

УДК 343

DOI: 10.34670/AR.2026.62.75.073

Обеспечение безопасности эксплуатации искусственного интеллекта: уголовно-правовой аспект

Курносова Валерия Михайловна

Аспирант,
Всероссийский государственный университет
юстиции (РПА Минюста России),
117638, Российская Федерация, Москва, ул. Азовская, 2, корп. 1;
e-mail: lerakurnosova@yandex.ru

Аннотация

Статья посвящена проблеме уголовно-правового регулирования общественно опасных деяний, связанных с эксплуатацией автономных систем искусственного интеллекта. Цель исследования — разработка концептуальной модели уголовной ответственности за причинение вреда высокоавтоматизированными ИИ-системами в условиях отсутствия непосредственного умышленного управления оператором. Автор выделяет два вектора интеграции ИИ в общественные отношения: информационно-когнитивное воздействие (эмпатийные чат-боты) и физическое воздействие (высокоавтоматизированные транспортные средства). Установлена недостаточность действующих норм УК РФ (ст. 238, 264) для охвата специфики автономных систем ввиду проблем определения специального субъекта, субъективной стороны и критериев опасности. Критически оценивается стратегия фрагментарного регулирования через введение точечных составов, способная привести к объективному вменению и избыточной казуистичности закона. Выявлены законодательные уголовно-правовые риски, обусловленные нормативной неопределенностью и дефицитом технического регулирования безопасности ИИ. Предложена унифицированная конструкция ответственности, основанная на: специальном субъекте-гаранте безопасности; необеспечении контура безопасности как объективной стороне; двойной форме вины; материальном составе преступления. Обоснована необходимость предварительной разработки императивных технических регламентов (ГОСТ, федеральное законодательство) как условия криминализации нарушений правил эксплуатации ИИ.

Для цитирования в научных исследованиях

Курносова В.М. Обеспечение безопасности эксплуатации искусственного интеллекта: уголовно-правовой аспект // Вопросы российского и международного права. 2026. Том 16. № 4А. С. 602-610. DOI: 10.34670/AR.2026.62.75.073

Ключевые слова

Искусственный интеллект, уголовная ответственность, автономные системы, высокоавтоматизированные транспортные средства, нарушение правил безопасности эксплуатации, уголовно-правовые риски, специальный субъект преступления, двойная форма вины, информационно-когнитивное воздействие, техническое регулирование.

Введение

Системы искусственного интеллекта (ИИ) стремительно эволюционируют от инструментального применения к высокоавтоматизированному функционированию. Ранее в фокусе уголовно-правовых исследований находилось использование ИИ как средства совершения преступления непосредственным злоумышленником (генерация дипфейков, вредоносного кода, фишинговые атаки, манипулирование рынком) [Курносова, 2025; Талан, 2025; Ващенко, 2017]. Однако на периферии доктринального анализа остаются общественно опасные деяния, не связанные с умышленными действиями конкретного оператора в момент причинения вреда.

На сегодняшний день ИИ-агенты автономно участвуют в цифровых правоотношениях: генерируют контент для социальных сетей, ведут высокочастотную торговлю на криптобиржах, создают медиа-материалы без участия человека [Гришин, 2020; Nazer, Savadattimath, Kumari, 2025]. Ключевая проблема заключается в том, что такие агенты способны причинять вред охраняемым уголовным законом интересам, но сам ИИ не может являться субъектом преступления ввиду отсутствия воли (субстрата вины). Следовательно, действия автономных систем, причиняющих вред, необходимо рассматривать через призму нарушения правил обеспечения безопасности их эксплуатации, где ИИ выступает не субъектом, а источником повышенной опасности [ИИ торгуют криптовалютой, 2025].

Основная часть

1. Проблема применимости действующих норм УК РФ в рамках активной цифровой динамики

Ранее сделан вывод о том, что защита общественных отношений может быть осуществлена посредством применения уже существующих составов УК РФ. Такой вывод сделан на основе анализа зарубежной судебной практики Гарсия против Character Technologies Inc. [Grok запретили создавать обнаженные фото, 2026]].

