Научная статья
УДК 343.01

УГОЛОВНО-ПРАВОВАЯ КВАЛИФИКАЦИЯ НЕПРАВОМЕРНОГО ВОЗДЕЙСТВИЯ НА ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ БЕСПИЛОТНЫХ ТРАНСПОРТНЫХ СРЕДСТВ

Мария Вячеславовна Талан,
Казанский (Приволжский) федеральный университет,
Университет управления «ТИСБИ», Казань, Россия,
mtalan@inbox.ru

Наталья Андреевна Каменова,
Казанский юридический институт МВД России, Казань, Россия,
kamenova.nat@mail.ru

Аннотация

Введение: в статье рассматриваются актуальные вопросы, касающиеся проблем уголовно-правовой квалификации деяний, направленных на преступные посягательства систем искусственного интеллекта беспилотных транспортных средств, повлекшие дорожно-транспортные происшествия.

Материалы и методы: основу исследования составили логический метод, а также метод анализа. В качестве материалов исследования выступили действующие нормативно-правовые акты Российской Федерации.

Результаты исследования: установлено, что, несмотря на безусловные преимущества беспилотных транспортных средств (далее – БТС) в радикальном снижении аварийности и смертности на дорогах, их использование порождает новые юридические коллизии. Действующий Уголовный кодекс Российской Федерации (далее – УК РФ) не содержит положений, позволяющих квалифицировать некоторые современные виды кибервоздействий на системы искусственного интеллекта беспилотных транспортных средств. Отсутствие подобных норм создаёт правовой пробел, обусловливающий необходимость законодательного закрепления в УК РФ отдельного состава преступления, регламентирующего уголовную ответственность за совершение кибервоздействия на беспилотные транспортные средства, повлекшего дорожно-транспортное происшествие с тяжкими последствиями.

Обсуждение и заключения: авторами статьи предложены направления совершенствования действующего законодательства, направленные на усиление правовой защиты общественной безопасности в сфере дорожного движения и предотвращение дорожно-транспортных происшествий, вызванных кибервоздействиями на системы искусственного интеллекта беспилотных транспортных средств.

Ключевые слова: беспилотное транспортное средство; искусственный интеллект; кибератака; дорожно-транспортное происшествие; смертельный исход; состязательные атаки; киберпреступность; компьютерная информация

Для цитирования: Талан М.В., Каменова Н.А. Уголовно-правовая квалификация неправомерного воздействия на искусственный интеллект беспилотных транспортных средств // Вестник Казанского юридического института МВД России. 2026. Т. 17. № 1 (63). С. 151 – 159.

Scientific article
UDC 343.01

CRIMINAL LAW CLASSIFICATION OF UNLAWFUL INTERFERENCE WITH THE ARTIFICIAL INTELLIGENCE OF UNMANNED VEHICLES

Maria Vyacheslavovna Talan,
Kazan (Volga Region) Federal University,
University of Management "TISBI", Kazan, Russia,
mtalan@inbox.ru

Natalya Andreevna Kamenova,
Kazan Law Institute of the Ministry of Internal Affairs of Russia, Kazan, Russia,
kamenova.nat@mail.ru

Abstract

Introduction: this article examines current issues related to the criminal law classification of acts aimed at criminally infringing the artificial intelligence systems of unmanned vehicles, resulting in traffic accidents.

Materials and Methods: the study was based on a logical and analytical method. Current legal and regulatory acts of the Russian Federation served as the research materials.

Results: it was established that, despite the undeniable advantages of unmanned vehicles (hereinafter referred to as UAVs) in dramatically reducing road accidents and fatalities, their use creates new legal conflicts. The current Criminal Code of the Russian Federation (hereinafter referred to as the CCRF) does not contain provisions to qualify certain modern types of cyber-influence on the artificial intelligence systems of unmanned vehicles. This lack of such provisions creates a legal gap, necessitating the legislative establishment of a separate offense in the CCRF regulating criminal liability for cyber-influence on unmanned vehicles resulting in a traffic accident with serious consequences.

Discussion and Conclusions: the authors of this article propose ways to improve current legislation aimed at strengthening legal protections for public safety in road traffic and preventing road accidents caused by cyberattacks on the artificial intelligence systems of unmanned vehicles.

