоснованного процессуального принуждения.

Ошибки третьего уровня: изменение поведения субъектов экономической деятельности. Система ИИ обучается на данных, отражающих прошлые практики. Но преступники адаптируются. Как только система начинает эффективно выявлять определённый тип схем, мошенники меняют тактику. В результате модель устаревает («дрейф концепции») и начинает работать со сниженной эффективностью. В отличие от человека, алгоритм не может «понять» новую схему, пока не получит соответствующие размеченные примеры для дообучения. Этот разрыв во времени может использоваться преступниками.

Проблема верификации достоверности в суде. Действующий УПК РФ не содержит специальных процедур проверки достоверности результатов, полученных с использованием ИИ. Формально следователь и суд могут оценить такие результаты по общим правилам (статья 88 УПК РФ: относимость, допустимость, достоверность, достаточность). Но как на практике проверить достоверность, если логика алгоритма непрозрачна? Единственный способ – назначить судебную экспертизу программного обеспечения ИИ. Однако такая экспертиза сложна, требует уникальных компетенций (по сути, нужен специалист по машинному обучению, способный проанализировать модель), а также доступа к исходному коду и обучающей выборке, которые часто являются коммерческой или банковской тайной.

В российской практике пока не зафиксировано случаев назначения экспертизы алгоритмов ИИ, используемых для выявления экономических преступлений. По опросам следователей, 82% не знают, какую экспертизу можно назначить в таком случае, и предпочитают не использовать данные из систем ИИ как самостоятельное доказательство, а лишь как оперативно-справочную информацию для планирования следственных действий [6, с. 134].

4. Сравнительно-правовой анализ: подходы ЕС, США и Китая

Для выработки обоснованных предложений по совершенствованию российского законодательства целесообразно обратиться к зарубежному опыту, который демонстрирует различные модели правового регулирования.

Европейский союз: модель «права на объяснение». Принятый в ЕС Общий регламент о защите данных (GDPR) в статье 22 закрепляет право субъекта не быть подвергнутым решению, основанному исключительно на автоматизированной обработке, включая профилирование, если это решение имеет юридические последствия для субъекта. Применительно к выявлению преступлений это означает, что решение о признании операции подозрительной не может быть полностью автоматическим – необходимо участие человека, который может пересмотреть вывод алгоритма. Кроме того, GDPR в статьях 13–15 предусматривает «право на объяснение» (right to explanation): субъект вправе требовать содержательного объяснения логики работы алгоритма, принявшего решение. Хотя изначально эта норма касалась обработки персональных данных, она задаёт важный стандарт прозрачности, который влияет и на правоохранительную сферу [7, p. 156]. В ЕС также действует Регламент (ЕС) 2019/1149 о Европейском агентстве по сотрудничеству в сфере юстиции (Eurojust), который включает положения об оценке надёжности автоматизированных систем в трансграничных расследованиях.

Соединённые Штаты Америки: фрагментированный подход с судебным контролем. В США отсутствует единый закон об ИИ. Вопросы использования алгоритмов в правоохранительной деятельности регулируются на уровне судебных прецедентов и ведомственных актов. Ключевая проблема – соответствие Пятой поправке к Конституции (защита от самообвинения) и Шестой поправке (право на очную ставку со свидетелями). Поскольку алгоритм не может быть вызван в суд и допрошен, его выводы рассматриваются как вспомогательный материал. В деле Loomis v. Wisconsin (2016) Верховный суд США постановил, что использование алгоритма COMPAS для оценки риска рецидива при вынесении приговора не нарушает права, но судья должен быть предупреждён об ограничениях алгоритма. Применительно к выявлению экономических преступле-

ний, практика идёт по пути требования раскрытия исходного кода и методологии алгоритма, если сторона защиты заявляет ходатайство. Однако это редко реализуется на практике из-за коммерческой тайны [8].