Анализ данного прецедента позволяет выделить следующие характеристики общественной опасности подобных ИИ-продуктов:

- предназначен для массового пользователя;
- направлен на эксплуатацию естественных человеческих потребностей (общение) и «паразитирование» на уязвимостях современного общества (одиночество, депрессия, возрастные кризисы);
- даже с учетом цифровой природы, может вызывать общественно-опасное последствие в объективной реальности (ухудшение психологического состояния, самоубийство).

Наиболее близким составом преступления в действующем УК РФ является ст. 238 (Производство, хранение, перевозка либо сбыт товаров и продукции, выполнение работ или оказание услуг, не отвечающих требованиям безопасности). Однако анализ показывает ее недостаточную эффективность для регулирования автономных алгоритмических систем:

1) Проблема специального субъекта.

Согласно Постановлению Пленума Верховного Суда Российской Федерации от 25.06.2019 № 18 «О судебной практике по делам о преступлениях, предусмотренных статьей 238 Уголовного кодекса Российской Федерации» [Постановление Пленума ВС РФ № 18, 2019]. субъектом преступления является лицо, фактически осуществляющее производство или оборот

продукции. В высокотехнологичных продуктах цепочка создания стоимости размыта: от разработчика нейросети до аналитика данных и конечного вендора. При ошибке алгоритма, заложенной на этапе обучения («data poisoning» (кибератака на данные обучения ИИ в целях их отравления вредоносной информацией) [Nazer, Savadattimath, Kumari, 2025] или архитектурный просчет), применение традиционного подхода к определению субъекта становится невозможным. Кто фактически осуществляет выполнение работ, если ошибку допустил алгоритм на этапе обучения?

2) Проблема субъективной стороны.

Деяния по ст. 238 УК РФ характеризуются умышленной формой вины (п. 6 ППВС от 25.06.2019 №18). Разработчик ИИ-сервиса, как правило, уверен в безопасности продукта. Если ИИ совершает ошибку («галлюцинирует»), это деяние вероятнее всего следует квалифицировать как неосторожность (ст. 109, 118 УК РФ) либо как невиновное причинение вреда- казус (ст. 28 УК РФ). Конструкция ст. 238 УК РФ не охватывает специфику вероятностной природы ошибок нейросетей.

3) Критерий опасности.

Толкование «реальной опасности» через призму «обычных условий» (ППВС № 18) создает правовой тупик. Высокотехнологичные системы характеризуются пробабиллизмом (вероятностным характером вывода) [Krause, Hübotter, 2025]. Оценить «качество» алгоритма через «обычные условия» невозможно, так как риск часто скрыт в самой архитектуре нейросети (проблема «Black Box») [Krause, Hübotter, 2025].

II. Уголовно-правовой анализ векторов интеграции искусственного интеллекта в общественные отношения

Невозможность универсальной квалификации деяний по ст. 238 УК РФ обусловлена гетерогенной природой самих технологий. Высокоавтоматизированные системы ИИ интегрированы в общественные отношения в рамках двух качественно разнородных векторов, каждый из которых порождает самостоятельную уголовно-правовую проблему:

1. Информационно-когнитивное воздействие (сфера антропоморфной коммуникации).

В данном случае эмпатийные алгоритмы (чат-боты) симулируют межличностный диалог, удовлетворяя социальные потребности человека. Однако бизнес-модели, ориентированные на максимальное вовлечение (удержание) уязвимых пользователей и лишённые встроенных контуров психологической безопасности, генерируют риски причинения латентного вреда. Данный тезис находит подтверждение в материалах дела *Garcia v. Character Technologies Inc.* Специфика общественной опасности заключается в том, что вредоносное последствие наступает не одномоментно, а кумулятивно — как результат длительного деструктивного информационного воздействия на психику. Это существенно затрудняет установление прямой причинно-следственной связи и требует проведения комплексных психолого-психиатрических и технических экспертиз.

2. Физическое воздействие (сфера функциональной автономии в материальном мире).

