Полицейская и следственная деятельность
Правильная ссылка на статью:
Яковлева Е.О. ИИ как криминогенный фактор: проблемы квалификации и тактики расследования // Полицейская и следственная деятельность. 2025. № 4. DOI: 10.25136/2409-7810.2025.4.77391 EDN: QRNFOM URL: https://nbpublish.com/library_read_article.php?id=77391

ИИ как криминогенный фактор: проблемы квалификации и тактики расследования

Яковлева Елена Олеговна

ORCID: 0000-0003-1733-3904

кандидат юридических наук

доцент; кафедра уголовного права; Юго-Западный государственный университет

305040, Россия, Курская область, г. Курск, ул. Пятьдесят Лет Октября, 94

pragmatik-alenka@yandex.ru

Статья из рубрики "Информационное обеспечение деятельности полиции"

DOI:

10.25136/2409-7810.2025.4.77391

EDN:

QRNFOM

Дата направления статьи в редакцию:

16-12-2025

Дата публикации:

23-12-2025

Аннотация: В статье рассматривается проблема отсутствия комплексного, опережающего правового ответа, основанного на глубоком понимании технологических рисков, позволяющего правоохранительным органам сохранить эффективность в условиях новой цифровой реальности и обеспечивать защиту национальной безопасности. Предметом исследования выступили нормы отечественного законодательства, регламентирующие отношения, возникающие при использовании ИИ. Целью исследования является выявление уголовно-правовых и криминалистических пробелов в противодействии преступности, связанной с технологиями искусственного интеллекта (ИИ), и разработка конкретных мер по их устранению. На основе анализа ведомственной статистики МВД России, Следственного комитета РФ и судебной практики

доказывается нарастающий разрыв между технологическими возможностями злоумышленников и адекватностью действующих правовых механизмов. В результате систематизации угроз предложена авторская классификация систем ИИ по степени автономности, сфере применения и уровню риска, служащая основой для дифференцированного правового подхода. Методология включает: 1) формально-юридический и сравнительно-правовой анализ; 2) социолого-правовые методы; 3) методы юридической техники (конструирование гипотез, диспозиций, санкций); 4) криминалистические методы моделирования способов совершения преступлений и тактик расследования. Использован комплекс общенаучных и частно-научных методов: диалектического, формально-юридического, сравнительно-правового, системно-структурного и прогностического методов. Научная новизна заключается в разработке уголовно-релевантного определения ИИ, выявлении специфических проблем квалификации (вменения, субъекта ответственности, причинной связи) и обосновании комплекса тактико-криминалистических рекомендаций и законодательных новелл, направленных на формирование адекватного инструментария для следственных органов. Ключевые выводы: 1) действующие нормы УК РФ (гл. 28, ст. 159 УК РФ) недостаточны для квалификации автономных действий ИИ; 2) необходимы новые составы (например, «Создание вредоносной системы ИИ») и квалифицирующие признаки; 3) требуется законодательное закрепление процедур изъятия и экспертизы алгоритмических моделей как вещественных доказательств; 4) основой системного противодействия должен стать риск-ориентированный федеральный закон об ИИ, устанавливающий требования к безопасности, прозрачности и аудиту высокорисковых систем.

Ключевые слова:

правоохранительные органы, закон, национальная безопасность, искусственный интеллект, киберпреступность, квалификация преступлений, тактика расследования, уголовная ответственность, криминалистические рекомендации, цифровая криминология

Работа выполнена в рамках Государственного задания Правовые меры обеспечения стратегических приоритетов по противодействию угрозам национальной безопасности (FENM-2025-0010). Регистрационный номер 1024031900131-7-5.5.1.

Введение

В XXI веке развитие и внедрение технологий искусственного интеллекта (ИИ) приобрело системный характер и затрагивает практически все сферы государственного управления, экономики и обороны. Вместе с очевидными преимуществами — автоматизацией процессов, повышением эффективности принятия решений, развитием научных и медицинских решений — ИИ порождает новые риски, которые имеют междисциплинарный характер: они включают военно-стратегические угрозы, уязвимости критической информационной инфраструктуры, риски массовой дезинформации, социально-экономические и этико-правовые последствия, способные дестабилизировать общественные отношения и снизить уровень государственного суверенитета. В силу перечисленного правовое реагирование на вызовы ИИ требует системного подхода от выработки правовой дефиниции и классификации систем ИИ до институциональных механизмов надзора, мер профилактики и международного взаимодействия.

В то же время стремительная эволюция технологий искусственного интеллекта

формирует новую криминогенную реальность. Если изначально ИИ рассматривался в контексте инновационного развития, то сегодня его деструктивный потенциал становится источником конкретных и масштабных угроз национальной безопасности, реализуемых через совершение общественно опасных деяний. Преступные использования ИИ качественно трансформируют традиционные способы совершения преступлений (мошенничество, клевета, неправомерный доступ к компьютерной информации), а также порождают новые формы общественно опасного поведения (массовая персонализированная манипуляция, автономные кибератаки, создание неуправляемых вредоносных алгоритмов).

