Дата поступления рукописи в редакцию: 14.09.2026 г. DOI: 10.24412/2782-3830-2026-11-318-323
Дата принятия рукописи в печать: 12.11.2026 г.

БАТОЧКО О.В.,
доцент кафедры уголовного права ФГБОУ ВО «Юго-Западный государственный университет», кандидат юридических наук, майор полиции в отставке, e-mail: mail@law-books.ru

ГУСЕЯН Г.О.,
студент группы ПД-22 специальности 40.05.02 Правоохранительная деятельность, специализация «Обеспечение безопасности в уголовно-исполнительной системе», e-mail: gulya.guseyan22@mail.ru

ОКУНЕВА А.О.,
студент группы ПД-22 специальности 40.05.02 Правоохранительная деятельность, специализация «Обеспечение безопасности в уголовно-исполнительной системе», e-mail: mail@law-books.ru

КВАЛИФИКАЦИЯ ПРЕСТУПЛЕНИЙ ТЕРРОРИСТИЧЕСКОЙ НАПРАВЛЕННОСТИ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И АВТОНОМНЫХ СИСТЕМ

Аннотация. *Статья посвящена проблема уголовно-правовой квалификации преступлений террористической направленности, совершенных с использованием технологий искусственного интеллекта и автономных систем. Авторами рассматривается понятие преступлений террористической направленности и террористического характера, оценивается их нормативная регламентация и определяется значение в квалификации деяний. Исследована специфика объективной стороны, причинной связи и субъективного вменения в условиях, когда общественно опасные последствия причиняются не непосредственно действиями человека, а через автономное алгоритмическое решение ИИ-агента. Подчеркивается, что искусственный интеллект и автономные системы не являются субъектами уголовного права и не могут нести ответственность.*

Ключевые слова: *технологии искусственного интеллекта, автономные системы, преступления террористической направленности, преступления террористического характера, субъект преступления, причинно-следственная связь.*

Для цитирования: *Баточко О. В., Гусеян Г. О., Окунева А. О. Квалификация преступлений террористической направленности, совершенных с использованием искусственного интеллекта и автономных систем // Российский научный вестник. 2026. № 11. С. 318–323.*

BATOCHKO O.V.,
associate professor at the Department of Criminal Law at the Southwest State University, Candidate of Legal Sciences, and a retired police major

GUSEYAN G.O.,
student in group PD-22, majoring in Law Enforcement, with a specialization in "Ensuring Security in the Penitentiary System"

OKUNEVA A.O.,
student in group PD-22, majoring in Law Enforcement, with a specialization in «Ensuring Security in the Penitentiary System»

QUALIFICATION OF CRIMES OF A TERRORIST NATURE COMMITTED USING ARTIFICIAL INTELLIGENCE AND AUTONOMOUS SYSTEMS

Annotation. *The article is devoted to the problem of criminal-legal classification of terrorist crimes committed using artificial intelligence technologies and autonomous systems. The authors examine the concept of terrorist crimes and crimes of a terrorist nature, assess their regulatory framework, and determine their significance in the classification of acts. The study examines the specifics of the objective side, the causal relationship, and subjective imputation in conditions where socially dangerous consequences are caused not directly by human actions, but through an autonomous algorithmic decision of an AI agent. It is emphasized that artificial intelligence and autonomous systems are not subjects of criminal law and cannot be held liable.*

Key words: *artificial intelligence technologies, autonomous systems, terrorist crimes, terrorist crimes, the subject of the crime, causation.*

For citation: *Batochko O. V., Guseyan G. O., Okuneva A. O. Qualification of crimes of a terrorist nature committed using artificial intelligence and autonomous systems. Russian scientific bulletin. 2026;(11):318–323. (In Russ.).*

28 сентября 2026 года по случаю 25 – летия со дня создания Контртеррористического комитета Совета Безопасности ООН глава Контртеррористического управления ООН Дмитрий Зуев заявил, что терроризм как общественно-опасное и деструктивное явление продолжает эволюционировать [1]. Пользуясь нестабильной и сложной обстановкой в мире, террористы расширяют географию своей деятельности, а также внедряют в нее новые и развивающиеся технологии, в числе которых немаловажное место занимают технологии искусственного интеллекта (далее по тексту – ИИ) [2, с.126].