Keywords: unmanned vehicle; artificial intelligence; cyberattack; road accident; fatality; adversarial attacks; cybercrime; computer information

For citation: Talan M.V., Kamenova N.A. Criminal Law Classification of Unlawful Interference with the Artificial Intelligence of Unmanned Vehicles. Bulletin of the Kazan Law Institute of MIA of Russia. 2026;17(1):151-159. (In Russ.).

Введение

Современная эпоха характеризуется беспрецедентными темпами технологического прогресса, ключевым элементом которого является повсеместное внедрение систем искусственного интеллекта (далее – ИИ). Масштаб этих преобразований был точно охарактеризован Президентом Российской Федерации В.В. Путиным, который 19 ноября 2025 года выступая на пленарном заседании конференции «Путешествие в мир искусственного интеллекта» заявил, что ИИ является «фундаментальным технологическим переходом во всей системе управления»[1]. Это утверждение в полной мере применимо и к сфере транспорта, где одним из наиболее значимых и перспективных направлений является разработка и внедрение беспилотных транспортных средств (далее – БТС)[2], функциониру-

[1] Владимир Путин об ИИ: «Это фундаментальный технологический переход во всей системе управления». URL: https://www.business-gazeta.ru/article/657048 (дата обращения: 10.01.2026).

[2] Согласно Концепции обеспечения безопасности дорожного движения с участием беспилотных транспортных средств на автомобильных дорогах общего пользования, утвержденной Распоряжением Правительства Российской Федерации от 25.03.2020 № 724-р, беспилотное транспортное средство – высоко- или полностью автоматизированное транспортное сред-

ющих под управлением систем искусственного интеллекта. Потенциал БТС в радикальном снижении аварийности и смертности на дорогах за счет исключения человеческого фактора и оптимизации логистических процессов является предметом широкого научного и практического интереса. Вместе с тем, наряду с ожидаемыми преимуществами, внедрение БТС сопряжено с возникновением ряда комплексных вызовов и угроз, одной из которых являются целенаправленные кибератаки на ИИ-системы БТС, способные привести к утрате функционального контроля и, как следствие, к дорожно-транспортным происшествиям с тяжкими последствиями.

Обзор литературы

Для российской уголовно-правовой доктрины проблематика преступных посягательств на функционирование систем искусственного интеллекта беспилотных транспортных средств представляет собой сравнительно новую область исследований. В отечественной литературе вопросы, непосредственно связанные с противоправными вмешательствами в работу интеллектуальных систем и их последствиями для безопасности дорожного движения, активно исследуются в работах А.И. Коробеева, А.И. Чучаева, Р.И. Дремлюги, Д.Е. Намиота. Правовые аспекты внедрения технологий ИИ в публичной сфере, включая анализ технических и правовых рисков, рассматриваются в трудах М.В. Талан, С.А. Талан, А.В. Русскевича, В.В. Хилюты, Е.А. Чехониной, В.В. Костюмова. Данные исследования позволяют проанализировать способы совершения преступлений в сфере искусственного интеллекта и предложить научно-обоснованные меры по их предотвращению.

Материалы и методы

В ходе исследования деструктивных кибервоздействий на системы искусственного интеллекта беспилотных транспортных средств применялись логический метод и метод анализа, что позволило системно изучить феномен неправомерного вмешательства в работу искусственного интеллекта беспилотных транспортных средств посредством кибератак. Также использовался системный подход для рассмотрения объекта исследования как целостной киберфизической системы, уязвимости которой носят комплексный характер.

Результаты исследования

Анализ действующего законодательства Российской Федерации свидетельствует о том, что уголовно-правовые нормы, сформированные в иной технологической парадигме, не в полной мере охватывают специфику подобных преступлений, совершаемых в киберфизическом пространстве. В связи с этим в рамках научной доктрины обоснованно высказывается позиция, согласно которой «уголовное право не может идти впереди «телеги», потому что если новые отношения еще не сложились и не понятно, о чем вообще идет речь, то и формулировать запрет в этой области весьма «чревато» [1, с. 125]. Безусловно, поспешное и недостаточно продуманное нормотворчество в столь динамично развивающейся сфере сопряжено с риском создания неэффективных или даже контрпродуктивных норм. Вместе с тем, парадоксально, но отсутствие адекватного законодательного регулирования, гарантирующего правовую определенность и безопасность, выступает существенным препятствием для широкомасштабной имплементации БТС. Наглядным свидетельством данного тезиса служит тот факт, что в Российской Федерации функционирование БТС в настоящее время осуществляется в соответствии с экспериментальным режимом, лишь на отдельных, специально утверждённых территориях (таких как Москва, Санкт-Петербург, Иннополис и некоторых других)[1]. Тем самым, возникает насущная потребность в поиске оптимального баланса между необходимостью оперативного правового реагирования и риском непродуманных законодательных инициатив.