Данные МВД России и Следственного комитета РФ за 2022-2024 гг. фиксируют рост числа преступлений в сфере компьютерной информации на 25%, при этом экспертная оценка позволяет утверждать, что в 30-40% таких эпизодов использовались элементы автоматизации, подпадающие под признаки ИИ (например, адаптивные боты для фишинга, ИИ-софт для подбора паролей). Количество мошенничеств, совершаемых с помощью голосовых клонов (deepfake) и интеллектуальных чат-ботов, по данным Генпрокуратуры РФ, выросло в 2023 г. в 1,7 раза, а средний ущерб по таким делам на 50% выше. По данным Генпрокуратуры РФ в 2024 г. на фоне общего снижения количества зарегистрированных преступлений, удельный вес преступлений в сфере ИКТ и с использованием цифровых инструментов достигло 40%. В отчете Генерального прокурора Президенту РФ подробно указаны возможные направления борьбы с подобными преступлениями, в том числе с использованием мер, обеспечивающих технологическую независимость правоохранительных органов, что направлено на обеспечение интересов национальной безопасности. Судебная практика по ст. 274.1 УК РФ («Неправомерное воздействие на критическую информационную инфраструктуру») показывает, что в 5 из 20 рассмотренных дел злоумышленники применяют самообучающиеся алгоритмы для поиска уязвимостей. В отдельных судебных решениях указывается на использование подсудимыми нейросетевой модели для генерации массовых фишинговых сообщений, что впоследствии признается отягчающим обстоятельством.

Стратегическое значение технологий искусственного интеллекта для национальной безопасности сопряжено с формированием принципиально новой криминогенной реальности. Дуализм ИИ, выступающего как драйвер инноваций и источник системных угроз, порождает правовой парадокс: скорость технологических изменений опережает темпы адаптации уголовно-правовых и процессуальных механизмов. Это создает «нормативный вакуум», которым активно пользуются злоумышленники.

Интеграция ИИ в системы правоохранительных структур, государственного управления, критическую инфраструктуру, оборонно-промышленный комплекс и экономику открывает широкие возможности повышения эффективности, но одновременно создает новые, качественно иные по своему характеру угрозы, требующие осуществления не только технологических мер противодействия, но и системного правового — разработки адекватных нормативно-правовых механизмов, институциональных инструментов и процедурного контроля [1]. Сказанное возможность воспринимать ИИ как источник угроз национальной безопасности по крайней мере тремя взаимосвязанными факторами:

1 . дуалистическая природа технологий ИИ, где одни и те же алгоритмические инструменты могут служить как обеспечению общественных благ (медицина, логистика, управление ресурсами), так и созданию рисков (кибератаки, манипуляция общественным мнением, автономные боевые системы);

2 . нормативно-процедурный контекст, где скорость технологических изменений существенно опережает темпы формирования системного правового регулирования, что порождает пробелы, неясности и фрагментарность применимого права;

3 . геополитическое значение ИИ, где технологическое лидерство превращается в фактор стратегического влияния и гарант национального суверенитета, повышая риски технологической зависимости при отсутствии собственных компетенций и стандартов.

Такая совокупность обстоятельств обосновывает необходимость комплексного юридического исследования по выявлению и систематизации угроз, порождаемых ИИ, и разработке конкретных правовых механизмов их минимизации, в том числе используемых правоохранительными органами в работе [2].

Целью данной работы является общий анализ рисков, и прикладной уголовно-правовой и криминалистический разбор конкретных механизмов использования ИИ в преступных целях, выявление пробелов в квалификации и расследовании преступлений, а также формулировка конкретных предложений для законодателя и правоприменителя.

Методология исследования основана на межотраслевом подходе и включает: 1) формально-юридический и сравнительно-правовой анализ норм УК РФ, УПК РФ и стратегических документов; 2) социолого-правовые методы (анализ ведомственной статистики, обобщение судебной практики) для оценки эмпирической базы угроз; 3) методы юридической техники для конструирования новых составов и процессуальных процедур; 4) криминалистические методы моделирования способов совершения преступлений и тактических алгоритмов расследования. Комбинация используемых в исследовании методов позволила проследить иерархию нормативных актов, соотнести технологические риски с правовыми институтами и предложить правовые решения возможные к применению на практике [3].

Результаты и обсуждение

Развитие ИИ открывает новые возможности в решении сложных задач, начиная от медицины и заканчивая космической отраслью, где традиционные методы оказываются недостаточно эффективными. Важность изучения ИИ определяется также растущей потребностью в специалистах, способных разрабатывать и внедрять интеллектуальные системы в реальный сектор экономики. Особую роль играет необходимость понимания этических и социальных аспектов развития ИИ, включая вопросы безопасности, конфиденциальности данных и влияния на рынок труда. Иными словами в условиях глобальной цифровизации изучение ИИ становится не просто желательным, а необходимым компонентом образования, позволяющим формировать компетенции, востребованные в будущем. Однако особую важность приобретает изучение ИИ как угрозы национальным российским интересам.

Сегодня ИИ – это перспективное и самостоятельное научное направление. Оно фокусируется на создании алгоритмов, способных имитировать работу человеческого мозга и образ мыслей человека. Некоторые авторы выделяют способность ИИ к самообучению, а также его автономность, т.е. возможность совершать действия без вмешательства человека, способность не только к действиям в соответствии с изначально заложенным алгоритмом, но и к принятию самостоятельных решений на основании самообучения с учетом предыдущего опыта. С другой стороны ученые отмечают, что ИИ не может быть сравним в полной мере с человеком, поскольку не имеет сознания, чувств и интересов. Однако технологии ИИ уже способны создавать

новый контент и идеи. Регулировать искусственный интеллект — сложная и дуальная задача. Избыточность мер правового реагирования может отрицательно сказаться на инновациях, в то время как недостаточное регулирование ИИ может привести к серьезному ущербу прав граждан, а также к потере возможности формировать стабильное будущее.