Речь идет о высокоавтоматизированных транспортных средствах (ВАТС) и иных робототехнических системах, функционирующих в физической реальности без непосредственного управления человеком [11]. В отличие от первого вектора, общественно опасные последствия (вред жизни, здоровью, имуществу) наступают здесь мгновенно — в момент нарушения алгоритмом правил безопасности (например, ПДД). Ключевая правовая проблема заключается в дефекте субъектного состава: диспозиция ст. 264 УК РФ указывает на «лицо, управляющее транспортным средством», которое в условиях полной автономности

системы фактически отсутствуют.

III. Тенденции уголовно-правового регулирования в сфере искусственного интеллекта: преимущества и недостатки

Для устранения законодательного пробела в доктрине предлагаются точечные решения. Так, В.Н. Куфлева и соавторы аргументируют необходимость дополнения уголовного закона ст. 264.1 УК РФ, устанавливающей ответственность за нарушение правил эксплуатации беспилотных транспортных средств, а также за выпуск в эксплуатацию систем управления с техническими неисправностями [Курсаев, 2020]. Данный подход имеет очевидное преимущество: он позволяет оперативно взять под охрану конкретные общественные отношения, определив непосредственный объект.

Однако стратегия фрагментарного регулирования обладает системными недостатками:

1) Риск объективного вменения.

Техногенная природа таких преступлений еще до конца не изучена — на этапе изучения остается причинно-следственная связь между ненадлежащим качеством разработки и «галлюцинированием» ИИ. Отсюда возникает риск объективного вменения, когда ответственность наступает по факту причинения вреда, а не по направленности умысла и возможности осознанного контроля над вероятными последствиями.

2) Избыточная казуистичность.

Стремительное развитие технологий сделает норму о ВАТС, устаревшей при появлении новых классов автономных систем (например, медицинских роботов-хирургов). Точечная криминализация ведет к необоснованному разрастанию Особенной части УК РФ и нарушению системности закона.

Мы согласны с тем, что уголовно-правовое регулирование не должно основываться на идеях законодательного «футуризма», но реактивное уголовно правовое регулирование в сфере новейших технологий может привести к возникновению уголовно-правовых рисков

IV. Технологическая неопределенность как источник уголовно-правовых рисков

Реактивное регулирование создает угрозу правовой определенности уголовного законодательства. Правовая норма должна быть ясна адресату. Если законодатель не имеет четкого представления о технологическом процессе (гипотеза), он не может сформулировать корректный запрет (диспозиция) [Уголовное право. Общая часть, 2008]. Законотворчество в сфере ИИ без участия технических специалистов порождает нормы с размытым содержанием. Опосредованность уголовного законодательства от реалий практики разработки может привести к появлению составов преступления, имманентно нарушающих принципы справедливости наказания и недопущение объективного вменения (ст. 5,6 УК РФ). Такое регулирование приводит к возникновению уголовно-правовых рисков.

Наиболее точно понятие современных уголовно правовых рисков вывел Соболев Н.Р.: «это обусловленная нормативной неопределённостью и технологической динамикой цифровой среды объективная вероятность деформации механизма уголовно-правовой охраны, выражающаяся либо в снижении уровня защищённости охраняемых уголовным законом общественных отношений, либо в необоснованном расширении пределов уголовной ответственности в отношении деятельности субъектов..., не обладающей достаточной степенью общественной опасности» [Соболев, 2026].

Применительно к предмету настоящего исследования уголовно-правовые риски возможно интерпретировать через предложенную автором типологию.

Законодательные (нормотворческие) риски обусловлены дефектами конструирования норм

и высокой степенью бланкетности.

1) В ст. 238 УК РФ используется категория «требования безопасности», которая отсылает к техническому регулированию. Однако в сфере ИИ (особенно генеративных моделей) требования безопасности либо малозначительны для квалификации (ГОСТ Р 59921.0—2022 – ИИ в сфере медицины), либо носят рекомендательный характер (Кодекс этики в сфере ИИ на финансовом рынке, разработанный Банком России). Это создает ситуацию правовой неопределенности: разработчик не может предвидеть, будет ли сбой нейросети (галлюцинация) расценен постфактум как нарушение требований безопасности.