Столь нарастающие темпы развития терроризма и всё более активное применение террористами новых технологий доказывают ограниченную эффективность борьбы с данным явлением как со стороны органов государственного управления, так и международных организаций. История борьбы с терроризмом насчитывает не одно десятилетие, однако полностью искоренить данное явление не представляется возможным по настоящее время. Показательно, что государства реагируют на угрозы террористической направленности и на институциональном уровне. Так, к примеру Указом президента Российской Федерации в 2015 году в Министерстве иностранных дел Российской Федерации была учреждена новая должность – заместителя министра по вопросам противодействия терроризму [3].

Появление и стремительное развитие технологий искусственного интеллекта несомненно сказалось на всех сферах общественной жизни, правоприменительная деятельность не стала исключением. Каждый технологический рост и прорыв ставят перед компетентными государственными органами вопрос: как правильно квалифицировать деяние, совершенное с использованием новых средств.

Проблемы квалификации во многом обусловлены тем, что правоприменитель сталкивается с явлениями, содержание которых остается неопределенным. В связи со сказанным, прежде чем рассматривать проблемы уголовно – правовой квалификации, обратимся к определению ключевых понятий по теме исследования.

В правоприменительной деятельности и юридической доктрине для обозначения деяний, связанных с терроризмом, используются два термина — «преступления террористического характера» и «преступления террористической направленности», которые имеют достаточно похожую сущностную схожесть, но принципиально различную степень нормативной легитимности. «Преступления террористического характера» фигурировали в тексте утратившего силу Федерального закона от 25 июля 1998 г. № 130-ФЗ «О борьбе с терроризмом», в котором под такими преступлениям подразумевался перечень деяний, связанных с терроризмом. Вместе с тем действующий Федеральный закон от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму» данного понятия не содержит, оперируя категориями «терроризм», «террористическая деятельность» и «террористический акт». Несмотря на это, термин «преступления террористического характера» продолжает встречаться в ряде нормативных актов, например в Концепции противодействия терроризму в Российской Федерации (утв. Президентом РФ 5 октября 2009 г.) и в ведомственных нормативных актах — без определения и без указания на конкретные статьи Уголовного кодекса РФ (далее по тексту — УК РФ), что порождает правовую неопределённость. Термин «преступления террористической направленности» никогда не являлся законодательно определенным: он отсутствует как в федеральных законах, так и в УК РФ. Его использование обусловлено исключительно

Постановлением Пленума Верховного Суда РФ от 9 февраля 2012 г. № 1, в названии которого — «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности» — фигурирует данная дефиниция. Использование в Постановлении Пленума данной категории дает основание утверждать, что названный документ посвящен категории преступлений, формально отсутствующей в федеральном законе и УК РФ. Таким образом, оба термина в настоящее время не имеют легального закрепления, однако если первый имел историческое нормативное основание, то второй представляет исключительно доктринально-правоприменительное использование. Как отмечают С.Ю. Субочев и А.Н. Шмыгун [8, с.146], действующий Федеральный закон не охватил понятия «преступления террористического характера», что не облегчит правоприменительную работу специалистов и не разрешит один из проблемных вопросов: что следует понимать под преступлениями террористического характера.

Отсутствие легального термина «преступления террористической направленности» представляет собой серьезную проблему применительно к деяниям, совершаемым с использованием технологий искусственного интеллекта и автономных систем. Если в отношении традиционных террористических преступлений, правоприменитель опирается на сложившуюся правоприменительную практику и на разъяснения Пленума ВС РФ, то в отношении террористических преступлений, совершенных с использованием новых технологий, такая практика практически отсутствует [5].

Рассмотрим, как именно террористы используют искусственный интеллект в своей деятельности, поскольку практика последних лет свидетельствует о том, что террористические организации активно адаптируют достижения в области искусственного интеллекта и автономных систем для подготовки и совершения преступлений [4].