Цифровизация, увеличение объёма данных, рост мощности компьютеров, развитие алгоритмов машинного обучения неизбежно приведут к законодательному переосмыслению правового регулирования ИИ. Ведь ИИ теперь способен выполнять задачи, которые раньше считались исключительной прерогативой человека: анализировать большие объёмы информации, самообучаться на основе опыта, принимать решения, общаться с людьми, создавать контент (музыку, тексты), управлять транспортными средствами. Технология проникла практически во все сферы жизни - от простых приложений на смартфонах до сложных систем в медицине, производстве и транспорте и прочие. В ряде задач ИИ уже демонстрирует результаты, превосходящие человеческие. И развитие этой технологии продолжается, открывая всё новые возможности для человечества.

На сегодняшний день более 30 государств разработали и внедрили национальные стратегии развития искусственного интеллекта, а также осуществляется активная работа по принятию международных правовых актов в данной сфере. Особое внимание уделяется вопросам кибербезопасности, защиты персональных данных и аутентификации цифрового контента. А в экономической плоскости возникает необходимость правового регулирования вопросов влияния искусственного интеллекта на рынок труда, противодействия мошенничеству с использованием данных технологий, а также определения ответственности разработчиков и пользователей систем искусственного интеллекта. Активное развитие правового регулирования в сфере ИИ рассматривается за рубежом в нескольких ключевых юрисдикциях. К числу государств, демонстрирующих последовательное развитие нормативной базы в данной области, относятся Европейский Союз, Соединенные Штаты Америки и Китайская Народная Республика. Детальный анализ передовых концепций правового регулирования ИИ требует тщательного изучения правовых систем указанных государств.

Так, в Европейском Союзе координацию развития ИИ осуществляет Европейская комиссия, которая реализует комплекс мер по стимулированию развития отрасли при соблюдении прав человека по трем основным направлениям: разработка правовой концепции регулирования систем ИИ; определение механизмов установления ответственности за вред, причиненный системами ИИ и формирование актуального отраслевого законодательства. На основе чего экспертное сообщество сформулировало четыре основных варианта правового регулирования ИИ:

1. Единообразный акт ЕС с добровольной сертификацией. Отраслевой подход.

2. Комплексный акт ЕС с принципом пропорциональности и рискориентированным подходом.

3. Комплексный акт ЕС с дополнительными этическими кодексами для систем с низким уровнем риска.

4. Единый акт ЕС с обязательными требованиями для всех систем ИИ

Ключевой особенностью является применение рискориентированного подхода к классификации систем ИИ по степени потенциальной угрозы для здоровья, безопасности

и основных прав человека. Где системы ИИ подразделяются на три категории:

1. Системы с неприемлемым риском (подлежащие запрету).

2. Высокорисковые системы (подлежащие строгому регулированию).

3. Системы с низким риском (не требующие специального регулирования).

Европейский совет по защите персональных данных (EDPB) и Европейский надзорный орган по защите персональных данных (EDPS) выступили с критикой некоторых положений проекта Регламента AIA, предложив распространить действие акта на государственные органы третьих стран и включить в регулирование уже существующие системы ИИ, при этом обеспечив соответствие систем ИИ требованиям на протяжении всего жизненного цикла. Такие действия должны по их решению происходить совместно с четким определением применимости законодательства о защите персональных данных, уточнением концепции «риск для основных прав» и учетом рисков для объединений лиц. Таким образом, процесс правового регулирования ИИ в Европейском Союзе характеризуется комплексным подходом, учитывающим как необходимость развития технологий, так и защиту прав граждан, что указывает на наличие определенных рисков, признаваемых в странах ЕС.

В Китайской Народной Республике сформирована следующая система регулирования:

·обязательная регистрация ИИ-сервисов;

· обязательная маркировка сгенерированного контента;

· предварительная проверка безопасности перед выпуском на рынок;

· создание механизма рассмотрения жалоб пользователей;

· формирование семи специализированных регуляторов в различных сферах.

В США с 2023 года фиксируется резкое увеличение законопроектов, регулирующих общественные отношения в области систем искусственного интеллекта. Так их количество за последние 3 года увеличилось во много раз. Их основными характеристиками являются: регулирование «пограничного ИИ»; противодействие использованию ИИ в террористических целях; предотвращение военных угроз; защита от экзистенциальных рисков. Это говорит о тождественном понимании наличия угроз для общественности в различных отраслях в США, наряду с ЕС.

В России классификация национальных угроз, возможных от использования ИИ, может быть представлена в следующем виде.

1. Военно-стратегические угрозы. Так, разработка и применение автономных боевых систем (LAWS) создаёт риск принятия решений о применении силы без человеческого контроля. Это рождает правовую проблему, связанную с определением ответственных субъектов, соблюдение принципов международного гуманитарного права и отсутствием адекватной международной регуляции. В то же время интеграция ИИ в стратегическое планирование и управление ядерными силами ставит под угрозу предсказуемость и устойчивость стратегических командных систем в случае программных ошибок или внешнего вмешательства. Обозначенные ассиметричные военные преимущества и технологическая экспансия может привести к тому, что ведущие государства получат преимущество, подрывая стратегический баланс. Поэтому верно суждение отдельных ученых, предлагающих закрепить в национальном праве принцип «значимого

человеческого контроля», устанавливающего специальные процедуры тестирования и сертификации военных ИИ-систем, включающие запреты в военном применении определённых классов автономных систем [9].