БТС представляет собой высокоинтегрированный киберфизический комплекс, где системообразующим элементом выступает искусственный интеллект. В контексте российского законодательства, согласно Указу Президента Российской Федерации от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации», искусственный интеллект определяется как комплекс технологических решений, позволяющий имитировать когнитивные функции человека и получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека или превосходящие их[2]. Применительно к беспилотным транспортным средствам данный комплекс реше-

ство, функционирующее без вмешательства человека (в беспилотном режиме).

[1] Об установлении экспериментального правового режима в сфере цифровых инноваций и утверждении Программы экспериментального правового режима в сфере цифровых инноваций по предоставлению транспортных услуг с использованием высокоавтоматизированных транспортных средств на территориях отдельных субъектов Российской Федерации: постановление Правительства Российской Федерации от 29 дек. 2022 г. № 2495: ред. от 21 сент. 2024 г. (в ред. 28.11.2025) // Официальный интернет-портал правовой информации. URL: http://publication.pravo.gov.ru

[2] О развитии искусственного интеллекта в Российской Федерации: Указ Президента Российской Федерации от 10.10.2019 №490 // Собрание законодательства РФ. 2019. № 41. Ст. 5700.

ний реализует критически важные для автономного движения когнитивные функции, включая восприятие окружающей среды, анализ дорожной ситуации, принятие решений и планирование траектории, стремясь при этом к максимальной безопасности и эффективности. Реализация указанных функций в БТС обеспечивается посредством скоординированной работы множества специализированных ИИ-модулей, каждый из которых выполняет конкретные задачи:

- системы восприятия (Perception Systems): осуществляют сбор и первичную обработку информации от комплекса сенсоров (камеры, радары, лидары, ультразвуковые датчики, GPS/ГЛОНАСС-приемники). ИИ-алгоритмы отвечают за распознавание объектов, их классификацию, сегментацию дорожного пространства, детектирование дорожных знаков, разметки и участников дорожного движения;

- системы слияния сенсорных данных (Sensor Fusion): высокоуровневые ИИ-алгоритмы интегрируют разнородные данные от всех сенсоров, формируя единую, когерентную и достоверную модель окружающей среды, нивелируя шумы и противоречия отдельных источников;

- системы предсказания поведения (Prediction Systems): анализируют траектории и вероятностные модели поведения других участников дорожного движения на основе ИИ-прогнозирования, что является критически важным для безопасного маневрирования;

- системы планирования (Planning Systems): ИИ генерирует оптимальные траектории движения, корректирует скорость и определяет маневры, исходя из текущей ситуации, предсказаний и соблюдения правил дорожного движения;

- системы контроля (Control Systems): осуществляют преобразование высокоуровневых команд планирования в низкоуровневые команды для исполнительных механизмов БТС (рулевое управление, тормозная система, двигатель);

- системы коммуникации (V2X Communications): ИИ управляет взаимодействием БТС с дорожной инфраструктурой, другими транспортными средствами и пешеходами, обмениваясь данными для повышения ситуационной осведомленности и координации движения.

Корректное и безопасное функционирование БТС детерминируется не только надежностью аппаратной части, но и, что особенно актуально, информационной целостностью, робастностью и точностью работы их программно-аппаратных ИИ-комплексов. Эти высокотехнологичные системы подвержены рискам как естественных технических отказов, так и целенаправленных злонамеренных кибернетических воздействий, которые, согласно Указу Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации», формируют «угрозу информационной безопасности Российской Федерации» как совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере[1].