Во-первых, технологии искусственного интеллекта позволяют автоматизировать и систематизировать часть процессов преступной деятельности. В качестве примера выступает нигерийская террористская группировка «Боко Харам», внесённая Советом Безопасности ООН в список террористических организаций, основной целью которой было введение законов шариата на всей территории Нигерии и полного уничтожения западного образа жизни. Члены группировки рассматривали любую общественную и политическую деятельность, связанную с западными ценностями, как подлежащую безусловному запрету. К числу таких ценностей они относили светское образование, демократию западного образца и принцип разделения властей, голосование на выборах, ношение западной одежды, а также использование элементов современной западной культуры. В июле 2026 года, Cambridge Programme on AI Science & Policy (CASP) при Кембриджском университете был опубликован отчёт о применении ИИ внутри действующей террористической организации. Доклад основан на 57 полуструктурированных интервью с 27 бывшими участниками «Боко харам», проведённых на северо-востоке Нигерии в 2025–2026 годах. По словам бывших участников группировки, «Боко Харам» применял в своей деятельности такие сервисы как ChatGPT, Claude, Gemini, Grok, Meta AI и DeepSeek для перевода, пропаганды, оперативного планирования и технического устранения неполадок [9]. Кроме того, террористы не имели штатных инженеров и специалистов по вооружению, которых проблематично нанять, перевезти через границу и удержать. Боевики описывали системе возникающие технические проблемы (характеристики мотоциклов, необходимое расстояние, другие параметры), а ИИ выдавал готовое решение. В период с 2023 по 2024 год для членов «Боко Харам» были проведены обучающие семинары, где боевиков учили использовать ведущие ИИ чат-боты, устанавливать VPN и программы шифрования. На примере «Боко Харам» можно сделать вывод о том, что технологии ИИ используются террористами в качестве средства автоматизации и систематизации боевой деятельности. Помимо прочего, данный пример наглядно показывает конкретный квалификационный вопрос: если боевик получил от чат-бота техническое решение, которое привело к созданию мощного взрывного устройства, как это отражается на установлении субъективной стороны и причинно-следственной связи?

Другим направлением использования ИИ технологий террористами выступает создание масштабируемого пропагандистского контента террористическими организациями. Террористические организации посредством технологий ИИ генерируют изображения различного рода: видео контент новостных выпусков, а также дипфейки - аудиофайлы с голосами лидеров, читающих религиозные тексты. По данным американского аналитического центра Center for Strategic and International Studies, запрещенная в Российской Федерации международная террористическая организация Аль-Каида распространяла изображения, созданные с помощью технологий искусственного интеллекта, а в 2024 году киберструктура Аль-Каиды – «Электронная армия Аль-Малахем» выпустила уникальное руководство «Удивительные способы использования чат-ботов

на базе искусственного интеллекта», в котором была дана подробная инструкция по использованию технологий ИИ в деятельности организации. Помимо прочего, Аль-Каида использует инструменты искусственного интеллекта для перевода сообщений на различные языки [10]. Проблема квалификации таких деяний заключается в определении субъекта преступления. В данном случае правоприменитель стоит перед сложным выбором: субъект — оператор, использовавший ИИ и задавший промпт, разработчик модели или лицо, распространившее контент?

Одной из наиболее острых на данный момент сфер применения новых технологий террористами выступает использование автономных боевых систем — дронов и транспортных средств, способных к автономному распознаванию и поражению целей. Благодаря алгоритмам машинного обучения дроны могут анализировать изображения в реальном времени, идентифицировать цели и наносить удары без участия человека [6].

Примером использования автономных систем в совершении атак выступает операция «Паутина», проведенная вооруженными силами Украины 1 июня 2025 года накануне переговоров в Стамбуле лидеров двух стран. Суть указанной операции заключалась в атаке более 117 дронов на военные аэродромы России. Российские системы радиоэлектронной борьбы смогли успешно прервать канал связи между дронами и операторами, однако атака не прервалась. Дроны продолжили полёт и поразили цели благодаря терминальной автономии — режиму, в котором система самостоятельно распознаёт и удерживает цель по визуальным данным, без участия человека [11].

Таким образом можно сделать вывод о том, что решение о поражении конкретной цели принималось не человеком-оператором, а бортовым алгоритмом. Оператор лишь задавал общий маршрут и тип цели, а финальный выбор и наведение осуществлялись автономно. Проблема квалификации деяний с использованием автономных систем также состоит в том, что классическая модель состава преступления, где обязательны субъективная сторона преступления и причинно-следственная связь ставится под сомнение.