2. Информационно-психологические угрозы. Генеративные технологии и deepfake все чаще повышают риск манипуляций массовым сознанием, подрыва доверия к государственным институтам. Поэтому определение преступных элементов в создании или распространении фейков, баланс свободы информации и защиты общественного порядка – относятся к актуальным юридическим вопросам. Уязвимость информационных систем, используемых в критической инфраструктуре, подтверждает необходимость выработки адекватных стандартов устойчивости и процедуры надежного реагирования. Масштабная автоматизация кибератак в виде использования ИИ для взлома, фишинга, подбора учётных данных лишь расширяет масштаб современных угроз. Минимизация степени подобного вреда, по справедливому мнению, возможна с учетом введения отдельных норм о безопасности ИИ-систем в критической инфраструктуре, а также их обязательной сертификацией и подготовкой регламентов уведомления о порядке реагирования на инциденты [10].

3. Социально-экономические угрозы. Сегодня автоматизация труда и социальная дестабилизация неизбежно приводят к массовой потере рабочих мест без программ адаптации, чем вызывает обоснованные риски для внутренней стабильности страны. Усиление цифрового неравенства и монополизация объяснима концентрацией технологий в руках «крупных субъектов» и иностранных компаний, что последовательно создаёт угрозы технологической зависимости. В то же время алгоритмическая торговля и автоматизированные кредитные решения способны породить системные финансовые риски. Следовательно, приоритетное значение приобретают механизмы защиты, пострадавших групп в сочетании с выработкой антимонопольных мер и стимулов для развития отечественных ИИ-разработок [11].

4. Этико-правовые угрозы. Сегодня достаточно проблематично соотнести традиционные институты ответственности с автономными системами. К возможным моделям разграничения их ответственности относятся — ответственность разработчика, оператора, производителя, солидарная ответственность, либо введение специальных институций ответственности. Алгоритмическая дискриминация служит отдельным риском в ущемлении прав и свобод при автоматизированных решениях (к примеру, в правосудии, трудоустройстве, кредитовании). К правовым рекомендациям в рассматриваемой области можно отнести введение специальных диспозитивных и императивных норм о безопасности, а также возможность внедрить механизмы независимого аудита алгоритмов [12].

Таким образом, современное правовое регулирование ИИ характеризуется комплексным подходом, направленным на создание сбалансированной системы, обеспечивающей как развитие технологий, так и защиту прав и интересов граждан. Данная система регулирования учитывает как потенциальные возможности, так и риски, связанные с развитием ИИ, что позволяет формировать эффективную правовую основу для его дальнейшего развития и внедрения в различные сферы общественной жизни, в том числе в сферу деятельности правоохранительных органов.

По нашему мнению, системы ИИ целесообразно классифицировать по трём ключевым критериям:

1. По степени автономности:

о ограниченно автономные (необходим постоянный человеческий контроль);

о полуавтономные (периодический человеческий контроль);

о полностью автономные (функционируют без непосредственного человеческого вмешательства).

2. По сфере применения:

о военного назначения;

о государственного управления и принятия решений;

о критической информационной инфраструктуры (энергетика, транспорт, связь, финансы);

о общего назначения (бытовые и коммерческие сервисы).

3. По уровню потенциального риска:

о неприемлемый риск (запрещённые системы);

о высокий риск (необходима сертификация, аудит, лицензирование);

о ограниченный риск (требуется обеспечивать прозрачность и уведомление);

о минимальный риск (общие требования по безопасности).

Такая градация служит возможной основой для установления дифференцированных требований к разработке, испытанию, сертификации и эксплуатации систем ИИ в России [7].

В Российской Федерации нормативную основу формирования государственного регулирования в сфере развития технологий ИИ составляют: Национальная стратегия развития Искусственного интеллекта до 2030 года; Федеральный закон № 123ФЗ от 24.04.2020 (эксперимент по специальному регулированию ИИ в г. Москве); Федеральный закон от 28.12.2010 г. № 390ФЗ «О безопасности»; Доктрина информационной безопасности (Указ Президента РФ от 05.12.2016 г. № 646); Стратегия национальной безопасности РФ, определенная Указом Президента РФ от 02.07.2021 № 400. Однако, легальное определение ИИ содержится в Национальной стратегии развития искусственного интеллекта до 2030 года и частично — в Федеральном законе от 24.04.2020 г. № 123ФЗ, где ИИ определяется как «комплекс технологических решений, позволяющий имитировать когнитивные функции человека…». Считаем, что законодательные формулировки стратегического и отраслевого характера нуждаются в уточнении применительно к целям регулирования: ответственности, обеспечения безопасности, защиты персональных данных и прав человека [4]. Поэтому, для целей уголовного права и процесса предлагается следующее легальное определение, интегрируемое в конструкцию норм: *«Искусственный интеллект — алгоритмическая система, способная к выполнению поставленных задач без явного указания на каждый шаг посредством обучения, анализа данных и адаптации своего поведения в условиях изменяющейся внешней среды, обладающая свойством автономности (самостоятельного принятия решений в рамках заданных параметров)».*

Ключевыми для права признаками в предлагаемом определении являются обучаемость,

адаптивность и автономность. Степень автономности становится классифицирующим признаком для определения оснований и границ ответственности человека. Несмотря на то, что в доктрине права и зарубежных проектах (например, упомянутый ранее проект Регламента ЕС об искусственном интеллекте — Artificial Intelligence Act) выделяются различные акцентуации: программно-алгоритмическая сущность ИИ, киберфизические воплощения и степень автономности, современная российская правоприменительная практика и нормативное проектирование должны исходить из функционального, а не только технологического подхода. Иными словами следует определять ИИ через совокупность его свойств и последствий применения для прав и обязанностей субъектов [5].