Уязвимость БТС к подобным кибератакам представляет собой один из наиболее значимых вызовов для их безопасной эксплуатации. Масштаб и нарастающая актуальность данной проблемы подтверждаются статистическими данными: по информации ГЛОНАСС и компании «Технологии безопасности транспорта», в 2025 году зафиксирован рост числа кибератак на автомобили на 20% по сравнению с предыдущим годом, достигнув 328 зарегистрированных инцидентов за первые восемь месяцев. При этом основной причиной таких взломов эксперты называют уязвимость систем беспроводной связи[2].

БТС, как сложные киберфизические комплексы, подвержены широкому спектру кибератак, которые обуславливает существование двух различных векторов преступного воздействия.

Первый вектор – традиционные инфраструктурные атаки. Данная группа угроз направлена на программно-аппаратную базу и сетевые узлы БТС. В контексте эксплуатации беспилотного транспорта данные посягательства могут быть классифицированы следующим образом:

Внедрение вредоносного и «шпионского» ПО. Помимо деструктивных модулей, нацеленных на вывод системы из строя, широкое распространение получает практика внедрения модулей для скрытого сбора телеметрии и данных об использовании. Сбор статистики передвижений, аудио- и видеоинформации из салона позволяет преступникам сформировать подробный профиль пользователя. Например, мониторинг геолокационных данных позволяет установить точный график отсутствия владельца дома для совершения квартирных краж, а эксфильтрация аудиозаписей конфиденциальных разговоров в салоне может стать инструментом последующего шантажа.

Компрометация механизмов обновления программного обеспечения. Деструктивное воздействие на прошивку БТС может быть реализо-

[1] Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 05.12.2016 № 646 // Собрание законодательства Российской Федерации. 2016. № 50. Ст. 7074.

[2] Киберугрозы для авто с какими рисками могут столкнуться водители // URL: https://www.rbc.ru/radio/25/11/2025/6925a51f9a7947408d76ec63 (дата обращения: 10.01.2026).

вано двумя основными способами: дистанционно через уязвимости в протоколах беспроводного обновления «по воздуху» или физически, через непосредственный доступ к блоку постоянного запоминающего устройства (ПЗУ) автомобиля (например, в ходе недобросовестного сервисного обслуживания). Так, при подмене легитимного файла обновления вредоносным, в систему может быть внедрена «логическая бомба», запрограммированная на принудительное отключение систем экстренного торможения или удержание рулевого управления в определенном положении при достижении автомобилем заданной скорости.

Аппаратное вмешательство и замена компонентов. В случаях, когда программная защита системы оказывается непреодолимой для внешнего взлома, возможен сценарий физической подмены носителей информации. Это включает в себя замену блоков ПЗУ или перепайку микросхем (чипов) на аппаратном уровне. К примеру, штатный чип может быть заменен на модифицированный, который изначально содержит алгоритм игнорирования сигналов лидара о препятствиях при определенных погодных условиях. Подобная манипуляция делает классические методы антивирусной защиты неэффективными, так как аппаратная среда функционирует по искаженному сценарию, который системой безопасности воспринимается как штатный.

Реализация DDoS-атак. Искусственная перегрузка бортового компьютера или каналов связи массовым потоком фиктивных запросов. Это может привести к «информационному коллапсу» системы, потере связи с дорожной инфраструктурой («умными» светофорами) и вынужденной аварийной остановке транспортного средства.

Фишинг и социальная инженерия. Данная категория атак, на наш взгляд, является наименее вероятным вектором прямого деструктивного воздействия на алгоритмы управления БТС. Это обосновано двумя фундаментальными факторами. Во-первых, это отсутствие психоэмоциональной уязвимости искусственного интеллекта: алгоритмы лишены когнитивных искажений (страха, любопытства, доверия), на которых базируется классическая социальная инженерия. Во-вторых, это принцип архитектурной сегментации: критические узлы управления (тормозная система, рулевое управление) физически или логически изолированы от информационно-развлекательных модулей, имеющих выход в глобальную сеть.

Тем не менее, несмотря на высокую теоретическую защищенность «интеллектуального ядра» БТС, нельзя полностью исключать риск компрометации системы через периферийные каналы. В данном контексте фишинг трансформируется из метода «обмана личности» в инструмент «технической провокации», реализуемый в следующих гипотетических, но технически достижимых сценариях:

1. Компрометация через «человеческий фактор» (пользовательский уровень). В этом случае целью атаки становится не сам автомобиль, а легитимный субъект доступа (владелец или оператор). Пример: злоумышленники рассылают поддельные уведомления о необходимости верификации аккаунта в приложении для управления БТС. Ввод учетных данных на фальшивом ресурсе позволяет похитить цифровой ключ доступа. Это открывает возможность для несанкционированного отслеживания местоположения, дистанционного открытия дверей или активации систем автомобиля через штатные функции удаленного доступа.