Рассмотрев основные направления использования ИИ технологий и автономных систем в совершении преступлений террористической направленности, можно отметить ряд проблем в квалификации таких деяний. Во-первых, классическая модель уголовного права предусматривает, что субъективная сторона преступления — это внутренняя, психическая сторона деяния, которая отражает отношение лица к совершаемому им общественно опасному действию (бездействию) и его последствиям. То есть преступное деяние состоит из схемы умысел – деяние – преступный результат. В то время технологии искусственного интеллекта и автономные системы «вставляют» нечеловеческого агента между человеческим намерением и применением силы. Человек может запустить дрон с намерением атаковать военный объект, но система, «самостоятельно» интерпретировав данные сенсоров, выберет гражданскую цель. Кроме того, искусственный интеллект не обладает сознанием, волей и правосубъектностью, поэтому не может быть субъектом преступления. Следовательно, его «решение», принимаемое автономными системами и ИИ не является умыслом в классическом уголовно-правовом смысле [7].

Помимо прочего, проблемным вопросом является квалификация таких деяний, где система принимает решение на основе самообучения, далее приводя дрон в действие. В таком случае крайне сложно доказать, что лицо, запустившее дрон, предвидело и желало наступления конкретных последствий. Это доказывает невозможность вменения прямого умысла и дальнейшего привлечения к ответственности конкретного лица. Также стоит отметить, что автономность алгоритмов затрудняет установление причинной связи в преступном деянии. Как указывают О.А. Козина и Е.А. Соколова, проблема усугубляется тем, что причинно-следственная связь между действиями разработчика или владельца и вредом, причиненным автономной системой, может быть разорвана. Разработчик не предвидел и не мог предвидеть конкретное решение, принятое системой на основе самообучения; владелец не вмешивался в работу алгоритма» [12, с.76].

Помимо прочего, использование в террористических преступлениях технологий ИИ и автономных систем подтверждает теорию «опосредованного вреда» - ситуация, когда вред наступает не напрямую от деяния виновного, а через цепочку событий или с использованием «посредника - через автономное алгоритмическое поведение ИИ-агента. Первоначальным звеном выступают действия разработчика — создание алгоритма, обучение модели, однако это действие отделено от наступившего и само по себе не порождает общественно опасных последствий. Далее оператор запускает систему, вводит исходные данные, ставит задачи или выбирает режим функционирования. Это звено также не находится в непосредственной причинной связи с конкретными общественно-опасными последствиями, поскольку оператор, как правило, не контролирует все последующие решения системы и не может предвидеть их в полном объёме. Затем в цепочку вступает автономное «решение» системы — выбор цели, определение способа и момента воздей-

ствия, которые осуществляются алгоритмом на основе самообучения. Именно это звено является ключевым: оно не является действием человека в уголовно-правовом смысле, но именно оно непосредственно обусловливает наступление вреда. Замыкающим звеном выступает наступление вреда — общественно опасных последствий, предусмотренных уголовным законом. Следовательно, причинная связь не обрывается, а растягивается: между действием человека и результатом возникает нечеловеческий агент, который принимает решение самостоятельно.

Таким образом, проведенный анализ позволяет утверждать, что применение террористической деятельности технологий ИИ и автономных систем подтверждает теорию опосредованного вреда в уголовном праве, при котором между действиями человека и преступным результатом появляется звено в виде автономного алгоритмического решения. Квалификация преступлений террористической направленности, совершенных с использованием ИИ и автономных систем, должна основываться на анализе следующих элементов: 1) роли и намерений разработчика; 2) действий оператора (запуск, ввод данных, постановка задач, выбор режима); 3) степени автономности и предсказуемости системы; 4) возможности и обязанности человека предвидеть и контролировать поведение системы; 5) наличия специальной цели террористического преступления. Совершение преступлений террористической направленности с использованием рассматриваемых технологий не создает нового состава, но влияет на квалификацию как способа, средства, обстановки и степени общественной опасности деяния, а в перспективе требует уточнения разъяснений Пленума ВС РФ и, возможно, введения квалифицирующего признака.

Список литературы:

[1] В ООН заявили, что террористы все чаще используют ИИ. URL: https://tass.ru/mezhdunarodnaya-panorama/28159243 (дата обращения: 03.10.2026).

[2] Рогожина С.Г. Квалификация преступлений, совершённых с использованием искусственного интеллекта: новые вызовы для уголовного закона // Всероссийский научный журнал «Вопросы права». 2026. № 4. С. 126-129.

[3] О заместителе Министра иностранных дел Российской Федерации по вопросам противодействия терроризму: Указ Президента Российской Федерации от 19.03.2015 № 143 // Доступ из справочно-правовой системы «КонсультантПлюс».