В целом, правовая дискуссия о подходах к регулированию ИИ носит принципиальный характер для уголовного права. С одной стороны, существует позиция, представленная, в частности, А.П. Боханом, о том, что существующего арсенала норм о киберпреступлениях (гл. 28 УК РФ) достаточно для противодействия любым технологическим новшествам, поскольку объект посягательства — компьютерная информация — остается неизменным [17]. По его мнению, «специальное регулирование ИИ излишне и создаст неоправданные сложности для правоприменения и инноваций». С другой стороны, В.А. Лаптев и ряд других ученых обоснованно указывают на уникальный признак ИИ — способность к недетерминированному, адаптивному поведению и автономному принятию решений, что стирает прямую причинно-следственную связь между действием (бездействием) человека и наступившим вредом [18]. Это ставит под вопрос применимость классических принципов вины и вменяемости. Справедливо разделять вторую позицию, где считается введение специального регулирования необходимым. Во-первых, нормы гл. 28 УК РФ предполагают наличие конкретного действия человека (доступа, создания, распространения). Автономная деятельность ИИ, инициированная человеком, но вышедшая за рамки его предвидения, не охватывается диспозицией. Во-вторых, специальный субъект — разработчик или оператор высокорискового ИИ — несет повышенную обязанность по обеспечению безопасности, что требует закрепления в уголовном законе (аналогично ст. 143, 216 УК РФ). В-третьих, контраргумент А.П. Бохана опровергается реальной практикой, где следователи вынуждены «подгонять» факты под существующие составы, не имея инструментария для квалификации самого факта создания или выпуска вредоносного ИИ.

К основным признакам ИИ, значимым для правового регулирования стоит отнести:

· способность к обработке данных, обучению и адаптации;

· возможность автономного принятия решений;

· имитацию когнитивных функций человека;

· направленность на решение конкретных задач;

· динамический, эволюционный характер поведения.

Исходя из этого, предлагается рассматривать ИИ как правовой объект комплексного характера (программно-алгоритмические решения сопряженные с инфраструктурой и процессами обработки данных), подлежащий дифференцированному правовому режиму в зависимости от риска и сферы применения [6].

Анализ мер действующего отечественного законодательного регулирования ИИ выявляет следующие системные пробелы в правовом поле:

1 . отсутствие комплексного федерального закона «Об искусственном интеллекте» с определением понятий и сферы действия;

2 . фрагментарность правового регулирования ответственности за вред, причинённый ИИ;

3. недостаточная детализация требований к прозрачности алгоритмов и аудиту ИИ;

4 . отсутствие институциональных механизмов сертификации и мониторинга ИИ на национальном уровне;

5. несовершенство механизмов защиты персональных данных применительно к методам обучения ИИ (реидентификация обезличенных данных, проблемы минимизации и объяснимости).

Правовые последствия таких пробелов могут оказывать прямое воздействие на возникновение рисков в отношении национальной безопасности России. К ним возможно отнести не только снижение качества управления критической инфраструктурой и усиление киберугроз, но и юридическую неопределённость при использовании ИИ в оборонной сфере [8].

Анализ действующих норм УК РФ на предмет их применимости к деяниям с использованием ИИ выявляет значительные сложности. Рассмотрим наиболее очевидные примеры.

1 . Мошенничество (ст. 159, 159.6 УК РФ). Использование ИИ для генерации контента (голосовые клоны, видео deepfake), имитирующего близкого человека или представителя власти, с целью хищения имущества, формально подпадает под состав. Однако проблема доказывания заключается в установлении факта именно «обмана» как сообщения заведомо ложной информации. Если ИИ синтезирует уникальный, не существовавший ранее, но правдоподобный голос, сложно квалифицировать это как «ложную информацию». Возможно, что новая редакция квалифицирующего признака «с использованием технологий искусственного интеллекта, имитирующих личность или создающих ложную реальность» в Примечании к ст. 159 УК РФ усилит санкцию и упростит квалификацию.

2 . Киберпреступления (ст. 272-274.1 УК РФ). ИИ может использоваться для автоматического поиска уязвимостей (ст. 272 УК РФ), создания и распространения самообучающихся вирусов (ст. 273 УК РФ), организации масштабных DDoS-атак (ст. 274.1 УК РФ). Главный пробел здесь — отсутствие ответственности за создание или передачу в эксплуатацию вредоносной системы ИИ, если ее деструктивный потенциал реализовался позже и автономно. Нами усматривается необходимость новой нормы «Создание, распространение или использование вредоносных искусственных интеллектуальных систем», помещенной в гл. 28 УК РФ с субъективной стороной в виде прямого или косвенного умысла относительно потенциального вреда.

3 . Преступления против общественной безопасности и здоровья населения. Использование ИИ для создания новых наркотических средств или токсичных веществ уже является реальностью. Алгоритмы способны моделировать молекулы с заданными свойствами, обходя законодательные запреты. Уголовный закон не учитывает этот опосредованный, но преднамеренный способ совершения преступления.