2. «Технический фишинг» через автоматизированный поиск данных (системный уровень). Данный сценарий возможен в случае избыточной автономности информационных систем БТС. Если архитектура автомобиля предполагает самостоятельный поиск, индексацию или парсинг данных из открытых интернет-источников (например, для динамического обновления медиа-библиотеки или сбора метаданных о дорожной инфраструктуре), возникает риск столкновения с вредоносным контентом. Пример: в процессе фонового интернет-серфинга система может обратиться к специально подготовленному фишинговому ресурсу. Вместо текстовой или визуальной информации системе «скармливается» вредоносный код (эксплойт), нацеленный на уязвимости встроенного браузера или обработчика данных. В случае успеха такая атака служит «точкой входа» (прекурсором) для внедрения в операционную систему автомобиля и последующей попытки преодоления барьеров между развлекательным и управляющим контурами.

Особое место в ряду инфраструктурных угроз занимает **несанкционированный перехват дистанционного управления**. Использование технологий передачи видеопотока в реальном времени (FPV-технологии[1]) позволяет преступнику, взломав протоколы аутентификации, полностью подавить автономный режим. В этом сценарии БТС

[1] FPV (First Person View – «вид от первого лица») – технология дистанционного управления, при которой видеопоток с камеры передается в реальном времени на очки или монитор оператора. В настоящее время данная технология применяется в зоне СВО: примером служит комплекс «Тихон», созданный на базе автомобиля УАЗ, управляемый через FPV-пульт или игровую консоль (по каналам Wi-Fi/4G). В контексте киберугроз для гражданских БТС несанкционированный взлом ана-

перестает быть «самоуправляемым» и превращается в дистанционно пилотируемый «снаряд», что создает критические риски использования автономного транспорта в террористических целях для точечной доставки поражающих элементов».

Ко второму вектору атак, на наш взгляд, следует отнести специфические алгоритмические (адверсариальные) атаки.

В отличие от инфраструктурного воздействия, данный вектор направлен не на программный код или аппаратную часть, а на математическую логику работы нейросетевых моделей. Ключевой особенностью таких посягательств является отсутствие необходимости в неправомерном доступе к системе (взломе). Преступное воздействие реализуется через манипуляцию входными данными, которые ИИ-система воспринимает как легитимные, но интерпретирует искаженно. К таким особо опасным и специфическим для ИИ-систем БТС угрозам относятся состязательные атаки (adversarial attacks), которые, по определению Д.Е. Намиота, В.П. Куприяновского и А.А. Пичугова, представляют собой «модификации данных на разных этапах стандартного конвейера машинного обучения, которые либо препятствуют корректной работе модели, либо заставляют ее работать нужным атакующему способом» [2, с. 139]. Суть данных атак заключается во внесении минимальных, часто незаметных для человеческого восприятия пертурбаций во входные данные системы искусственного интеллекта (например, в изображения с камер, показания радаров или лидаров), которые, однако, провоцируют ошибочную интерпретацию со стороны автономной системы. Это может выражаться в неправильной идентификации объектов, ложном распознавании дорожных знаков, пешеходов или других транспортных средств, что приводит к дезадаптации алгоритмов принятия решений и, как следствие, к принятию некорректных решений и аварийным ситуациям. Ключевая особенность состязательных атак состоит в том, что они не требуют несанкционированного доступа к внутренним вычислительным ресурсам БТС, а воздействуют на саму логику восприятия и обработки информации ИИ через модификацию её внешних входных потоков.

«Состязательные атаки могут быть реализованы в цифровом и физическом мире. В цифровом мире характеристики целевого объекта при обучении и применении атаки не изменяются, а злоумышленник стремится использовать нестандартные конфигурации, которые могут обмануть нейронную сеть. При атаках в физическом мире после создания цифровой атаки необходимо её реализовать, например распечатать патч. При реализации атаки её эффективность может уменьшиться по следующим причинам: различия цветопередачи из цифрового в реальный мир, несовершенства устройства воспроизведения, сложные условия окружающей среды — различное освещение, тень, перекрытие целевого объекта, изменение яркости, вращение, деформация и так далее» [3, с. 11].