[4] Российская Федерация. Законы. О борьбе с терроризмом: Федеральный закон от 25.07.1998 № 130-ФЗ: [утратил силу с 1 января 2007 г.] // Доступ из справочно-правовой системы «КонсультантПлюс».

[5] Российская Федерация. Законы. О противодействии терроризму: Федеральный закон от 06.03.2006 № 35-ФЗ: (ред. от 25.05.2026) // Доступ из справочно-правовой системы «КонсультантПлюс».

[6] Концепция противодействия терроризму в Российской Федерации: утв. Президентом Российской Федерации 05.10.2009 № Пр-2540 // Доступ из справочно-правовой системы «КонсультантПлюс».

[7] О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности: постановление Пленума Верховного Суда Российской Федерации от 09.02.2012 № 1: (ред. от 03.11.2016) // Доступ из справочно-правовой системы «КонсультантПлюс».

[8] Субачев С. Ю., Шмыгун А.Н. Закрепление категории "преступления террористического характера" в федеральном законе "о противодействии терроризму" // Общество и право. 2006. № 2(12). С. 146-147.

[9] В Кембридже описали использование ChatGPT, Claude и Gemini боевиками «Боко харам». URL: https://citforum.ru/news/47204/ (дата обращения: 07.10.2026).

[10] Аль-Каида: предыстория, текущее состояние и политика США. URL: https://www.iimes.ru/?p=108966/ (дата обращения: 07.10.2026).

[11] Бортников: Украина провела операцию "Паутина" под руководством Британии. URL: https://rg.ru/2025/10/16/bortnikov-ukraina-provela-operaciiu-pautina-pod-rukovodstvom-britanii.html/ (дата обращения: 07.10.2026).

[12] Козина О. А. Искусственный интеллект как орудие преступления: проблемы вменения и субъекта ответственности // Сфера науки. 2026. Т. 1, № 6. С. 70-81.

References:

[1] The UN said terrorists are increasingly using AI. URL: https://tass.ru/mezhdunarodnaya-panorama/28159243 (access date: 03.10.2026).

[2] Rogozhina S.G. Qualification of crimes committed using artificial intelligence: new challenges for the criminal law // All-Russian scientific journal "Questions of Law." 2026. № 4. S. 126-129.

[3] On the Deputy Minister of Foreign Affairs of the Russian Federation for Countering Terrorism: Decree of the President of the Russian Federation of 19.03.2015 No. 143 // Access from the ConsultantPlus legal system.

[4] Russian Federation. Laws. On the fight against terrorism: Federal Law of 25.07.1998 No. 130-FZ: [expired on January 1, 2007] // Access from the ConsultantPlus legal reference system.

[5] Russian Federation. Laws. On countering terrorism: Federal Law No. 06.03.2006 of 35-FZ: (as amended by 25.05.2026) // Access from the ConsultantPlus legal system.

[6] The concept of countering terrorism in the Russian Federation: approved by The President of the Russian Federation 05.10.2009 No. Pr-2540 // Access from the ConsultantPlus legal system.

[7] On some issues of judicial practice in criminal cases of terrorist crimes: decision of the Plenum of the Supreme Court of the Russian Federation of 09.02.2012 No. 1: (ed. 03.11.2016) // Access from the ConsultantPlus reference and legal system.

[8] Subachev S. Yu., Shmygun A.N. Consolidation of the category "crimes of a terrorist nature" in the federal law "on countering terrorism" // Society and law. 2006. № 2(12). S. 146-147.

[9] Cambridge described the use of ChatGPT, Claude and Gemini by Boko Haram militants. URL: https://citforum.ru/news/47204/ (access date: 07.10.2026).

[10] Al Qaeda: Background, Current Status, and U.S. Policy. URL: https://www.iimes.ru/?p=108966/ (access date: 07.10.2026).

[11] Bortnikov: Ukraine conducted Operation Web under British leadership. URL: https://rg.ru/2025/10/16/bortnikov-ukraina-provela-operaciiu-pautina-pod-rukovodstvom-britanii.html/ (дата обращения: 07.10.2026).

[12] Kozina O. A. Artificial intelligence as an instrument of crime: problems of imputation and the subject of responsibility // Sphere of science. 2026. T. 1, NO. 6. S. 70-81.