4 . Проблема субъекта ответственности. Дискуссия о целесообразности введения специального субъекта — разработчика ИИ — крайне актуальна. По аналогии с

ответственностью владельца источника повышенной опасности (ст. 1079 ГК РФ) предлагается установить уголовную ответственность для разработчиков и операторов высокорисковых автономных систем ИИ за непринятие достаточных мер по предотвращению вреда, если будет доказана их неосторожность. Это требует закрепления в законе критериев «высокорисковой автономной системы ИИ» и введение в Примечание к ст. 285 УК РФ понятия «лицо, ответственное за эксплуатацию высокорисковой автономной системы искусственного интеллекта» как специального субъекта для статей о халатности (ст. 293 УК РФ) и злоупотреблении полномочиями (ст. 285, 286 УК РФ).

Анализ деятельности правоохранительных органов также показал наличие противоречий. К ключевым проблемам тактики расследования преступлений с использованием ИИ и доказывания в первую очередь стоит отнести фиксацию процессуального статуса ИИ. Так, ИИ не является субъектом права, но его «действия» (логи принятия решений, выходные данные) должны быть доказательствами. Необходимо разработать и законодательно закрепить процедуру экспертного изъятия и исследования алгоритмической модели (исходный код, обучающие данные, логи) как вещественного доказательства, аналогично исследованию компьютерной программы. Второй проблемой можно назвать установление причинной связи между преступными действиями и негативными последствиями. Поэтому требуются новые методики проведения экспертиз, способные реконструировать цепочку: команда человека - обучение и настройка ИИ - автономное действие ИИ - наступление вреда. Это задача для комплексной судебной экспертизы (компьютерно-технической, программно-алгоритмической, возможно, психолингвистической — для анализа контента).

С этим учетом можно дать некоторые тактические рекомендации. При проведении выемки у подозреваемого (разработчика): обязательно изымать не только результаты работы ИИ, но и все версии алгоритмов, наборы обучающих данных, журналы обучения и тестирования. Допрашивая подозреваемого, необходимо детально выяснять степень его контроля над системой, понимания принципов ее работы и возможных рисков. При назначении экспертизы перед экспертом следует ставить вопросы не только о факте использования ИИ, но и о степени его автономности в конкретной ситуации, наличии «сбоев» или нештатных режимов работы. Также рекомендуется активно использовать оперативно-розыскные мероприятия для документирования процесса настройки и «обучения» ИИ преступным целям (например, при вербовке в террористические сообщества через чат-боты).

Предполагается, что ныне объективно дополнить перечень вещественных доказательств (ст. 81 УПК РФ) «материальными носителями информации, содержащими алгоритмические модели искусственного интеллекта, их обучающие наборы данных и логи принятия решений», а в ст. 195 УПК РФ целесообразно закрепить право следователя назначать «судебную экспертизу искусственных интеллектуальных систем», определив ее предмет и компетенцию экспертов.

Законодательная инициатива по созданию системного федерального законодательства «Об искусственном интеллекте» в связке с мерами по модернизации смежного законодательства и созданием национальных органов регулирования должна стать приоритетом политики обеспечения национальной безопасности в цифровую эпоху [13]. В проект Федерального закона «Об искусственном интеллекте в Российской Федерации» возможно включить предложенное выше уголовно-релевантное определение ИИ и критерии отнесения систем ИИ к категории «высокорисковые» для целей уголовной

ответственности. Также федеральное законодательство должно предусматривать обязанность разработчиков и операторов вести журналы аудита решений для обеспечения прослеживаемости действий ИИ.

Эффективная защита национальной безопасности в эпоху ИИ возможна лишь при сочетании законодательных мер, институциональных механизмов и международного сотрудничества [14]. Регулирование должно сохранить баланс, т.е. обеспечить безопасность и защиту прав граждан, одновременно не создавая непреодолимых барьеров для инноваций[15]. Предложенные институциональные решения от современных угроз [16] в рамках статьи направлены на достижение такой сбалансированной модели регулирования, где технологический прогресс сопровождается предсказуемыми правовыми гарантиями и адекватными механизмами ответственности.

Выводы

Проведенный анализ подтверждает, что технологическая эволюция ИИ формирует устойчивый криминогенный тренд, а правовое поле демонстрирует системное отставание. Противодействие требует не точечных поправок, а концептуального обновления уголовного и уголовно-процессуального законодательства в связке с принятием базового риск-ориентированного федерального закона об ИИ. Степенное внедрение технологий ИИ сопровождается определенными рисками, носящими многоаспектный характер, отметим, что исходя из масштаба и характера угроз, а также степени общественной опасности преступных посягательств, возможных с использованием технологий ИИ, требуется комплексная работа по его нормативно-правовому регулированию. Такая работа, должна базироваться на решении следующих научно-исследовательских задач:

1. Разработка принципов регулирования ИИ (безопасность, соблюдение прав человека, прозрачность, ответственность, технологический суверенитет).

2. Разработка классификации и правовых режимов распределения систем ИИ по уровням риска и установления для каждой категории процедур разработки, сертификации и мониторинга.

3. Разработка требований безопасности, прозрачности, аргументированию и оценке воздействия ИИ.

4. Определение единого механизма возмещения вреда от действий, сопряженных с использованием ИИ (правила распределения ответственности между участниками технологической цепочки).

5. Подготовка норм о трансграничном обмене данными и технологиями, участии в международных стандартах и договорах. В этой специфике транснациональный характер рисков требует международного взаимодействия по следующим направлениям: инициирование международных договоров по безопасному развитию ИИ (принципы, запреты, механизмы контроля); отдельные договоры по автономным боевым системам, включая запрет на полностью автономные ударные комплексы без значимого человеческого контроля; участие в формировании международных стандартов сертификации и тестирования (ISO, ООН); создание глобальных и региональных механизмов мониторинга и раннего предупреждения преступлений.