2) Риск декларативности охраны. Диспозиции действующих норм (ст. 264, 109, 238 УК РФ) не охватывают специфику информационно-когнитивного воздействия. Отсутствие прямого запрета на создание алгоритмов, эксплуатирующих психологические уязвимости (по аналогии с «социальной инженерией»), приводит к тому, что общественно опасные деяния остаются вне уголовно-правового поля (дефицит защищенности).

V. Концептуальная модель уголовно-правовой охраны

Учитывая выявленные риски и природу векторов воздействия ИИ (информационно-когнитивный и физический) на общественные отношения, представляется, что попытка урегулировать данную сферу путем введения одной универсальной нормы (например, «Нарушение правил эксплуатации ИИ») является несовершенной. Такой подход нарушит родовую систематику Особенной части УК РФ, объединив посягательства на безопасность движения (гл. 27) и здоровье личности (гл. 17).

Предлагаем к рассмотрению унифицированную конструкцию ответственности, которая может быть имплементирована в профильные главы УК РФ в зависимости от сферы применения автономного агента. Данная конструкция базируется на четырех обязательных элементах:

1. Специальный субъект как гарант безопасности.

Субъектом уголовно-правовой ответственности является не разработчик кода (чьи действия отдалены от последствий) и не конечный пользователь, а лицо, принявшее решение о вводе автономной системы в эксплуатацию или о продолжении ее работы при наличии сведений о критических уязвимостях.

2. Конструкция объективной стороны.

Деяние должно заключаться не в самой ошибке алгоритма (которая может быть случайной), а в необеспечении контура безопасности. В этом смысле, перспектива появления подобных уголовно-правовых составов находится в прямой зависимости от появления точных требований к обеспечению безопасности искусственного интеллекта (ГОСТ, Роскомнадзор, Минцифры или даже специального федерального законодательства в сфере). Уголовная ответственность невозможна до появления четких технических регламентов для разработки и безопасности ИИ. Нельзя нарушить «правила безопасности», если их нет или они носят рекомендательный характер (как Кодекс этики). Это фундаментальный принцип *nullum crimen sine lege* (нет преступления без указания в законе) [Курсаев, 2020].

3. Двойная форма вины

Для исключения объективного вменения (ст. 5 УК РФ) необходима конструкция, при которой:

- по отношению к нарушению правил (выпуск сырого продукта, отключение фильтров безопасности) у субъекта имеется умысел (как правило корыстный в рамках осуществления предпринимательской деятельности);

- по отношению к наступившим последствиям (смерть, тяжкий вред) — неосторожность.

4. Материальный состав преступления.

Во избежание необоснованной криминализации научно-исследовательской или инновационной деятельности, конструирование нормы по модели формального состава, по аналогии со ст. 273 УК РФ («Создание вредоносных компьютерных программ»), недопустимо.

Автономные системы ИИ являются технологиями двойного назначения, а не заведомо криминальным инструментарием. Следовательно, уголовная ответственность (за исключением случаев административной преюдиции) должна наступать исключительно при наступлении общественно опасных последствий. При этом важно, чтобы такие последствия были четко определены и не носили абстрактный характер («существенный вред, существенное нарушение прав» - ст. 201, 285, 293 УК РФ). Предлагается использовать традиционный подход:

- тяжкий вред здоровью человека;
- смерть человека;
- крупного имущественного ущерба.

Любые нарушения правил эксплуатации, создавшие лишь угрозу причинения вреда, должны оставаться в поле административного регулирования.

При этом разграничение со ст. 273 УК РФ проводится по критерию заведомости вредоносности. Если продукт изначально создан и позиционируется как легитимный (чат-бот для общения, ВАТС для транспорта), но не обеспечена безопасность, применяются предложенные нормы о нарушении правил эксплуатации. Если же ИИ-система создана исключительно для совершения преступлений (например, автоматизированный фишинг-бот с обходом капчи), квалификация — по ст. 273 УК РФ.