В контексте данной классификации цифровые состязательные атаки предполагают манипуляции непосредственно с цифровыми входными данными ИИ (например, изменение пикселей в потоковом видеоизображении), тогда как физические атаки включают преобразование цифровых пертурбаций в реальные, осязаемые воздействия на объекты окружающей среды (например, нанесение специального рисунка на дорожный знак), которые затем воспринимаются сенсорами БТС и искажаются при их оцифровке. При этом, как справедливо указывают авторы, эффективность физических атак может варьироваться в зависимости от внешних условий, таких как освещенность или угол обзора. Однако, независимо от способа реализации – будь то цифровое или физическое воздействие – ключевая особенность состязательных атак заключается в том, что они осуществляются без неправомерного доступа к внутренней компьютерной информации БТС и не предполагают внедрения вредоносного программного обеспечения в традиционном его понимании. Этот внешний характер воздействия на ИИ, направлен на обман алгоритмов восприятия и принятия решений.

Обсуждение и заключение

Исходя из проведенного анализа технических особенностей беспилотных транспортных средств и рассмотренных возможных методов воздействия на их ИИ-системы, становится очевидным, что повсеместное внедрение БТС в повседневную жизнь в перспективном будущем неизбежно породит качественно новые виды общественно опасных деяний. Эти деяния, будучи неразрывно связанными с манипуляцией информационными процессами и цифровыми данными автономных систем, безусловно, должны регулироваться уголовно-правовыми запретами. Вместе с тем действующий УК РФ не содержит соответствующих норм, которые устанавливают уголовную ответственность за преступные деяния, совершенные посредством описанных воздействий

логичных интерфейсов позволяет преступнику перехватить прямой «физический» контроль над машиной в обход всех алгоритмов безопасности ИИ.

на ИИ-системы БТС, повлекших за собой тяжкий вред здоровью или смерть человека.

Анализ действующих уголовно-правовых норм позволяет выявить основные сложности их применения к рассматриваемым деяниям:

Применение положений статьи 264 УК РФ («Нарушение правил дорожного движения и эксплуатации транспортных средств») сталкивается с проблемой определения надлежащего субъекта преступления. Данная норма традиционно предусматривает в качестве субъекта преступления физическое лицо, управляющее транспортным средством. Однако в условиях функционирования БТС, оснащенных автоматизированными системами управления, определение надлежащего субъекта уголовной ответственности при причинении тяжкого вреда или смерти в результате ДТП приобретает дискуссионный характер. А.И. Коробеев и А.И. Чучаев предлагают расширить субъектный состав, включая персонифицированных разработчиков программного обеспечения БТС, лиц, контролирующих их безопасную эксплуатацию, владельцев транспортных средств, обязанных осуществлять текущий контроль, а также лиц, находящихся в БТС и непосредственно контролирующих его функционирование [4, с. 25]. Несмотря на то, что для указанных категорий субъектов теоретически возможно выстроить систему ответственности посредством корректировки дефиниции «водитель» [5, с. 147] или иных законодательных мер [6, с. 240], квалификация действий лица, осуществившего состязательную атаку, останется неразрешенной. Это обусловлено тем, что злоумышленник, реализующий подобное преступное деяние, не подпадает ни под одну из перечисленных категорий субъектов, поскольку он не осуществляет прямое управление транспортным средством и не относится к ответственным за его штатное функционирование. Природа воздействия является внешней, направленной на дезинформацию и обман алгоритмов автономной системы, что концептуально отличается от непосредственного управления (даже с учетом информационно-телекоммуникационных способов) и выводит действия такого лица за рамки традиционных квалификационных признаков субъекта дорожно-транспортных преступлений.