Изучение зарубежного опыта в сфере правового регулирования ИИ позволило выявить наиболее эффективные механизмы регулирования, предотвратить возможные ошибки и создать оптимальные инструменты адаптации международного опыта в национальной правовой системе. Это способствует успешной интеграции в глобальную систему регулирования ИИ и формированию эффективных механизмов правового контроля за развитием и применением данных технологий. Нами предполагается, что исследование зарубежного опыта правового регулирования ИИ представляется необходимым условием для формирования адекватной современным вызовам нормативно-правовой базы, способствующей сбалансированному развитию данной сферы и защите интересов всех участников правоотношений. Так, мировое сообщество активно формирует правовые режимы для ИИ. Европейский Союз с его риск-ориентированным подходом (AI Act) движется к жесткому регулированию, запрещая одни системы и вводя строгие требования для других (высокорисковых). Китай комбинирует стимулирование разработок с жестким государственным контролем, включая обязательную проверку безопасности и маркировку контента. США придерживаются более гибкой, отраслевой модели, делая акцент на саморегулировании отрасли при усилении контроля в сферах национальной безопасности и правах человека. Общими трендами для них являются: создание специализированных регуляторных органов; усиление защиты персональных данных в контексте ИИ; разработка механизмов аудита и сертификации; фокус на кибербезопасности и аутентификации цифрового контента. Для России критически важно не просто копировать, а адаптировать эти подходы, исходя из приоритетов обеспечения суверенитета и безопасности. Отсутствие сопоставимых по строгости механизмов контроля, особенно над системами двойного назначения, создает для страны репутационные и практические риски.

Модернизация уголовного законодательства и создание эффективных институтов контроля являются не бюрократической необходимостью, а условием сохранения государственного суверенитета в цифровую эпоху. Безопасное будущее в эпоху ИИ возможно только при условии, что технологический прогресс будет надежно заключен в рамки права, обеспечивающего защиту национальных интересов, прав граждан и стратегическую стабильность.

Предложенные изменения — введение новых квалифицирующих признаков, специального состава за создание вредоносного ИИ, следственных процедур фиксации и экспертизы алгоритмов, направлены на то, чтобы дать правоохранительным органам реальный, а не декларативный инструментарий для борьбы с этой новой формой преступности. Баланс между инновациями и безопасностью будет обеспечен не отсутствием регулирования, а его четкостью, предсказуемостью и ориентированностью на конкретные, эмпирически подтвержденные угрозы.

Библиография

1. Мохат П.М. Правосубъектность искусственного интеллекта в сфере права интеллектуальной собственности: гражданско-правовые проблемы: монография. М.: Юнити-Дана, 2018. 256 с.
2. Шестак В.А., Волеводз А.Г. Современные потребности правового обеспечения искусственного интеллекта: взгляд из России // Всероссийский криминологический журнал. 2019. Т. 13. № 2. С. 197-206. DOI: 10.17150/2500-4255.2019.13(2).197-206. EDN: SZXCZM.
3. Понкин И.В., Редькина А.И. Искусственный интеллект с точки зрения права // Вестник РУДН. Серия: Юридические науки. 2018. Т. 22. № 1. С. 91-109. DOI: 10.22363/2313-

2337-2018-22-1-91-109. EDN: YVXKVA.
4. Незнамов А.В., Наумов В.Б. Стратегия регулирования робототехники и киберфизических систем // Закон. 2018. № 2. С. 69-90. EDN: TIGDET.
5. Тихомиров Ю.А., Крысенкова Н.Б., Нанба С.Б., Маргушева Ж.А. Робот и человек: новое партнерство? // Журнал зарубежного законодательства и сравнительного правоведения. 2018. № 5. С. 5-10. DOI: 10.12737/art.2018.5.1. EDN: MGFCHR.
6. Бостром Н. Искусственный интеллект. Этапы. Угрозы. Стратегии. М.: Манн, Иванов и Фербер, 2016. 496 с.
7. Хисамова З.И., Бегишев И.Р. Уголовная ответственность и искусственный интеллект: теоретические и прикладные аспекты // Всероссийский криминологический журнал. 2019. Т. 13. № 4. С. 564-574. DOI: 10.17150/2500-4255.2019.13(4).564-574. EDN: QOFRXQ.
8. Чеботарева А.А. Правовое обеспечение информационной безопасности личности в условиях развития технологий искусственного интеллекта // Юридический вестник ДГУ. 2019. Т. 31. № 3. С. 114-118.
9. Юрьева А.С. Искусственный интеллект как угроза национальной безопасности // Вестник Московского университета. Серия 12: Политические науки. 2020. № 1. С. 57-67.
10. Карцхия А.А. Искусственный интеллект как средство управления в условиях глобальных рисков // Гуманитарные, социально-экономические и общественные науки. 2019. № 9. С. 130-133.
11. Яковлева Е.О. Методики психологического диагностирования осужденных / Е. О. Яковлева // Уголовное право в эволюционирующем обществе: проблемы и перспективы: Сборник научных статей по материалам IX очной Международной научно-практической конференции, Курск, 04-06 октября 2018 года. Том Часть 1. – Курск: Юго-Западный государственный университет, 2019. – С. 375-379. – EDN XRDRVI.
12. Яковлева Е.О., Лунева К.А., Тарыкин В.К. Перспективы использования искусственного интеллекта в правоохранительной деятельности // Полицейская деятельность. 2025. № 2. С. 1-14. DOI: 10.7256/2454-0692.2025.2.71931 EDN: FPKMKL URL: https://nbpublish.com/library_read_article.php?id=71931
13. Яковлева Е.О., Маслова А.В. Искусственный интеллект и уголовная ответственность: проблемы соотношения // Уголовное право в эволюционирующем обществе: Сборник научных статей научно-практической конференции молодых учёных и студентов, Курск, 30 мая 2025 года. – Курск: ЗАО "Университетская книга", 2025. – С. 107-112. – EDN HLYSFV.
14. Ильин А.В. Искусственный интеллект как инструмент современных информационных войн: угрозы для национальной безопасности / А. В. Ильин // Время науки: актуальные вопросы, достижения и инновации: сборник статей VII Международной научно-практической конференции, Пенза, 10 июня 2025 года. – Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2025. – С. 331-334. – EDN WOWIWX.
15. Никеров Д.М. Искусственный интеллект, как актуальная угроза национальной безопасности / Д. М. Никеров // Право и государство: теория и практика. – 2025. – № 6. – С. 578-581. – DOI: 10.47643/1815-1337_2025_6_578. – EDN FFNCHC.
16. Малых Е.Б. Угрозы, связанные с развитием технологий искусственного интеллекта / Е. Б. Малых // Трансформация бизнеса и общественных институтов в условиях цифровизации экономики: сборник научных трудов VII Национальной (российской) научно-практической конференции, Санкт-Петербург, 17-18 апреля 2025 года. – Санкт-Петербург: Санкт-Петербургский университет технологий управления и экономики, 2025. – С. 72-74. – EDN MQKNZM.
17. Бохан А.П. Ответственность за киберпреступления в международных и Российских нормах / А.П. Бохан // Мир криминалистики. 2025. № 1. С. 37-41. EDN: QKOIHM