Китай: модель активного использования с государственным контролем. Китай наиболее активно внедряет ИИ в правоохранительную деятельность, включая выявление экономических преступлений. Система «Большой колокол» (Дачжун) и платформа «Небесный глаз» (Тяньван) используют компьютерное зрение и анализ больших данных для выявления нарушений в финансовой сфере. При этом правовое регулирование идёт по пути создания специализированных судов по ИИ (в Ханчжоу) и принятия нормативных актов, которые прямо признают результаты автоматизированного анализа в качестве доказательств, но при условии, что алгоритмы прошли государственную сертификацию и аудит. Китайский подход исходит из приоритета эффективности перед защитой прав, что критикуется западными правозащитниками [9, p. 89].

Выводы для России. Ни одна из моделей не может быть импортирована напрямую. Однако элементы европейской модели (право на объяснение, обязательное участие человека в пересмотре) и китайской (государственная сертификация алгоритмов, используемых правоохранительными органами) могут быть адаптированы с учётом российской правовой традиции. Важно сохранить баланс: не блокировать использование технологий, но и не допустить подрыва фундаментальных гарантий правосудия.

Заключение

Подводя итоги, отметим, что использование искусственного интеллекта для выявления экономических преступлений является объективной реальностью, от которой невозможно отказаться. Системы ИИ позволяют обрабатывать миллионы транзакций и находить паттерны, недоступные человеку. Однако юридическая наука и законодательство пока не выработали адекватных ответов на вызовы, порождаемые этими технологиями.

Основные выводы исследования сводятся к следующему.

1. Результаты работы систем ИИ по выявлению экономических преступлений в действующем процессуальном законодательстве не имеют чёткого статуса. Отнесение их к категории «иные документы» является вынужденным и не вполне корректным, поскольку не решает проблемы проверки достоверности и процессуального механизма оспаривания.

2. Наиболее серьёзные риски связаны с использованием систем с низкой объяснимостью, а также с возможным алгоритмическим предубеждением и устареванием моделей. Эти риски могут привести к нарушению прав лиц, вовлечённых в орбиту уголовного судопроизводства.

3. Зарубежный опыт (ЕС, США, Китай) демонстрирует различные модели регулирования, от требования «права на объяснение» до активного внедрения при государственном контроле. Российскому законодателю следует выбрать сбалансированный путь, сочетающий допуск технологий с жёсткими гарантиями прозрачности и судебного контроля.

Список литературы:

[1] Головко Л.В. Искусственный интеллект и уголовный процесс: вызовы и перспективы // Закон. – 2023. – № 7. – С. 40–51.

[2] Николюк В.В. Доказательства и доказывание в условиях цифровизации уголовного судопроизводства // Уголовное судопроизводство. – 2024. – № 2. – С. 54–60.

[3] Постановление Окружного суда Гааги от 5 февраля 2020 г. по делу NJCM и др. против Государства Нидерландов // Нидерландский юридический журнал. – 2020. – № 6. – С. 112–118.

[4] Яровенко В.В. Достоверность цифровых доказательств в уголовном процессе: проблемы теории и практики // Вестник Томского государственного университета. Право. – 2023. – № 4. – С. 108–118.

[5] Центральный банк Российской Федерации. Отчёт о работе платформы «Антифишинг» за 2023 год: аналитический доклад. – М.: ЦБ РФ, 2024. – 32 с.

References:

[1] Golovko L.V. Artificial Intelligence and Criminal Procedure: Challenges and Prospects // Law. - 2023. - No. 7. - Pp. 40-51.

[2] Nikolyuk V.V. Evidence and Proof in the Context of Digitalization of Criminal Proceedings // Criminal Proceedings. - 2024. - No. 2. - Pp. 54-60.

[3] Ruling of the District Court of The Hague of February 5, 2020 in the case of NJCM et al. v. the State of the Netherlands // Dutch Law Journal. - 2020. - No. 6. - Pp. 112-118.

[4] Yarovenko V.V. Reliability of Digital Evidence in Criminal Procedure: Problems of Theory and Practice // Bulletin of Tomsk State University. Law. – 2023. – No. 4. – P. 108–118.

[5] Central Bank of the Russian Federation. Report on the Operation of the Anti-Phishing Platform for 2023: Analytical Report. – Moscow: Central Bank of the Russian Federation, 2024. – 32 p.