Заключение

Проведенное исследование позволяет сформулировать следующие выводы.

Во-первых, действующие нормы УК РФ (ст. 238, 264) не приспособлены для регулирования общественно опасных деяний, связанных с эксплуатацией автономных ИИ-систем, ввиду проблем определения специального субъекта, субъективной стороны и критериев опасности.

Во-вторых, стратегия фрагментарного регулирования через введение точечных составов чревата риском объективного вменения и избыточной казуистичности закона, что нарушает системность уголовного законодательства.

В-третьих, уголовно-правовые риски в сфере ИИ обусловлены нормативной неопределенностью и дефицитом технического регулирования безопасности, что создает препятствия для реализации принципа *nullum crimen sine lege*.

В-четвертых, предлагаемая унифицированная конструкция ответственности, основанная на специальном субъекте-гаранте безопасности, необеспечении контура безопасности как объективной стороне, двойной форме вины и материальном составе преступления, позволяет преодолеть выявленные пробелы и может быть имплементирована в профильные главы УК РФ в зависимости от сферы применения автономного агента.

В-пятых, уголовная ответственность за нарушение правил эксплуатации ИИ должна быть поставлена в зависимость от предварительной разработки императивных технических регламентов (ГОСТ, федеральное законодательство), без которых криминализация соответствующих деяний невозможна. Любые нарушения, создавшие лишь угрозу причинения вреда, должны оставаться в поле административного регулирования.

Библиография

1. Ващенко Т. В. Финансовые инновации как элемент развития финансового сектора экономики // Азимут научных исследований: экономика и управление. 2017. Т. 6, № 4(21). С. 75-78.
2. Грачева Ю. В., Арямов А. А. Роботизация и искусственный интеллект: уголовно-правовые риски в сфере общественной безопасности // Актуальные проблемы российского права. 2020. Т. 15, № 6 (115). С. 169–178.
3. Гришин А.А. К вопросу о правовом регулировании высокоавтоматизированных транспортных средств как источника повышенной опасности // Экономика. Право. Общество. 2020. Т. 5, № 2 (22). С. 119–126.
4. Grok запретили создавать обнаженные фото: социальная сеть «X» вводит ограничение. – URL: <https://www.vedomosti.ru/technology/news/2026/01/14/1169262-grok-zapretili-sozdavat> .
5. ИИ торгуют криптой: высокоавтоматизированные системы на финансовых рынках. – URL: <https://www.vedomosti.ru/society/articles/2025/11/05/1151995-ii-torguyut-kripto> .
6. Кочои С. М. Уголовно-правовые риски использования беспилотных транспортных средств // Актуальные проблемы российского права. 2021. Т. 16, № 7 (128). С. 116–127.
7. Курносова В.М. Преступления против общественной нравственности, совершаемые с использованием технологии дипфейк // Юридическая наука. 2025. № 6. С. 112–118.
8. Курсаев А.В. Принцип nullum crimen sine lege в российском уголовном праве // Вестник экономической безопасности. 2020. № 2. С. 138–144.
9. Куфлева В.Н., Соболев Д.В., Фирсов В.В. Проблемные аспекты квалификации преступлений с использованием беспилотного транспортного средства // Человек: преступление и наказание. 2019. Т. 27, № 3. С. 314–319.
10. Постановление Пленума Верховного Суда Российской Федерации от 25.06.2019 № 18 «О судебной практике по делам о преступлениях, предусмотренных статьей 238 Уголовного кодекса Российской Федерации» // Бюллетень Верховного Суда РФ. 2019. № 8.
11. Соболев Н.Р. Юридическая природа и типология уголовно-правовых рисков оборота персональных данных // Юридическая наука. 2026. № 2. С. 320-323.
12. Талан А.С., Талан М.В. Преступления, совершаемые с использованием искусственного интеллекта: анализ рисков и правовые перспективы // Вестник экономики, права и социологии. 2025. № 3. С. 84–89.
13. Уголовное право. Общая часть : учебник / под ред. Л.В. Иногамовой-Хегай, А.И. Рапога, А.И. Чучаева. – 2-е изд., перераб. и доп. – М.: Контракт: ИНФРА-М, 2008. – 560 с.
14. Blattner L., Nelson S., Spiess J. Unpacking the Black Box: Regulating Algorithmic Decisions. – URL: <https://arxiv.org/pdf/2110.03443> .
15. Garcia v. Character Technologies, Inc. No. 6:24-cv-1903-A CC-UAM. – URL: <https://www.courtlistener.com/docket/69300919/garcia-v-character-technologies-inc/> .
16. Krause A., Hübotter J. Probabilistic Artificial Intelligence. – 2025. – arXiv:2502.05244. – URL: <https://arxiv.org/abs/2502.05244>.
17. Nazer B., Savadattimath P., Kumari S. Data Poisoning Attacks and Defenses in Machine Learning: A Survey with Focus on Computer Vision // 2025 IEEE International Conference on Computer Vision and Machine Intelligence (CVMI). – Rourkela, India, 2025. – DOI: 10.1109/CVMI66673.2025.11337510.