18. Лаптев В.А. Понятие искусственного интеллекта и юридическая ответственность за его работу // Право. Журнал Высшей школы экономики. № 2. 2019. С. 79-102. DOI: 10.17323/2072-8166.2019.2.79.102 EDN: GQATHO

Результаты процедуры рецензирования статьи

Рецензия выполнена специалистами Национального Института Научного Рецензирования по заказу ООО "НБ-Медиа".
В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов можно ознакомиться здесь.

Рецензия на статью «ИИ как криминогенный фактор: проблемы квалификации и тактики расследования»

Предметом исследования являются общественные отношения, возникающие в связи с использованием технологий искусственного интеллекта (ИИ) в преступной деятельности, а также системные проблемы уголовного и уголовно-процессуального законодательства Российской Федерации, связанные с квалификацией таких деяний и тактикой их расследования.

Методология исследования носит комплексный, межотраслевой характер. Применялись формально-юридический, сравнительно-правовой методы (анализ опыта ЕС, США, Китая), социолого-правовые методы, а также криминалистические методы моделирования способов совершения преступлений и тактических алгоритмов расследования. Для анализа правовых пробелов использовались статистические данные МВД и СК РФ.

Актуальность темы неоспорима. Скорость развития технологий ИИ значительно опережает темпы адаптации правовых механизмов, что создает «нормативный вакуум», которым пользуются злоумышленники. Рост числа IT-преступлений, совершаемых с использованием элементов автоматизации или ИИ (рост мошенничеств с deepfake в 1,7 раза за 2023 г.), подчеркивает острую практическую значимость исследования для правоохранительной деятельности и обеспечения национальной безопасности.

Научная новизна заключается в разработке конкретных предложений по квалификации преступлений (например, введение нового квалифицирующего признака для мошенничества), предложении нового легального определения ИИ для целей уголовного права, а также в формулировании тактических рекомендаций по сбору и закреплению доказательств (алгоритмических моделей, журналов аудита) в рамках УПК РФ. Вводится классификация систем ИИ по степени автономности и риска, которая может служить основой для дифференцированного правового регулирования в России.

Статья отличается логичной структурой и последовательным изложением материала: от теоретических основ и зарубежного опыта к конкретным проблемам российского законодательства и практическим рекомендациям. Язык изложения является научным, четким и аргументированным. Содержание глубоко раскрывает заявленную тему, предлагая системный анализ и обоснованные решения.

Библиографический список обширен и актуален, включает работы ведущих российских и зарубежных экспертов в области права ИИ, кибербезопасности и криминалистики (П.М.

Морхат, В.А. Шестак, А.Г. Волеводз и др.). Это демонстрирует глубокое погружение автора в современную научную дискуссию.

Автор активно апеллирует к оппонентам, рассматривая две ключевые позиции в правовой доктрине: достаточность существующих норм (А.П. Бохан) и необходимость специального регулирования из-за уникальных свойств ИИ (В.А. Лаптев). Автор занимает обоснованную позицию в пользу второго подхода, аргументируя это стиранием прямой причинно-следственной связи при автономном поведении ИИ.

Выводы статьи носят конструктивный характер и призывают к концептуальному обновлению законодательства.

Материал представляет значительный интерес для широкой читательской аудитории.

Основные замечания:
1. Вопрос о субъекте ответственности (разработчик, оператор, владелец) остается открытым и вызывает споры в научном сообществе. Подход автора, хоть и обоснован, может быть подвергнут критике за усложнение доказывания вины.
2. Автор предлагает классификацию по уровням риска (высокий, неприемлемый и т.д.), в тексте нет четких, юридически прописанных критериев, по которым можно однозначно отнести ту или иную систему к определенной категории.
Указанные недостатки не влияют на общую оценку работы и может быть рекомендована к публикации.