Аналогичные сложности возникают и при попытке квалификации указанных деяний по нормам главы 28 УК РФ («Преступления в сфере компьютерной информации»). Основная проблема заключается в том, что рассмотренные атаки не всегда предполагают неправомерный доступ к охраняемой компьютерной информации в классическом понимании статьи 272 УК РФ или создание и использование вредоносных программ по статье 273 УК РФ. Как справедливо отмечают Р.И. Дремлюга, А.И. Коробеев «состязательные атаки способны дестабилизировать дорожное движение без неправомерного доступа к компьютерным системам» [7, с. 9]. Воздействие преимущественно осуществляется извне, посредством манипуляции входными данными или компонентами, которые искусственный интеллект воспринимает как легитимные, что приводит к принятию ошибочных решений без прямого «взлома» системы. Так, состязательные атаки искажают внешние данные, минуя несанкционированное вторжение в целевую систему. Таким образом, традиционные составы компьютерных преступлений не в полной мере охватывают механизм и объект посягательства подобных действий.

На этом фоне актуализируется дискуссия о целесообразности разработки новых уголовно-правовых норм для цифровых деяний. Некоторые эксперты, например, А.В. Русскевич, утверждают: «Все проблемы с ИИ решаются в рамках традиционных механизмов, поэтому я резко против цифровой казуализации особой части и появления цифровых двойников уголовно-правовых запретов. Иначе так можно дойти до разделения вымогательства и кибервымогательства или убийства и киберубийства»[1]. Вместе с тем, при всей обоснованности позиции о недопустимости необоснованного дублирования уголовно-правовых запретов, проведенный анализ показывает, что ряд видов преступных деяний, в частности состязательные воздействия на ИИ-системы БТС не могут быть квалифицированы в рамках действующих уголовно-правовых механизмов, сформированных в иных технологических реалиях. Это связано не с простым применением цифровых средств для совершения традиционных преступлений, а с появлением качественно нового способа воздействия, который обходит классические понятия «управления» транспортным средством и «неправомерного доступа» к компьютерной информации. Искусственный интеллект в этих случаях автономно принимает общественно опасные решения под внешним дезинформационным влиянием, что не является ни прямым управлением, ни взломом. Следовательно, действующая правовая база оказывается недостаточной для адекватного охвата этого специфического механизма причинения вреда.

[1] Квазисубъект или орудие преступления: что делать с ИИ: репортаж с Петербургского международного юридического форума // URL: https://pravo.ru/lf/story/258776/ (дата обращения: 10.12.2025).

Также при квалификации подобных деяний следует учитывать умысел правонарушителя. В зависимости от установленного умысла преступника квалификация содеянного может быть различной. Если имелся прямой или косвенный умысел на причинение смерти или тяжкого вреда здоровью конкретному лицу, действия атакующего будут квалифицироваться по статьям 105 УК РФ («Убийство») или 111 УК РФ («Умышленное причинение тяжкого вреда здоровью») соответственно. В таком случае кибератака на ИИ-систему БТС будет рассматриваться как способ совершения особо тяжкого преступления, возможно, с квалифицирующим признаком убийства, совершенного общеопасным способом (п. «е» ч. 2 ст. 105 УК РФ), поскольку манипуляция автономным транспортным средством создает угрозу неопределенному кругу лиц.

На наш взгляд, наиболее острый правовой пробел проявляется в ситуациях, когда злоумышленник целенаправленно воздействовал на ИИ-систему БТС (например, ради эксперимента или хулиганства), но не имел умысла на причинение тяжкого вреда здоровью или смерти, а такие последствия наступили по неосторожности. В данном случае ни глава 28 УК РФ, ни статья 264 УК РФ (даже с расширенным субъектом) не могут быть применены в полной мере для адекватной уголовно-правовой оценки.

Результаты проведенного анализа свидетельствуют о необходимости предусмотреть в главе 28 УК РФ «Преступления в сфере компьютерной информации» новый состав преступления, который бы охватывал неправомерное воздействие на системы искусственного интеллекта автономных транспортных средств, повлекшее тяжкие последствия по неосторожности. Это позволит устранить существующий правовой пробел и обеспечить адекватную защиту общественной безопасности в условиях технологического прогресса.