Ensuring the Safety of Artificial Intelligence Operation: Criminal Law Aspect

Valeriya M. Kurnosova

Postgraduate Student,
All-Russian State University of Justice
(RPA of the Ministry of Justice of Russia),
117638, 2, bldg. 1, Azovskaya str., Moscow, Russian Federation;
e-mail: lerakurnosova@yandex.ru

Abstract

The article is devoted to the problem of criminal law regulation of socially dangerous acts related

to the operation of autonomous artificial intelligence systems. The aim of the study is to develop a conceptual model of criminal liability for causing harm by highly automated AI systems in the absence of direct intentional control by the operator. The author identifies two vectors of AI integration into social relations: information-cognitive impact (empathic chatbots) and physical impact (highly automated vehicles). The insufficiency of the current norms of the Criminal Code of the Russian Federation (Articles 238, 264) to cover the specifics of autonomous systems due to the problems of determining the special subject, the subjective side, and the criteria of danger is established. The strategy of fragmentary regulation through the introduction of specific *corpus delicti*, capable of leading to objective imputation and excessive casuistry of the law, is critically assessed. Legislative criminal law risks caused by regulatory uncertainty and a deficit of technical regulation of AI safety are identified. A unified construction of liability is proposed, based on: a special subject — the safety guarantor; failure to ensure the safety contour as the objective side; a double form of guilt; material *corpus delicti*. The necessity of preliminary development of mandatory technical regulations (GOST, federal legislation) as a condition for the criminalization of violations of AI operation rules is substantiated.

For citation

Kurnosova V.M. (2026) Obespechenie bezopasnosti ekspluatatsii iskusstvennogo intellekta: ugovovno-pravovoy aspekt [Ensuring the Safety of Artificial Intelligence Operation: Criminal Law Aspect]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 16 (4A), pp. 602-610. DOI: 10.34670/AR.2026.62.75.073

Keywords

Artificial intelligence, criminal liability, autonomous systems, highly automated vehicles, violation of safety operation rules, criminal law risks, special subject of crime, double form of guilt, information-cognitive impact, technical regulation.