СПИСОК ИСТОЧНИКОВ

1. Хилюта В. В. Уголовное право в социальном измерении (контуры перемен и новой стратегии развития). Москва, 2023. 440 с.
2. Намиот Д.Е., Куприяновский В.П., Пичугов А.А. Состязательные атаки для автономных транспортных средств // International Journal of Open Information Technologies. 2024. Т. 12. № 7. С. 139–149.
3. Чехонина Е.А., Костюмов В.В. Обзор состязательных атак и методов защиты для детекторов объектов // International Journal of Open Information Technologies. 2023. Т. 11. № 7. С. 11–20.
4. Коробеев А.И., Чучаев А.И. Беспилотные транспортные средства: новые вызовы общественной безопасности // Lex Russica (Русский закон). 2019. № 2. С. 9–28.
5. Каменова Н.А. Проблемы квалификации дорожно-транспортных преступлений с участием транспортных средств, оснащенных автоматизированной системой управления // Юридическая наука и правоохранительная практика. 2025. № 4 (74). С. 141–147.
6. 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. 235–241.
7. Дремлюга Р.И., Коробеев А.И. Преступные посягательства на системы искусственного интеллекта: уголовно-правовая характеристика // Russian Journal of Criminology. 2023. Т. 17. № 1. С. 5–12.

REFERENCES

1. Hilyuta V. V. Ugolovnoe pravo v social'nom izmerenii (kontury peremen i novoj strategii razvitiya). Moscow, 2023. 440 s.
2. Namiot D.E., Kupriyanovskij V.P., Pichugov A.A. Sostyazatel'nye ataki dlya avtonomnyh transportnyh sredstv // International Journal of Open Information Technologies. 2024. T. 12. № 7. S. 139–149.
3. Chekhonina E.A., Kostyumov V.V. Obzor sostyazatel'nyh atak i metodov zashchity dlya detektorov ob"ektov // International Journal of Open Information Technologies. 2023. T. 11. № 7. S. 11–20.
4. Korobeev A.I., Chuchaev A.I. Bespilotnye transportnye sredstva: novye vyzovy obshchestvennoj bezopasnosti // Lex Russica (Russkij zakon). 2019. № 2. S. 9–28.
5. Kamenova N.A. Problemy kvalifikacii dorozhno-transportnyh prestuplenij s uchastiem transportnyh sredstv, osnashchennyh avtomatizirovannoj sistemoj upravleniya // Yuridicheskaya nauka i pravoohranitel'naya praktika. 2025. № 4 (74). S. 141–147.
6. Talan A.S., Talan M.V. Prestupleniya, sovershaemye s ispol'zovaniem iskusstvennogo intellekta: analiz riskov i pravovye perspektivy // Vestnik ekonomiki, prava i sociologii. 2025. № 3. S. 235–241.
7. Dremlyuga R.I., Korobeev A.I. Prestupnye posyagatel'stva na sistemy iskusstvennogo intellekta: ugolovno-pravovaya harakteristika // Russian Journal of Criminology. 2023. T. 17. № 1. S. 5–12.

Информация об авторах:
Талан Мария Вячеславовна, доктор юридических наук, профессор, заведующая кафедрой уголовного права Казанского (Приволжского) федерального университета, профессор кафедры уголовного права и процесса Университета управления «ТИСБИ» (Казань), e-mail: mtalan@inbox.ru
Каменова Наталья Андреевна, преподаватель кафедры административного права, административной деятельности и управления органов внутренних дел Казанского юридического института МВД России, e-mail: kamenova.nat@mail.ru
Авторы прочитали и одобрили окончательный вариант рукописи

Information about the authors:
Talan Maria V., Doctor of Law (Doctor habilitatus) Professor, Head of the Criminal Law Department at Kazan (Volga Region) Federal University, Professor of the Criminal Law and Procedure Department at the University of Management "TISBI" (Kazan), e-mail: mtalan@inbox.ru
Kamenova Natalya A., Lecturer in the Department of Administrative Law, Administrative Activity, and Management of Internal Affairs Bodies at the Kazan Law Institute of the Ministry of Internal Affairs of Russia, e-mail: kamenova.nat@mail.ru
The authors have read and approved the final version of the manuscript.

Заявленный вклад авторов
Талан Мария Вячеславовна – постановка проблемы и концепция исследования; поиск аналитических материалов в официальных источниках; формирование выводов исследования; окончательное утверждение версии для публикации.
Каменова Наталья Андреевна – сбор, анализ, интерпретация полученных данных; подготовка первоначального варианта текста; описание результатов исследования; осуществление критического анализа и доработка текста.

Статья получена: 27.11.2025.
Статья принята к публикации: 23.03.2026.
Статья опубликована онлайн: 31.03.2026.
Против размещения полнотекстовой версии статьи в открытом доступе в сети Интернет не возражаем.