References

1. Blattner, L., Nelson, S., & Spiess, J. (2026). Unpacking the black box: Regulating algorithmic decisions. arXiv. Retrieved from <https://arxiv.org/pdf/2110.03443>
2. Garcia v. Character Technologies, Inc., No. 6:24-cv-1903-ACC-UAM. (n.d.). CourtListener. Retrieved from <https://www.courtlistener.com/docket/69300919/garcia-v-character-technologies-inc/>
3. Gracheva, Yu. V., & Aryamov, A. A. (2020). Robotizatsiya i iskusstvennyy intellekt: ugovovno-pravovye riski v sfere obshchestvennoy bezopasnosti [Robotization and artificial intelligence: criminal-legal risks in the sphere of public safety]. *Aktualnye problemy rossiyskogo prava*, 15(6), 169-178.
4. Grishin, A. A. (2020). K voprosu o pravovom regulirovanii vysokoavtomatizirovannykh transportnykh sredstv kak istochnika povyshennoy opasnosti [On the legal regulation of highly automated vehicles as a source of increased danger]. *Ekonomika. Pravo. Obshchestvo*, 5(2), 119-126.
5. Grok zapretili sozdavat obnazhennye foto: sotsialnaya set "X" vvodit ogranichenie [Grok banned from creating nude photos: social network "X" introduces restrictions]. (2026). *Vedomosti*. Retrieved from <https://www.vedomosti.ru/technology/news/2026/01/14/1169262-grok-zapretili-sozdavat>
6. II torguyut kriptoy: vysokoavtomatizirovannye sistemy na finansovykh rynkakh [AI trades crypto: highly automated systems in financial markets]. (2025). *Vedomosti*. Retrieved from <https://www.vedomosti.ru/society/articles/2025/11/05/1151995-ii-torguyut-kriptoi>
7. Kochoi, S. M. (2021). Ugolovno-pravovye riski ispolzovaniya bespilotnykh transportnykh sredstv [Criminal-legal risks of using unmanned vehicles]. *Aktualnye problemy rossiyskogo prava*, 16(7), 116-127.
8. Krause, A., & Hübotter, J. (2025). Probabilistic artificial intelligence. arXiv:2502.05244. Retrieved from <https://arxiv.org/abs/2502.05244>
9. Kufleva, V. N., Sobolev, D. V., & Firsov, V. V. (2019). Problemnye aspekty kvalifikatsii prestupleniy s ispolzovaniem bespilotnogo transportnogo sredstva [Problematic aspects of the qualification of crimes involving the use of an

- unmanned vehicle]. *Chelovek: prestuplenie i nakazanie*, 27(3), 314-319.
10. Kurnosova, V. M. (2025). Prestupleniya protiv obshchestvennoy нравstvennosti, sovershaemye s ispolzovaniem tekhnologii deepfake [Crimes against public morality committed using deepfake technology]. *Yuridicheskaya nauka*, 6, 112-118.
 11. Kursae, A. V. (2020). Printsip nullum crimen sine lege v rossiyskomugolovnomprave [The principle of nullum crimen sine lege in Russian criminal law]. *Vestnik ekonomicheskoy bezopasnosti*, 2, 138-144.
 12. Nazer, B., Savadattimath, P., & Kumari, S. (2025). Data poisoning attacks and defenses in machine learning: A survey with focus on computer vision. In 2025 IEEE International Conference on Computer Vision and Machine Intelligence (CVMI). Rourkela, India. <https://doi.org/10.1109/CVMI66673.2025.11337510>
 13. Resolution of the Plenum of the Supreme Court of the Russian Federation No. 18 of June 25, 2019 "On Judicial Practice in Cases of Crimes under Article 238 of the Criminal Code of the Russian Federation". (2019). *Bulletin of the Supreme Court of the Russian Federation*, 8.
 14. Sobolev, N. R. (2026). Yuridicheskaya priroda i tipologiya ugovolno-pravovykh riskov oborota personalnykh dannykh [Legal nature and typology of criminal-law risks of personal data circulation]. *Yuridicheskaya nauka*, 2, 320-323.
 15. Talan, A. S., & Talan, M. V. (2025). Prestupleniya, sovershaemye s ispolzovaniem iskusstvennogo intellekta: analiz riskov i pravovye perspektivy [Crimes committed with the use of artificial intelligence: risk analysis and legal prospects]. *Vestnik ekonomiki, prava i sotsiologii*, 3, 84-89.
 16. *Ugolovnoe pravo. Obshchaya chast* [Criminal law. General part]. (2008). (L. V. Inogamova-Khegay, A. I. Rarog, & A. I. Chuchaev, Eds.) (2nd ed.). Moscow: Kontrakt: INFRA-M.
 17. Vashchenko, T. V. (2017). Finansovye innovatsii kak element razvitiya finansovogo sektora ekonomiki [Financial innovations as an element of development of the financial sector of the economy]. *Azimut nauchnykh issledovaniy: ekonomika i upravlenie*, 6(4), 75-78.